

Microsoft Corporation

Microsoft Data Processing Unit (DPU) Entropy Source Public Use Document

ESV Public Use Document

Prepared By	EWA-Canada
On behalf of	Microsoft Corporation One Microsoft Way Redmond, WA 98052-6399
Document Version	1.0
Updated On	May 17, 2026

COPYRIGHT AND DISCLAIMER

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2026 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, Azure, Visual Basic, Visual Studio, Windows, the Windows logo, Windows NT, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

© 2026 Microsoft Corporation.

Contents

1 Introduction 4
2 Security boundary 4
3 Operating Conditions 5
4 Configuration Settings 5
5 Physical Security Mechanisms 5
6 Conceptual Interfaces 5
7 Min-Entropy Rate 5
8 Health Tests 6
9 Maintenance 6
10 User Verification 6
11 Reuse 6

1 Introduction

This public use document describes the design of the Microsoft Data Processing Unit (DPU) Entropy Source (referred to as the "entropy source" in this document), a physical entropy source developed by Microsoft. This entropy source exploits ring oscillator timing jitter to generate random binary data. The entropy source itself consists of the hardware and firmware which, in combination, constitute the health tests, noise source, and conditioning component of the entropy source.

This entropy source was tested against the requirements prescribed within the 10 Jan 2018 publication of SP 800-90B and the 16 Apr 2026 publication of the FIPS 140-3 Implementation Guidance.[1]

Table 1 below contains the tested operating environments which contain implementations of the entropy source.

Table 1: Tested Operating Environments

E-OE Name	Device	Firmware Version	CAVP
Microsoft DPU-SBP-F2 rev A0	DPU SBP	25130-f2-fips	A8255

2 Security boundary

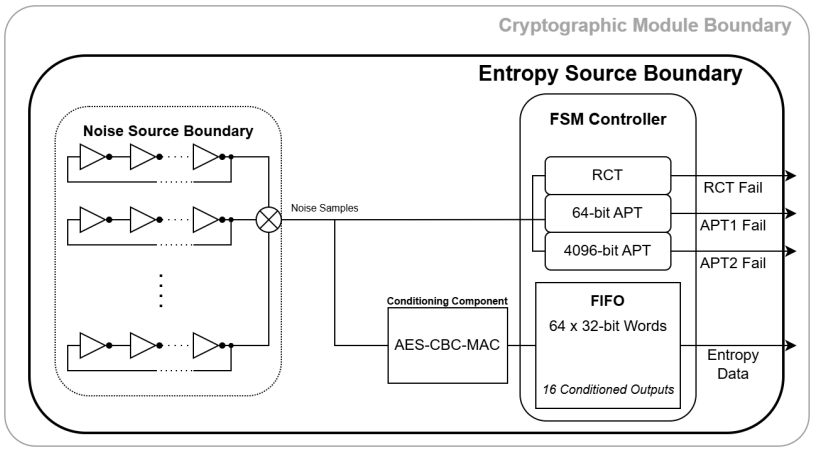


Figure 1: Block Diagram Of Microsoft Data Processing Unit (DPU) Entropy Source

The entropy source is intended to be implemented within the cryptographic boundary of a cryptographic module; as such, both the firmware and hardware components should be considered part of the cryptographic module.

[1] With the 05 Nov 2021 update of IG D.J and the 16 Apr 2026 update of IG D.K.

3 Operating Conditions

The entropy source is capable of operating under the following conditions for each E-OE:

E-OE Name	Temperature (C)		Voltage (V)	
	Low	High	Low	High
Microsoft DPU-SBP-F2 rev A0	-10	+100	0.65	0.825

4 Configuration Settings

The entropy source does not have configuration parameters accessible to the user. All configuration parameters are tied and built into the firmware.

5 Physical Security Mechanisms

The entropy source is assumed to be implemented within a cryptographic module's cryptographic boundary. As such, the entropy source will inherit the physical protections of the cryptographic module.

6 Conceptual Interfaces

NIST defines three conceptual interfaces within SP 800-90B:

GetNoise An interface with which the consumer of the entropy source can get material from the noise source, without conditioning.

GetEntropy An interface with which the consumer of the entropy source can get entropy material from the entropy source.

HealthTest An interface with which the entropy source communicates information about the health of the noise source.

Table 3 below lists how the consumer of the entropy source can access these interfaces, and a description of the response format.

Table 3: Entropy Source Interfaces

Interface	Access	Response Format
GetNoise	*Not provided*	
GetEntropy	`Get_Entropy(int Num_Bytes)`	Returns `Num_Bytes` bytes of entropy material.
HealthTest	via Interrupt and Status Registers	Upon failure, a non-maskable interrupt triggers and the entropy source is disabled.

7 Min-Entropy Rate

The entropy source provides 128 bits of entropy per 128-bit block (i.e., provides full entropy).

8 Health Tests

The SP 800-90B-defined Repetition Count Test (RCT) in addition to a 4096-sample and a 64-sample window Adaptive Proportion Test are used to ensure the entropy source's behavior at start-up and during continuous use.

Upon a failure, the entropy source will write the failure information to a status register and trigger a non-maskable interrupt to the host processor. The processor may restart the entropy source to reinitiate health testing and attempt to use the entropy source again.

9 Maintenance

There are no maintenance requirements for this entropy source.

10 User Verification

To ensure proper instantiation of this entropy source in a cryptographic module, the tester shall verify that the hardware revision, installed firmware version, and configuration settings match those described in this document.

11 Reuse

Reuse of this entropy source in another certificate submission by an organization other than Microsoft requires explicit written permission from Microsoft.