SP 800-90B Non-Proprietary Public Use Document

Ultra IC Entropy Source

Firmware Version: 1.0

Ultra Intelligence and Communications
5990 Côte-de-Liesse
Montréal, Québec, Canada
H4T 1V7

Document Version 0.6

October 11, 2023

Revision History

Version	Change
0.1 – 0.4	Initial Draft and vendor/lab comments and updates.
0.5	First version for ESV submission.
0.6	Second version for ESV submission based on CMVP comments.

Table of Contents

1. Description

The Ultra IC Entropy Source is a proprietary non-physical entropy source. The entropy source has been designed solely for use in the Ultra Intelligence and Communications FIPS 140-3 validated radio products. The Ultra IC Entropy Source makes no IID claim for the entropy source.

2. Operating Environments and Conditions

Table 1 summarizes the operating conditions for the tested platform.

Parameter	Value
Operating System	Ultra IC Kernel v1.0
Processor	Freescale® QorIQ P2020 - Power PC with SEC 3.3.
Temperature	0 °C – 125 °C
Voltage	0.75V-1.35V
Clock speed	800 MHz, 1,200 MHz, 1,333 MHz

Table 1 - Operating Environment and Conditions

3. Configuration Settings

There are no specific configuration settings for the entropy source.

4. Physical Security Mechanisms

The Ultra IC Entropy Source is enclosed entirely within the module's cryptographic boundary, which is protected by tamper evident seals, anti-probing barriers and is assessed for FIPS level 2 Physical Security compliance.

5. Min-Entropy Rate

The Ultra IC Entropy Source provides 0.9 bits of entropy per output bit.

6. Health Tests

The NIST SP 800-90B (section 4) Repetition Count Test (RCT) and Adaptive Proportion Test (APT) health tests are run at start up and continuously during operation. The design aims to satisfy the Health Tests requirements specified in Section 4.3 of NIST SP 800-90B.

Two types of failures are handled: intermittent and persistent. The intermittent failures are designed to have a false positive probability between 2^{-20} and 2^{-40}, as specified in Section 4.3 in NIST SP 800-90B, paragraph 3. For a "stuck sample", the Noise Source output is suppressed during the intermittent failure but is allowed to return to normal functioning. When a persistent failure of the Raw Data is detected, a "Hard Error State" is declared, so that the application cannot access the Entropy Source and the operator must reboot to attempt to correct the operation of the entropy source.

7. Maintenance

The Entropy Source does not require maintenance.

8. Required Testing

Validation testing was carried out on the Ultra IC Entropy Source in accordance with section 3 of SP 800-90B on data sets containing raw data samples, post non-vetted conditioning samples and restart samples. Users can verify operation by collecting data samples from the non-vetted conditioned output of the entropy source and testing with the NIST SP 800-90B test tool.