

Update of German Guidance for RNG Evaluation

Wolfgang Killmann
T-Systems



Motivation

Why random number generators?

- Randomness
 - The outcome of random experiments are unpredictable.
 - Outcomes of ideal random experiments are independent and unbiased.
- Random number generator (RNG) are IT security primitives.
 - RNG are ideal generators of **secrets** like cryptographic keys.
 - RNG produce **fresh numbers** like challenges of cryptographic protocols. (because of birthday paradox deterministic RNG may be suitable better than true physical RNG)
- RNG are often critical vulnerabilities of products!
 - e.g. Debian Linux OpenSSL vulnerability of key generation



Motivation

Why guidance for RNG evaluation?

- RNG use specific technology.
 - Normally computers work deterministically.
How does RNG generate random numbers?
 - Even deterministic RNG need a random seed.
- Evaluation must consider the specific of RNG by application of appropriate evaluation methodology
 - Understanding of random sources, cryptographic algorithms
 - Tests of random source, quality self-tests, statistical tests
 - Specific vulnerability analysis



Motivation

Why update of the guidance AIS20 / AIS 31?

- German evaluation guidance are effective for
 - deterministic RNG (AIS 20) since 1999 and
 - physical RNG (AIS 31) since 2001
- Goal of the update
 - Taking into consideration the experience got in evaluation projects
 - New classes of RNG: hybrid RNG, non-physical true RNG
 - More precise guidance for the evaluators and certifiers in accordance with CC version 3.1



Overview of the Content

AIS 20 / AIS 31 Guidance

- Basic concepts
 - Concept of randomness and mathematical background
 - Basic design principals of random number generators
- Functional component FCS_RNG.1
 - Definition of the component FCS_RNG.1
 - Definition of predefined classes of RNG (based on previous classes)
 - Description of the expected evidence for the predefined RNG classes
- Evaluation guidance
 - Specific evaluation aspects for the assurance components (especially for ASE, ADV, ATE, AVA classes)
 - Examples



Overview of the Content

Basic Concepts

- The concept of randomness and the mathematical background
 - Term “randomness” as used for RNG design and analysis
 - Entropy and guess work
 - RNG as IT security primitive
 - Statistical tests (AIS20/AIS30 test suite, NIST test suite, special tests)
- Basic design principals of random number generators
 - Stochastic models of the noise source
 - Description of deterministic RNG as automaton



Functional Requirements

Functional Component FCS_RNG.1

FCS_RNG.1 Random number generation

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RNG.1.1 The TSF shall provide a [selection: *physical, non-physical true, deterministic, physical hybrid, deterministic hybrid*] random number generator, which implements: [assignment: *list of security capabilities*].

FCS_RNG.1.2 The TSF shall provide random numbers that meet [assignment: *a defined quality metric*].

Operations of the SFR component

- selection of the RNG type
- assignment of the security capabilities (depending on RNG type)
- assignment of the quality of the generated random numbers



Functional Requirements

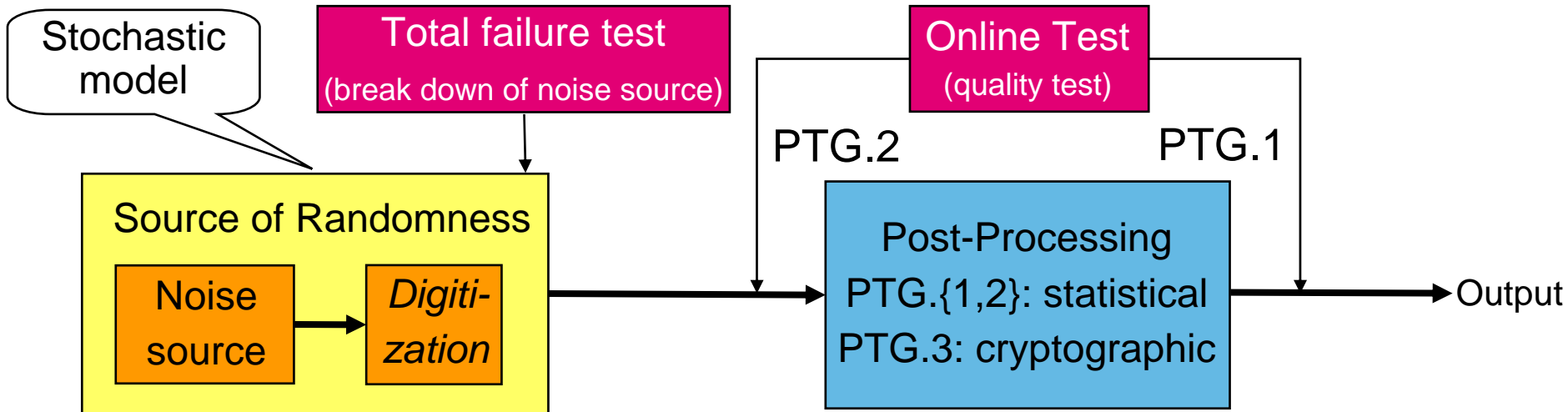
RNG Types

- **Physical RNG**
 - Physical noise source like radioactive decay, thermal noise, ...
- **Non-physical true RNG**
 - Non-physical noise source like human user input, waiting time of HD
- **Deterministic RNG**
 - Deterministic generation of sequences from random internal state
 - Standards are available (e.g. NIST SP 800-90)
- **Hybrid RNG**
 - Combination of true and deterministic RNG design
 - Physical hybrid RNG: true RNG produces more entropy than output
 - Deterministic hybrid RNG: RNG produces more output than entropy



Security Capabilities of RNG

True physical RNG



- Quality of the random numbers
 - PTG.{1,2,3}: random numbers pass statistical tests
 - PTG.{2,3}: entropy of the random numbers
- Hybrid true RNG combine true and deterministic RNG (PTG.3)

Security Capabilities of RNG

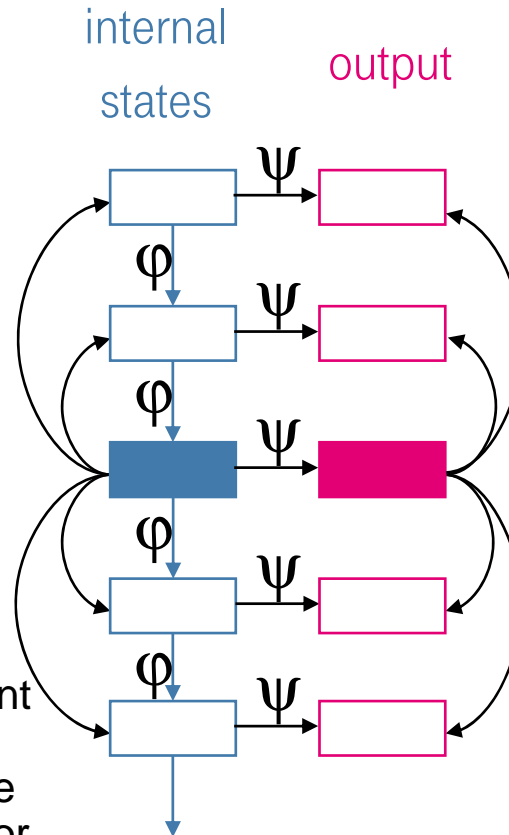
Deterministic RNG

- **Enhanced backward secrecy (DRG.3)**

The assurance that previous output values of a DRNG cannot be determined from the current internal state, the current or future output values.

- **Enhanced forward secrecy (DRG.4)**

The assurance that subsequent (future) values of a DRNG cannot be determined from the current internal state, current or previous output values.



- **Backward secrecy (DRG.2)**

The assurance that previous output values cannot be determined from current or future output values.

- **Forward secrecy (DRG.1)**

The assurance that subsequent (future) values cannot be determined from current or previous output values.



Functional Requirements

Quality Metric of Random Numbers

- Entropy in the RNG output as random source
 - Min-entropy as most conservative estimation of guess workfactor

$$\left\lfloor \frac{1}{2 \max_i \{p_i\}} \right\rfloor \leq \min_k \left\{ \frac{1}{2} < \sum_{i=1}^k p_i \right\} \leq \lceil (1 - \|p - u\|)n \rceil$$

$$\frac{n}{2} \|p - u\| \leq \frac{n-1}{2} - \left(\sum_{i=1}^n ip_i \right) \leq n \cdot \|p - u\|$$

- Other entropy measure for other purposes (e.g. distinct numbers)
- Note
 - Entropy in the deterministic RNG output is limited by the entropy of the internal state but not distinguishable from true random numbers



Evaluation Guidance

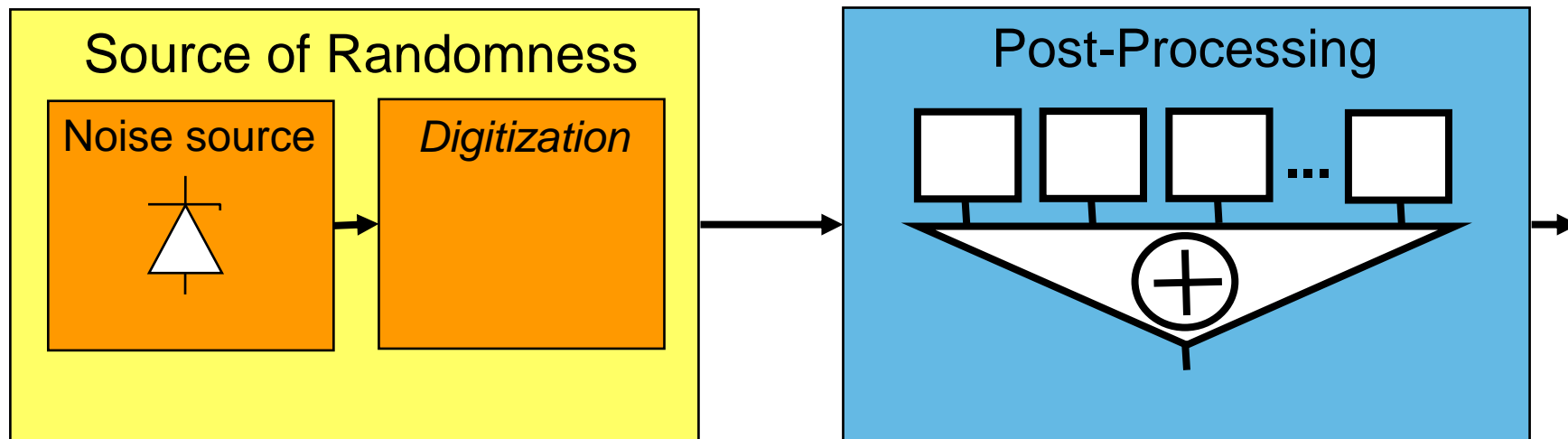
Principals

- The document guides the evaluator (and certifier) **how to apply** the evaluator work units of the CEM to RNG.
- Guidance is provided for all
 - RNG types
 - RNG specific aspects like APE/ASE, ADV, ATE and AVA
 - Evaluation levels
- Examples illustrate the application of the guidance.
 - Stochastic model
 - Statistical and penetration tests



Evaluation Guidance

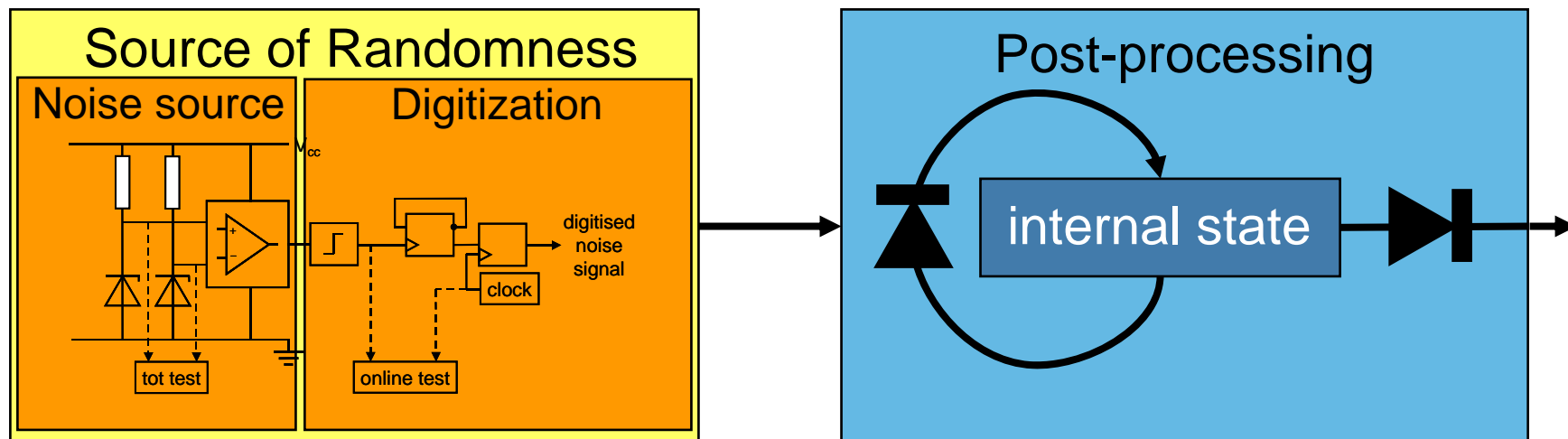
ADV_TDS.{1,2}: RNG Design



- ADV_TDS.1 (summary of behavior):
 - Identification of the noise source, overview how the random numbers are generated from the noise signal, allow for understanding of the effect of post-processing
- ADV_TDS.2 (description of behavior):
 - Description of the behavior of the noise source and the digitization,
 - Allow for understanding the effect of post-processing, state whether post-processing is mathematical or cryptographic

Evaluation Guidance

ADV_TDS.{3,4,5,6}: RNG Design



- purpose (mechanism level of description) of
 - noise source and digitization of the noise signal,
 - generation of the internal numbers by deterministic parts (automaton)
- purpose of security capabilities mechanisms
 - tot tests of the noise source, online (quality) tests of internal sequences
 - entropy estimator of non-physical true RNG

Evaluation Guidance

ATE: Testing of RNG

- Functional testing of the security capabilities
 - Tests of correct implementation of the deterministic parts
 - Effectiveness of the tot test and the (online) quality self-tests
- Statistical testing
 - Statistical tests substantiate the stochastic model of the noise source
 - Statistical tests of the RNG output
 - tests on external (ATE_COV) resp. internal interface (ATE_DPT)
- Note
 - Statistical tests after cryptographic post-processing are necessary but by no means sufficient for quality of the output.
 - Statistical tests of deterministic RNG check whether output can be distinguished from true random sequences by easy tests.



Evaluation Guidance

AVA: Typical Vulnerability

- Undetected breakdown of the noise source or non-tolerable statistical defects decreases the entropy of the output.
 - Physical noise sources may be affected by environmental conditions (e.g. power, temperature, clock).
 - Non-physical random sources may be manipulated or disabled.
 - Internal sequence and therefore the output may be guessed even in case of cryptographic post-processing if random source does not provide sufficient entropy.
- Internal states of deterministic RNG may be compromised.
 - Unprotected resources of RNG (ADV_ARC!)
 - Missing enhanced backwards and forwards secrecy as security capability



Evaluation Guidance

AVA: Attack Potential Quotation

	Security bits	Success probability of a single guess	Required min-entropy of the internal state	Recommended length of internal state
AVA_VAN.{1,2} (basic)	≥ 40 security bits	$\varepsilon \leq 2 \cdot 10^{-12}$	≥ 40 bit	≥ 80 bit
AVA_VAN.3 (extended basic)	≥ 48 security bits	$\varepsilon \leq 3 \cdot 10^{-15}$	≥ 48 bit	≥ 96 bit
AVA_VAN.4 (moderate)	≥ 64 security bits	$\varepsilon \leq 5 \cdot 10^{-20}$	≥ 64 bit	≥ 128 bit
AVA_VAN.5 (high)	≥ 100 security bits	$\varepsilon \leq 10^{-30}$	≥ 100 bit	≥ 200 bit



Summary

- The evaluation practice demonstrates the need of technology specific guidance. RNG is one example of such technology.
- Random number generators are important security primitives and unfortunately often critical vulnerabilities of the TOE.
- The update of the German guidance AIS 20 / AIS 31 is based on gained experience and actual developments in RNG technology and evaluation methodology.



Thank you for your attention.
Any question?

Wolfgang Killmann
T-Systems GEI GmbH
D-53111 Bonn, Rabinstrasse 8
wolfgang.killmann@t-systems.com

