# New AIS 20/31 with a focus on cryptographic postprocessing

Werner Schindler

Bundesamt für Sicherheit in der Informationstechnik

Bonn, Germany

## Abstract

In the German certification scheme (Common Criteria) the evaluation guidelines AIS 20 (deterministic RNGs) and AIS 31 (physical RNGs) have been effective since 1999 and 2001, respectively.

Version 3.0 of the mathematical-technical reference, often shortly denoted as AIS 20/31, has been published in September 2024.

The presentation begins with a brief overview of the functionality classes.

A new feature of AIS 20/31 is that min-entropy claims are possible.

In particular, functionality class PTG.3 allows to claim a lower bound $v \in [0.98, 1-2^{-32}]$ for the min-entropy per output bit.

The presentation addresses the question of how entropy claims can be verified.