Utimaco Entropy Source

SP800-90B Non-Proprietary Public Use Document

User Manual

utimaco®

Imprint

Copyright 2023	Utimaco IS GmbH Germanusstr. 4 D-52080 Aachen Germany
Phone	AMERICAS: +1-844-UTIMACO (+1 844-884-6226) EMEA: +49 800-627-3081 APAC: +81 800-919-1301
Internet	https://support.utimaco.com
Email	support@utimaco.com
Document version	0.0.3
Date	2023-07-31
Status	Wrk
Document No.	2023-0013
	CERT team
All Rights reserved	No part of this documentation may be reproduced in any form (printing, photocopy or according to any other process) without the written approval of Utimaco IS GmbH or be processed, reproduced or distributed using electronic systems. Utimaco IS GmbH reserves the right to modify or amend the documentation at any time without prior notice. Utimaco IS GmbH assumes no liability for typographical errors and damages incurred due to them. Any mention of the company name Utimaco in this document refers to the Utimaco IS GmbH. All trademarks and registered trademarks are the property of their respective owners.

Table of Contents

Change History

Version	Date	Change Description	Author
0.0.0	31/07/2023	First draft	CERT team
0.0.1	04/08/2023	First reviews and updates	DOC team HW team PM team CERT lab
0.0.2	15/09/2023	Lab review and updates	CERT team
0.0.3	05/10/2023	Updates no CryptoServer	CERT team

1 Description

The Utimaco true random number generator is a physical entropy source implemented in Utimaco's hardware security module product bundle with the family name SecurityServer including but not limited to different u.trust Anchor variants.

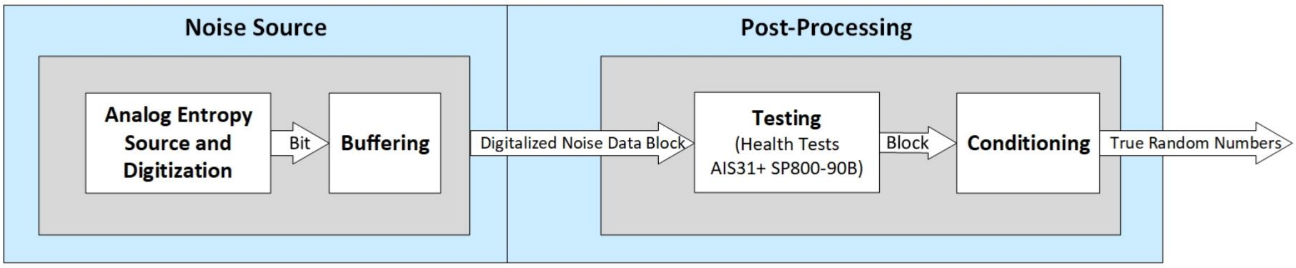

Figure 1: A single entropy source block diagram and its security boundary (blue).

The entropy source consists of both hardware and software components.

The hardware component includes the analog entropy source (noise source) and a Field Programmable Gate Array (FPGA). The digitization and buffering are part of the FPGA implementation (see HDL-FPGA in Table 1).

Software components include the driver and the RNGS service.

- The driver implements the hardware-level access to the FIFO.
- The RNGS is a service through which the random numbers are made available to the user space. It also implements a suite of health tests (AIS31, ACT, RCT) performed on raw data and conditions the raw data before making it available to consumer applications like the DRBG.

Figure 1 shows the block diagram of a single TRNG and its security boundary in blue.

Component version numbers are listed in Table 1.

Multiple instances of the TRNG can be implemented in parallel in a way that keeps the noise sources' data paths separated from each other.

Table 1: Entropy relevant version numbers

Component Name	Version Number
HW Noise Source	03.00.03
HDL-FPGA	3.0.1
Driver	2.0.1
RNGS	2.0.0

Note that the TRNG complies with all requirements of the AIS31 PTG.2 class. It has been already validated according the AIS31 test methodology as also to 90B (Cert#4151 https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4151).

2 Security Boundary

The security boundary of the entropy source shown as blue box in Figure 1 includes the components listed in Table 1.

The components of the random number generator are protected by the physical security mechanisms of the product.

3 Operating Conditions

Operation conditions match those described in the security policy of the product where the entropy source is embedded.

4 Configuration Settings

No external configuration is possible.

5 Physical Security Mechanisms

The entropy source inherits the physical security mechanisms of the product, where it is embedded. Please refer to the product security policy for more details.

6 Conceptual Interfaces

The entropy source provides proprietary interfaces only accessible in special development devices to provide access to raw data of the noise source.

No external interface is available to end-users except the possibility to restart the module to perform on-demand health testing.

7 Min-Entropy Rate

The Physical True Random Number Generator entropy source provides 0.815 bits of min-entropy per output bit. Therefore, it provides 417 bits of entropy per 512 bits input.

8 Health Tests

Tests on the digitalized noise data are continuously performed to check whether the TRNG is working correctly and to guarantee that only high-quality random numbers are validated as true random numbers.

The entropy source is tested at each start-up with the following test suite:

- Repetition Count Test (RCT) according to SP 800-90B section 4.4.1,
- Adaptive Proportion Test (APT) according to SP 800-90B section 4.4.2,
- Continuous Chi-Squared Test according to AIS 20/31 “A Proposal for Functionality Classes for Random Number" section 5.5.3 (version 2.0 Sep. 2011),

  Start-up Chi-Squared Test according to AIS 20/31 “A Proposal for Functionality Classes for Random Number" section 5.5.2 (version 2.0 Sep. 2011).

Apart from the Start-up Chi-Squared Test, the above-listed tests are also performed as continuous tests during operation.

Table 2 gives an overview about implemented health tests, their scopes, error states and error indicators if they fail.

Table 2: Health tests scopes and states by failure.

<table>
<tr><th>Defect</th><th>Test</th><th>Error State</th><th>Error Indicator</th></tr>
<tr><td>Stuck on single value for a long period of time</td><td>RCT</td><td>Noise alarm.</td><td rowspan="3">Audit log entry indicates noise alarm and

commands requiring TRNG are blocked</td></tr>
<tr><td>Large loss of entropy</td><td>APT</td><td>Noise alarm.</td></tr>
<tr><td>Non-tolerable entropy defects of the raw random numbers during continuous operation including stuck on single value, outer range numbers of pattern occurrences</td><td>Continuous Chi Squared Test</td><td>Noise alarm</td></tr>
</table>

Defect	Test	Error State	Error Indicator
Total failure of the physical noise source and severe statistical weaknesses on start-up	Start-up Chi-Squared Test	TRNG defective. u.trust Anchor RNGS service will continue with the other TRNGs. If they all fail, the module will try to boot the secondary boot image and initialize its multiple TRNG implementations. If they all fail, the module will boot in recovery mode.	

In case of a noise alarm, all buffered TRNG random blocks are erased and the TRNG is blocked.

On-demand testing is initialized by resetting, rebooting, or powering-up the module.

We choose α = 2^{-30}, C = 35 for RPT and C = 645 for APT which is sufficient for all devices with min entropy <= 0.9.

For the AIS 31 start-up and continuous tests, we took the parameters listed in Table 3 as proposed in AIS 20/31 “A Proposal for Functionality Classes for Random Number" section 5.5.2 (version 2.0 Sep. 2011).

Table 3: AIS3 test constants

Constant	Value
STMAX	65.00
CMAX	26.75
TMIN	13.00
TMAX	17.00
CTOT	269.5

9 Maintenance

There are no special maintenance requirements.

10 Required Testing

The user must rely on the health tests to detect any drops in entropy.

11 Vendor Permissions and Relationship

Companies other than the vendor, or subsidiaries of another company with validation, can only use the certificate with written and signed permission from Utimaco IS GmbH, Germanusstr. 4, 52080 Aachen, Germany.