Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Neufassung der BSI-Vorgaben zu Zufallszahlengeneratoren (AIS 20/31)

Prof. Dr. Werner Schindler, Dr. Matthias Peter

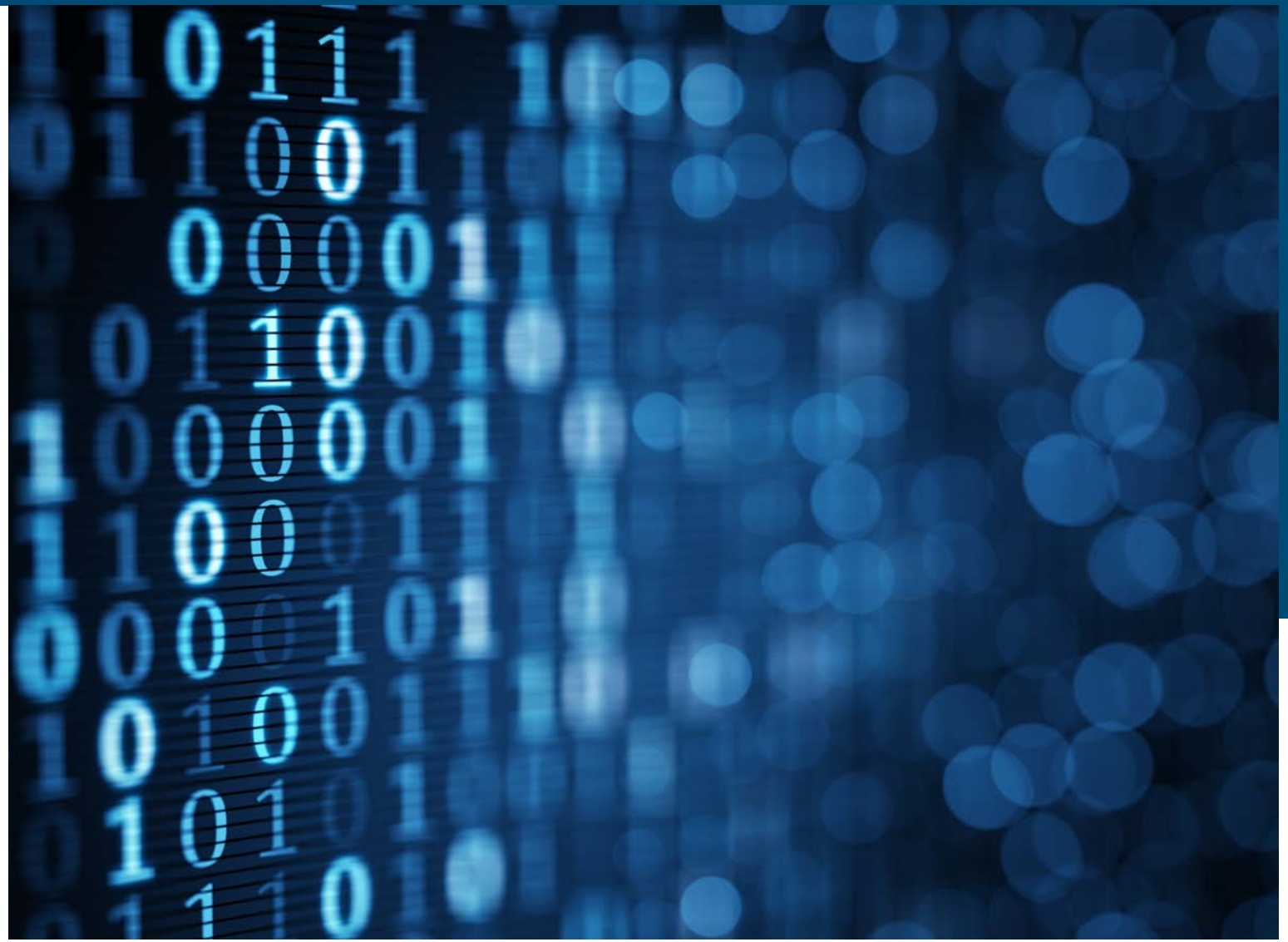
Bundesamt für Sicherheit in der Informationstechnik

Omnisecure 2024

Berlin, den 24.01.2024

Übersicht

- Motivation
- Klassifizierung von Zufallszahlengeneratoren
- AIS 20/31
- Zusammenfassung und Ausblick
- Fragen



Zufallszahlen in kryptographischen Anwendungen

- Schlüssel (Langzeitschlüssel, Sessionkeys)
- Signaturschlüssel und Signaturparameter
- Schlüsseleinigungsprotokolle
- Ephemeralschlüssel, Nonces
- Blinding- und Masking-Werte
- Challenge-Response-Verfahren
- …

Zufallszahlengeneratoren (RNGs): Bekannte Negativbeispiele

Ist es einfach, einen guten RNG zu designen und herzustellen?

- Linux Debian (2008)
  - Über ein Jahr lang konnten die Zufallszahlen nur 2^{15} = 32.768 Werte annehmen.
  - Ursache: 1 Codezeile war versehentlich auskommentiert worden.
- Digitale Taiwanesische Bürgerzertifikate (2013, Bernstein et al.)
  - Von ca. 2 Mio. RSA-Instanzen (1024-Bit) besaßen 46 RSA-Moduli die Primzahl
    0xc000000000000000000000000000000000000000000000000000000000000000000000000000
    00000000000000000000000000000000000000000000000002f9
    (= kleinste Primzahl > $2^{511} + 2^{510}$)

Anforderungen an Zufallszahlengeneratoren (RNGs)

Schwache Zufallszahlengeneratoren können grundsätzlich starke kryptographische Mechanismen entscheidend schwächen.

- Intuitive Anforderung:

Zufallszahlen sollten auf ihrer Wertemenge gleichverteilt und unabhängig von ihren Vorgängern sein.

- Problem: Dies charakterisiert einen idealen RNG. **Ideale RNGs existieren in der realen Welt nicht!**
- Ziel: Ein RNG sollte sich *in gewisser Hinsicht* (nahezu) wie ein idealer RNG verhalten.

Einteilung in Klassen

Es gibt sehr viele unterschiedlicher RNG-Designs. Diese kann man grob in drei Klassen unterteilen.

- **DRNG**s (deterministische RNGs; auch: Pseudozufallszahlengeneratoren)
  - Die Zufallszahlen hängen nur von Seed (und ggf. zusätzlichem Input ab)
- **PTRNG**s (physikalische RNGs)
  - Eine physikalische Rauschquelle nutzt physikalische Phänomene von dediziertem Hardwaredesign oder von physikalischen Experimenten aus.
  - Beispiele: Diodenschaltungen, Oszillatorschaltungen usw.
- **NPTRNG**s (nichtphysikalische nichtdeterministische RNGs)
  - Nichtphysikalische Rauschquellen nutzen üblicherweise Systemdaten (Timer, RAM usw.) oder Nutzerinteraktionen (Mausbewegungen usw.)

25 Jahre AIS 20 / 31

- Die Common Criteria machen keine Vorgaben, wie RNGs evaluiert werden sollen.
- Im deutschen Zertifizierungsschema (CC) sind die AIS 20 (deterministische Zufallszahlengeneratoren) seit 1999 und die AIS 31 (physikalische Zufallszahlengeneratoren) seit 2001 verbindlich.
- AIS 20 und AIS 31 referenzieren auf eine mathematisch-technische Anlage, welche im Sprachgebrauch (je nach Zusammenhang) selbst als AIS 20, AIS 31 oder AIS 20/31 bezeichnet wird.
- Aktuelle Version: seit 2011

- Die TR 02102 (empfohlene kryptographische Verfahren) referenziert die AIS 20/31.
- Die AIS 20/31 ist auch für VS-Zulassungsverfahren relevant.

AIS 20 / 31: Update

- Die AIS 20/31 befindet sich seit mehreren Jahren in einem Updateprozess
  - Autoren: Matthias Peter, Werner Schindler

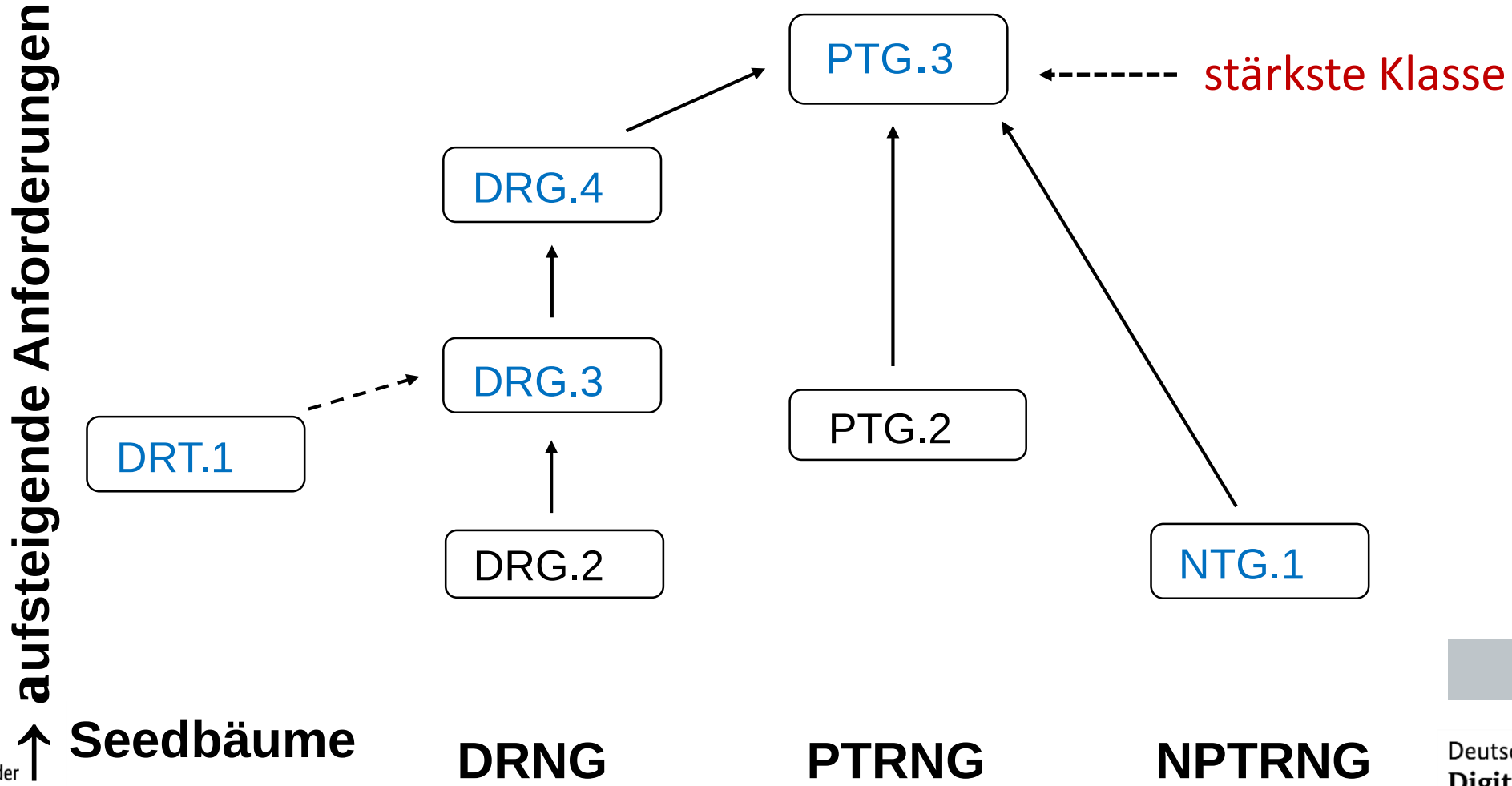
- Timeline
  - September 2022: Draft wird veröffentlicht
  - Februar 2023: Ende der Kommentierungsperiode
  - Juni 2023: Internationaler AIS 20/31-Workshop
  - Neue AIS 20/31 soll in Q2 / 2024 veröffentlicht werden.

Grundphilosophie der AIS 20/31

- Die AIS 20/31 ist technologieneutral.
- Es gibt keine „Approved Designs“.
- Stattdessen definiert die AIS 20/31 sieben Funktionalitätsklassen. Dort sind Anforderungen formuliert, die ein RNG erfüllen muss, um zu dieser Klasse konform zu sein.

- Der Antragsteller und die Prüfstelle müssen nachweisen, dass alle Anforderungen der angestrebten Funktionalitätsklasse erfüllt sind.

AIS 20 / 31: Funktionalitätsklassen (neu)



Stochastisches Modell

- Für die Evaluierung von physikalischen RNGs verlangt die AIS 20/31 ein *stochastische Modell*.
- Ein stochastische Modell beschreibt die relevanten Eigenschaften einer physikalischen Rauschquelle durch Zufallsvariablen.
  - Im Idealfall spezifiziert das stochastische Modell eine Familie von Wahrscheinlichkeitsverteilungen, die zu jedem Zeitpunkt die tatsächliche Verteilung der Rohzufallszahlen enthält.
- **Ziel**: zuverlässige Quantifizierung einer unteren Entropieschranke für die ausgegebenen Zufallszahlen.

- ISO/IEC 20543 erfordert für PTRNGs ebenfalls ein stochastisches Modell.
- NIST SP 800-90 B verlangt eine Begründung, woher die Entropie stammt (Entropienachweis mit stochastischem Modell z. Zt. noch optional).
- In der wissenschaftlichen Literatur ist die Konformität von physikalischen RNGs zur AIS 31 seit vielen Jahren ein übliches Ziel.

BSI, ANSSI, NIST

- Seit 2015 besteht ein gegenseitiges Anerkennungsabkommen zwischen BSI und ANSSI bezüglich PTG.2-Zertifizierungen.

- BSI und NIST arbeiten daran, die AIS 20/31 und NIST SP 800-90 zu harmonisieren.
- In Kürze geben NIST und BSI ein gemeinsames Dokument heraus, in denen Gemeinsamkeiten und Unterschiede zwischen den Funktionalitätsklassen der AIS 20/31 und den RBG-Konstruktionen der NIST SP 800-90 erläutert werden.
  - Dies soll Hersteller unterstützen, RNGs zu entwickeln, die sowohl zur AIS 20/31 als auch zu NIST SP 800-90 konform sind.

Zusammenfassung und Ausblick

- Die Evaluierung von RNGs benötigt geeignete Vorgaben / Standards.
- Im deutschen Zertifizierungsschema (CC) sind seit mehr als 20 Jahren die AIS 20 und AIS 31 verbindlich.
- Eine neue Version der AIS 20/31 tritt in Kürze in Kraft.
- BSI und NIST arbeiten an der Harmonisierung der AIS 20/31 und NIST SP 800-90.

Vielen Dank für Ihre Aufmerksamkeit!

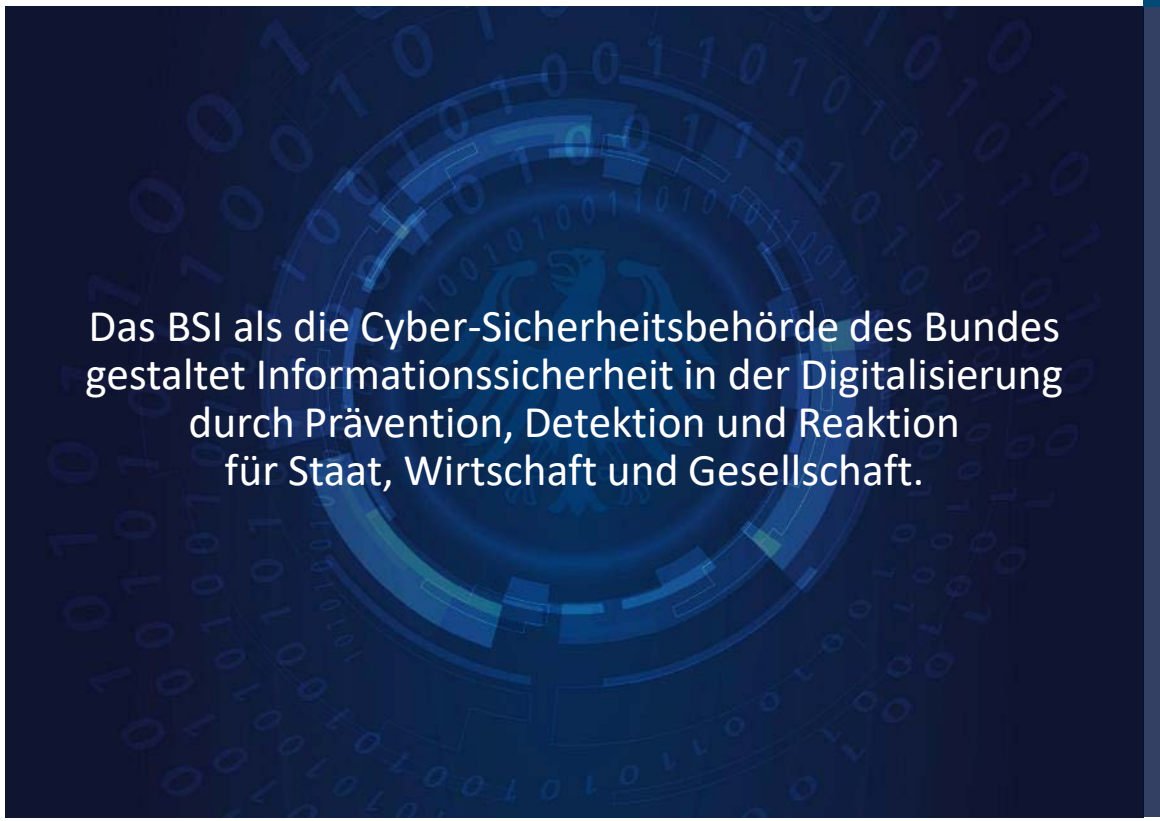
Deutschland
Digital•Sicher•BSI•

Kontakt

Prof. Dr. Werner Schindler (RL KM 22),
Dr. Matthias Peter (RL KM 24)

vorname.name@bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189
53175 Bonn
www.bsi.bund.de



Bundesamt
für Sicherheit in der
Informationstechnik