SP 800-90B Non-Proprietary Public Use Document

VaultIC408

Document Version 1.0

WISeKey Semiconductors
Arteparc de Bachasson, Bât A
13590 Meyreuil,
France

September 27, 2022

Revision History

Version	Change
1.0	First draft for VaultIC408

Table of Contents

Description

The Wisekey entropy source VaultIC408 is a hardware implemented, physical (P) entropy source consisting of several individual ring oscillators combined to produce a non-IID single bit raw data output, which is provided with no conditioning.

The entropy source was tested by collecting data from an instance of the entropy source operating in normal conditions.

Table 1. Evaluated Version

Identifier	Version
Part Number	AT90SO28RS
Hardware Revision	Rev A
Firmware Version	1.1.0

Security Boundary

The noise source is located within the security boundary described in "6d-VaultIC408 1.0.1 – Security Policy L3 V0.1.docx". The cryptographic module consists of a single chip embodiment that contains a single die, which contains, among other IPs, the oscillators composing the noise source. Therefore, the security boundary of the noise source coincides with the cryptographic boundary described in Figure 1.

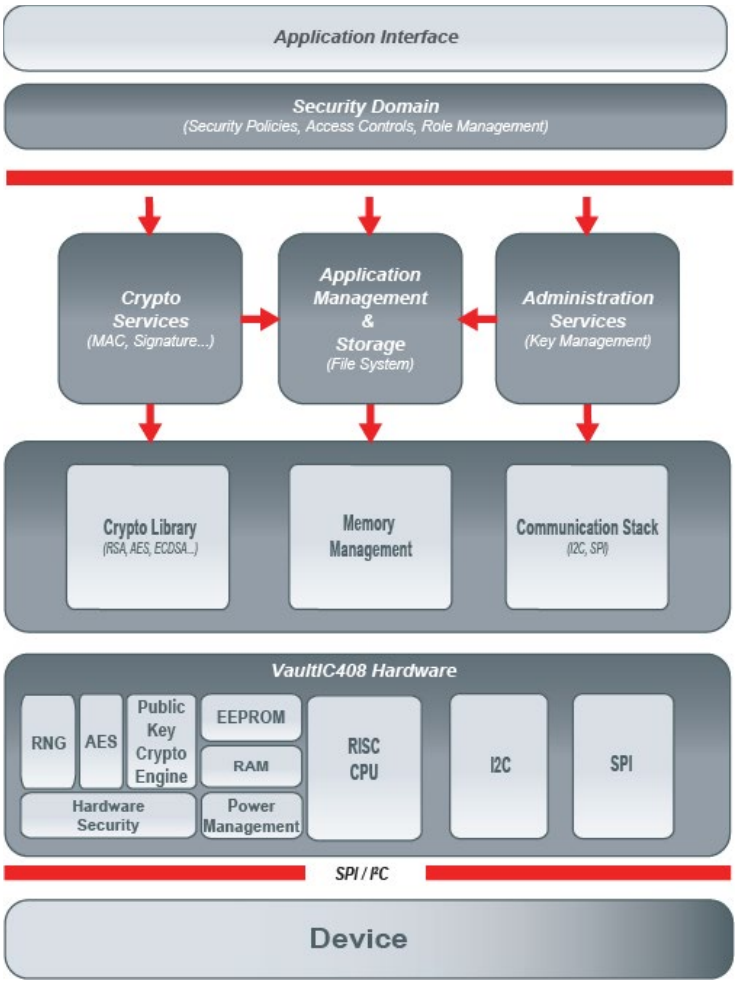

Figure 1. Cryptographic Boundaries

Operating Conditions

The entropy source was analyzed for the effects of differing voltage and temperature. Table 2 contains the operational conditions in which the entropy source will operate in and maintain entropy production at the assessed value.

Table 2. Entropy-Relevant Parameters

Configuration Parameter	Value	Description
Temperature	-40°Cto 105°C	Temperature has limited impact on the oscillator's frequency, which remains in the expected range, from -40°C to +105°C .
Voltage	1.6V -6V	Voltage has limited impact on the oscillator's frequency, which remains in the expected range, from 1.6V to 6V .
Clock speed	36MHz	Internal VFO frequency is fixed to 36 MHz.

Configuration Settings

There are no configuration settings available for noise source operation.

Physical Security Mechanisms

Voltage Monitor, Frequency Monitor, Temperature Monitor, Hardware protection, Glitch detector, Bus encryption, Light protection, Parity errors, Mirroring, CStack Checker

Conceptual Interfaces

In normal operation, the entropy source fills an internal buffer for continuous testing, available for the firmware. There are no conceptual interfaces giving direct access to the entropy source.

Min-Entropy Rate

The VaultIC408 entropy source provides 0.52427 bits of min entropy per bit of sample output. These samples are provided unconditioned to the consuming cryptographic module.

Health Tests

The VaultIC408 entropy source performs all required health tests of Section 4.4 of SP 800-90B. This includes startup, continuous, and on-demand tests. Health tests include the SP 800-90B approved continuous tests: Repetition Count Test (RCT) and Adaptive Proportion Test (APT). An additional developer defined test, the Ultra Low Frequency Monitor (ULFM), flags individual ring oscillators whose frequency drops or stops functioning. Health tests are set to flag errors with a false positive probability of 2^{-20}.

Maintenance

There are no specific maintenance requirements for the entropy source.

Required Testing

The VaultIC408 entropy source was tested by collected data from the device operating in its designated operational range and processed with the SP 800-90B tool. Test data was collected following the requirements of Section 3 of SP 800-90B. All tested data was evaluated at a higher entropy than the claimed entropy of the assessment, and all restart sanity checks passed.

No additional testing is required.