



## **DPU BMC SPDM Attestation via Redfish**

# Table of contents

## Redfish Commands

---

Get Measurements Response Data

---

Get ComponentIntegrity Collection

---

Get Certificate Chain of Specific Attestation Target

---

Handling the Response

---

Monitoring Task Progress

---

Get Measurements from Attestation Target

---

## Redfish Event Log

---

The DPU BMC attestation process enables secure verification of device identity and firmware integrity using standardized protocols. This implementation leverages SPDm (Security Protocol and Data Models) over MCTP (Management Component Transport Protocol) to provide remote attestation capabilities via the Redfish API.

## Redfish Commands

### Note

For detailed information about the DPU attestation process, measurement descriptions, and reference values, refer to the [DPU Attestation](#) documentation.

## Get Component Integrity Collection

```
curl -k -u root:<password> -H "Content-Type: application/json" -X GET  
https://<bmc ip>/redfish/v1/ComponentIntegrity
```

This command returns a collection of all attestation targets in the system.

In DPU BMC, the available attestation targets are:

- `Bluefield_DPU_IROt` – The BlueField IROt (Initial Root of Trust), a Platform Security Controller (PSC) that stores measurements related to the Arm and NIC components
- `Bluefield_ERoT` – The BlueField BMC ERoT (External Root of Trust), which contains measurements related to the DPU BMC

## Get Certificate Chain of Specific Attestation Target

```
curl -k -u root:'<password>' -H "Content-Type: application/json" -X GET
https://<bmc ip>/redfish/v1/Chassis/<target-id>/Certificates/CertChain
```

This command retrieves the certificate chain for a specific attestation target. The response is a JSON structure containing the entire certificate chain, which can be used to verify the authenticity of the component.

## Get Measurements from Attestation Target

```
# 1. Request all available measurements
```

```
curl -k -u root:'<password>' -H "Content-Type: application/json" -X POST \
  https://<bmc ip>/redfish/v1/ComponentIntegrity/<target
id>/Actions/ComponentIntegrity.SPDMGetSignedMeasurements
```

```
# 2. Request specific measurements
```

```
curl -k -u root:'<password>' -H "Content-Type: application/json" -X POST \
  -d '{"SlotId": 0, "MeasurementIndices": [2,5], "Nonce":
"d42a0594c5cd5743ee08fe5ec3cf884b1fac4f106879cda98b7d1c51652b04b7"}' \
  https://<bmc
ip>/redfish/v1/ComponentIntegrity/HGX_IoT_NIC_0/Actions/ComponentIntegrity.SPDMGetSignedMeasurements
```

This command retrieves signed measurements from the specified component.

### Parameters:

#### 1. Nonce

- Description: A unique, randomly generated value used to prevent replay attacks.
- Format: 32-byte (64-character) hexadecimal string.
- Usage:

- Must be generated and provided by the client for each request.
- Ensures that each request is fresh and secure.

## 2. Certificate Slot ID

- Description: Indicates which slot contains the certificate chain used for signing.
- Supported Value: 0
- Default: 0
- Note: Only Slot 0 is supported, which holds the NVIDIA certificate chain.

## 3. Measurement Indices

- Description: Specifies the measurement indices to request.
- Format: Array of integers.
- Default: If omitted, 0xFF is used to request all available measurements.

## Handling the Response

This operation is asynchronous and returns a task object rather than the measurement data itself.

Example response:

```
{
  "@odata.id": "/redfish/v1/TaskService/Tasks/0",
  "@odata.type": "#Task.v1_4_3.Task",
  "Id": "<id>",
  "TaskState": "Running",
  "TaskStatus": "OK"
}
```

## Monitoring Task Progress

Periodically check the task until completion using:

```
curl -k -u root:'<password>' -H "Content-Type: application/json" \
-X GET https://<bmc ip>/redfish/v1/TaskService/Tasks/<id>
```

A completed task appears as

```
{
  ...
  "PercentComplete" : 100,
  ...
  "TaskState" : "Completed",
  "TaskStatus" : "OK"
}
```

## Get Measurements Response Data

```
curl -k -u root:'<password>' -H "Content-Type: application/json" -X GET \
https://<bmc ip>/redfish/v1/ComponentIntegrity/<target
id>/Actions/ComponentIntegrity.SPDMGetSignedMeasurements/data
```

This command retrieves the signed measurement data previously requested via the `SPDMGetSignedMeasurements` action.

Example output:

```
{
  "HashingAlgorithm": "TPM_ALG_SHA_512",
  "SignedMeasurements": "<base64 encoded measurements>",
  "SigningAlgorithm": "TPM_ALG_ECDSA_ECC_NIST_P384",
  "Version": "1.1.0"
}
```

## Redfish Event Log

Each time a new *Get Measurements* command is issued, a Redfish event log entry is generated.

Example entry:

```
{
  "@odata.id": "/redfish/v1/Systems/Bluefield/LogServices/EventLog/Entries/<id>",
  "@odata.type": "#LogEntry.v1_15_0.LogEntry",
  "Created": "<date>",
  "EntryType": "Event",
  "Id": "<id>",
  "Message": "Redfish attestation measurements POST request received",
  "Modified": "<date>",
  "Name": "System Event Log Entry",
  "Resolved": false,
  "Severity": "OK"
}
```

## Notice

This document is provided for information purposes only and shall not be regarded as a warranty of a certain functionality, condition, or quality of a product. NVIDIA Corporation ("NVIDIA") makes no representations or warranties, expressed or implied, as to the accuracy or completeness of the information contained in this document and assumes no responsibility for any errors contained herein. NVIDIA shall have no liability for the consequences or use of such information or for any infringement of patents or other rights of third parties that may result from its use. This document is not a commitment to develop, release, or deliver any Material (defined below), code, or functionality.

NVIDIA reserves the right to make corrections, modifications, enhancements, improvements, and any other changes to this document, at any time without notice.

Customer should obtain the latest relevant information before placing orders and should verify that such information is current and complete.

NVIDIA products are sold subject to the NVIDIA standard terms and conditions of sale supplied at the time of order acknowledgement, unless otherwise agreed in an individual sales agreement signed by authorized representatives of NVIDIA and customer ("Terms of Sale"). NVIDIA hereby expressly objects to applying any customer general terms and conditions with regards to the purchase of the NVIDIA product referenced in this document. No contractual obligations are formed either directly or indirectly by this document.

NVIDIA products are not designed, authorized, or warranted to be suitable for use in medical, military, aircraft, space, or life support equipment, nor in applications where failure or malfunction of the NVIDIA product can reasonably be expected to result in personal injury, death, or property or environmental damage. NVIDIA accepts no liability for inclusion and/or use of NVIDIA products in such equipment or applications and therefore such inclusion and/or use is at customer's own risk.

NVIDIA makes no representation or warranty that products based on this document will be suitable for any specified use. Testing of all parameters of each product is not necessarily performed by NVIDIA. It is customer's sole responsibility to evaluate and determine the applicability of any information contained in this document, ensure the product is suitable and fit for the application planned by customer, and perform the necessary testing for the application in order to avoid a default of the application or the product. Weaknesses in customer's product designs may affect the quality and reliability of the NVIDIA product and may result in additional or different conditions and/or requirements beyond those contained in this document. NVIDIA accepts no liability related to any default, damage, costs, or problem which may be based on or attributable to: (i) the use of the NVIDIA product in any manner that is contrary to this document or (ii) customer product designs.

No license, either expressed or implied, is granted under any NVIDIA patent right, copyright, or other NVIDIA intellectual property right under this document. Information published by NVIDIA regarding third-party products or services does not constitute a license from NVIDIA to use such products or services or a warranty or endorsement thereof. Use of such information may require a license from a third party under the patents or other intellectual property rights of the third party, or a license from NVIDIA under the patents or other intellectual property rights of NVIDIA.

Reproduction of information in this document is permissible only if approved in advance by NVIDIA in writing, reproduced without alteration and in full compliance with all applicable export laws and regulations, and accompanied by all associated conditions, limitations, and notices.

THIS DOCUMENT AND ALL NVIDIA DESIGN SPECIFICATIONS, REFERENCE BOARDS, FILES, DRAWINGS, DIAGNOSTICS, LISTS, AND OTHER DOCUMENTS (TOGETHER AND SEPARATELY, "MATERIALS") ARE BEING PROVIDED "AS IS." NVIDIA MAKES NO WARRANTIES, EXPRESSED, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE MATERIALS, AND EXPRESSLY DISCLAIMS ALL IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL NVIDIA BE LIABLE FOR ANY DAMAGES, INCLUDING WITHOUT LIMITATION ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF

ANY USE OF THIS DOCUMENT, EVEN IF NVIDIA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Notwithstanding any damages that customer might incur for any reason whatsoever, NVIDIA's aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms of Sale for the product.

## **Trademarks**

NVIDIA and the NVIDIA logo are trademarks and/or registered trademarks of NVIDIA Corporation in the U.S. and other countries. Other company and product names may be trademarks of the respective companies with which they are associated.

© Copyright 2026, NVIDIA. PDF Generated on 02/28/2026