



Document Identifier: DSP0270

Date: 2016-12-07

Version: 1.0.0a

Redfish Host Interface Specification

Information for Work-in-Progress version:

IMPORTANT: This document is not a standard. It does not necessarily reflect the views of the DMTF or its members. Because this document is a Work in Progress, this document may still change, perhaps profoundly and without notice. This document is available for public review and comment until superseded.

Provide any comments through the DMTF Feedback Portal: <http://www.dmtf.org/standards/feedback>

Document Class: Normative

Document Status: Work in Progress

Document Language: en-US

Copyright Notice

Copyright © 2014-2016 Distributed Management Task Force, Inc. (DMTF). All rights reserved.

DMTF is a not-for-profit association of industry members dedicated to promoting enterprise and systems management and interoperability. Members and non-members may reproduce DMTF specifications and documents, provided that correct attribution is given. As DMTF specifications may be revised from time to time, the particular version and release date should always be noted.

Implementation of certain elements of this standard or proposed standard may be subject to third party patent rights, including provisional patent rights (herein "patent rights"). DMTF makes no representations to users of the standard as to the existence of such rights, and is not responsible to recognize, disclose, or identify any or all such third party patent right, owners or claimants, nor for any incomplete or inaccurate identification or disclosure of such rights, owners or claimants. DMTF shall have no liability to any party, in any manner or circumstance, under any legal theory whatsoever, for failure to recognize, disclose, or identify any such third party patent rights, or for such party's reliance on the standard or incorporation thereof in its product, protocols or testing procedures. DMTF shall have no liability to any party implementing such standard, whether such implementation is foreseeable or not, nor to any patent owner or claimant, and shall have no liability or responsibility for costs or losses incurred if a standard is withdrawn or modified after publication, and shall be indemnified and held harmless by any party implementing the standard from any and all claims of infringement by a patent owner for such implementations.

For information about patents held by third-parties which have notified the DMTF that, in their opinion, such patent may relate to or impact implementations of DMTF standards, visit <http://www.dmtf.org/about/policies/disclosures.php>.

This document's normative language is English. Translation into other languages is permitted.

CONTENTS

1. Abstract 6

2. Normative references 6

3. Terms and definitions 6

4. Symbols and abbreviated terms 7

5. Introduction..... 8

6. Scope 9

 6.1. Goals..... 9

7. Protocol details 9

 7.1. Network Host Interface Protocol Details 10

8. SMBIOS Support 11

 8.1. SMBIOS Type 42 Struct General Layout 11

 8.2. Table-1: SMBIOS Type 42 Struct Definition for Redfish Host Interfaces 12

 8.3. Table-2: Interface Specific Data (for Interface Type 40h)..... 12

 8.4. Table-3: Device Descriptor Data 13

 8.5. Table-4: Protocol Records Data format: 13

 8.6. Table-5: "Redfish Over IP" Protocol-specific Record Data 14

9. Delivery of Kernel Authentication Information via UEFI Runtime Variables 15

 9.1. Credential Generation and Management for Use by Firmware and OS kernel 16

 9.2. Security Considerations for Protecting Auto-generated Credentials 16

 9.3. UEFI Implementation 17

 9.3.1. Prototype 17

 9.3.2. Related Definitions 17

 9.3.3. Description..... 17

 9.3.4. Variable Format 18

10. ANNEX A (informative)..... 19

 10.1. Change log..... 19

Foreword

The Redfish Host Interface Specification was prepared by the Scalable Platforms Management Forum of the DMTF.

DMTF is a not-for-profit association of industry members dedicated to promoting enterprise and systems management and interoperability. For information about the DMTF, see <http://www.dmtf.org>.

Acknowledgments

The DMTF acknowledges the following individuals for their contributions to this document:

- Jeff Autor - Hewlett Packard Enterprise
- Jeff Bobzin - Insyde Software Corp
- Patrick Caporale - Lenovo
- Phil Chidester – Dell Inc.
- Chris Davenport - Hewlett Packard Enterprise
- Samer El-Haj-Mahmoud - Lenovo
- Jeff Hilland - Hewlett Packard Enterprise
- John Leung - Intel Corporation
- Edward Newman - Hewlett Packard Enterprise
- Michael Raineri - Dell Inc.
- Hemal Shah - Broadcom Limited
- Paul Vancil - Dell Inc.

1. Abstract

This specification defines functional requirements for Redfish Host Interfaces. In the context of this document, the term "host interface" refers to interfaces that can be used by software running on a computer system to access the Redfish Service that is used to manage that computer system.

The target audience for this specification is system manufacturers that are providing Redfish Host Interfaces within computer systems, system and component manufactures that are providing devices or firmware that include or support Redfish Host interfaces, and system firmware and software writers that are creating software or firmware that uses Redfish Host Interfaces .

2. Normative references

The following referenced documents are indispensable for the application of this document. For dated or versioned references, only the edition cited (including any corrigenda or DMTF update versions) applies. For references without a date or version, the latest published edition of the referenced document (including any corrigenda or DMTF update versions) applies.

- [DMTF DSP0134](http://www.dmtf.org/sites/default/files/standards/documents/DSP0134_3.0.pdf) System Management BIOS Reference Specification (SMBIOS), http://www.dmtf.org/sites/default/files/standards/documents/DSP0134_3.0.pdf
- [UEFI](http://www.uefi.org/sites/default/files/resources/UEFI_Spec_2_6.pdf) Unified Extensible Firmware Interface Specification (UEFI), Version 2.6, http://www.uefi.org/sites/default/files/resources/UEFI_Spec_2_6.pdf
- [DMTF DSP0239](http://www.dmtf.org/sites/default/files/standards/documents/DSP0239_1.4.pdf) Management Component Transport Protocol (MCTP) IDs and Codes, Version 1.4, http://www.dmtf.org/sites/default/files/standards/documents/DSP0239_1.4.pdf
- [DMTF DSP0266](http://www.dmtf.org/sites/default/files/standards/documents/DSP0266_1.0.pdf) Redfish Scalable Platforms Management API Specification, http://www.dmtf.org/sites/default/files/standards/documents/DSP0266_1.0.pdf
- [ISO/IEC Directives, Part 2](http://isotc.iso.org/livelink/livelink.exe?func=ll&objId=4230456&objAction=browse&sort=subtype) Rules for the structure and drafting of International Standards, <http://isotc.iso.org/livelink/livelink.exe?func=ll&objId=4230456&objAction=browse&sort=subtype>

3. Terms and definitions

In this document, some terms have a specific meaning beyond the normal English meaning. Those terms are defined in this clause.

The terms "shall" ("required"), "shall not", "should" ("recommended"), "should not" ("not recommended"), "may", "need not" ("not required"), "can" and "cannot" in this document are to be interpreted as described in ISO/IEC Directives, Part 2, Annex H. The terms in parenthesis are alternatives for the preceding term, for use in exceptional cases when the preceding term cannot be used for linguistic reasons. Note that ISO/IEC Directives, Part 2, Annex H specifies additional alternatives. Occurrences of such additional alternatives shall be interpreted in their normal English meaning.

The terms "clause", "subclause", "paragraph", and "annex" in this document are to be interpreted as described in ISO/IEC Directives, Part 2, Clause 5.

The terms "normative" and "informative" in this document are to be interpreted as described in ISO/IEC Directives, Part 2, Clause 3. In this document, clauses, subclauses, or annexes labeled "(informative)" do not contain normative content. Notes and examples are always informative elements.

The following additional terms are used in this document.

Term	Definition
Host	The Computer System that is managed by a Redfish Service
Host Software	Software running on the Host Computer System, including Operating System and it's Software components (such as drivers or applications), as well as pre-boot software such as UEFI or BIOS drivers and applications.
Redfish Service	Also referred to as the "Service". The collection of functionality that implements the protocols, resources, and functions that deliver the interface defined by the Redfish API specification and its associated behaviors for one or more managed systems.
Redfish Service Entry Point	Also referred to as "Service Entry Point". The interface through which a particular instance of a Redfish Service is accessed. A Redfish Service may have more than one Service Entry Point.
Redfish Manager	Also referred to as "Manager". The entity that manages a Computer System and other peripherals through a Redfish Service.

4. Symbols and abbreviated terms

The following additional abbreviations are used in this document.

Term	Definition
BIOS	Basic I/O System. Name for system firmware typically used for initialization and launching the boot of an ISA (Industry Standard Architecture), aka 'x86' or 'PC', architecture-based computer system.
BSP	Board Support Package. Name for system firmware typically used for initialization and launching the boot of Linux in a computer system that uses a non-ISA architecture, but may be used for booting other types of operating systems or run-time software.

Term	Definition
SMBIOS	System Management BIOS. Refers to DSP0134. Defines memory mapped tables, typically implemented by system firmware/BIOS and mapped into system firmware/BIOS memory space, that provide inventory and management information for the computer system.
UEFI	Unified Extensible Firmware Interface. A modern firmware standard that defines the interfaces between hardware and Operating Systems in a Computer System. UEFI is supported on multiple processor architectures, including x86, x64, ia64, and AARCH64.
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over TLS
IP	Internet Protocol
IPMI	Intelligent Platform Management Interface
NIC	Network Interface Card
PCI	Peripheral Component Interconnect
PCIe	PCI Express
TCP	Transmission Control Protocol
UUID	Universally Unique Identifier

5. Introduction

Redfish is a flexible system management tool that can be successfully applied to various system architectures. One important architecture consists of one or more CPUs assigned to the system application (The Host CPUs) and a separate CPU or CPUs assigned solely to management including publishing the Redfish interface. In many management schemes it is necessary to provide standardized Redfish-based communication between the Host CPU and the Redfish service in the Management unit. This communication is in addition to the Redfish services available via the external network. Implementation of the Redfish Host Interface is optional for the system designer. If provided, this interface may be used in both the pre-boot (firmware) stage and by drivers and applications within the Host Operating system and is designed to be available without use of external networking. This specification provides design details for several methods of Host-to-Manager communication. Additional methods may be added in future revisions of this specification.

6. Scope

This specification is targeted to system manufacturers that are providing Redfish Host Interfaces within computer systems, system and component manufactures that are providing devices or firmware that include or support Redfish Host interfaces, and system firmware and software writers that are creating software or firmware that uses Redfish Host Interfaces.

The specification covers host accessible physical and logical communication paths and protocols that are used to access the Redfish Service that manages that host.

The specification also defines certain supporting elements in the host, such as SMBIOS extensions, that enable inventory and discovery functions.

The specification does not seek to place specific hardware implementation requirements; however, it does in some cases specify how hardware-specific interfaces are identified for host software (e.g. SMBIOS structures).

The specification defines connectivity between a Redfish Service and a host. Any network routing or other connectivity beyond the Redfish Service or other networks is out of scope.

6.1. Goals

The following are the goals for the Redfish Host Interface:

- Implementable with existing management controller technology
- Easily integrated into products
- Host Interface and out-of-band API must be the same (where possible) so that client apps have minimal (if any) change to adapt
- Support authentication, confidentiality, and integrity:
 - Support environments where users do not want to solely rely on host/OS access control mechanisms
 - Provide mechanism to optionally (if configured) pass credentials to an OS Kernel for sensor monitoring (with configurable privilege)
- Support multi-manager to multi-host architectures:
 - Blade system with Chassis Manager as well as sled management controller on each blade, each with a host interface
- Support security requirements with authentication and confidentiality.

7. Protocol details

A Redfish Host Interface shall support one of the following protocols:

- Network HI -- Redfish HTTP requests/responses over a TCP/IP network connection between a Host and Manager

7.1. Network Host Interface Protocol Details

Implementations that support the "Network Host Interface" protocol shall implement the following requirements:

- Implementations shall provide a TCP/IP network connection that route TCP/IP traffic between a Redfish client executing on the host and the Manager.
- Any link-level driver and interconnect that implements a TCP/IP network connection between the host and manager may be used. Example implementations include:
 - A USB Network Connection between host and manager
 - A host PCIe NIC that connects to a manager NIC
 - A host PCIe NIC that connects to a management LAN that connects to a manager
- Authentication, and privilege authorization equivalent to the out-of-band Redfish API as specified in DSP0266 shall be supported by the implementation when enabled from the manager configuration.
 - Authentication credentials that are valid on the normal out-of-band Redfish network interface shall also be valid on the HI.
 - Implementations may optionally support a configurable AuthNone authentication mode (no authentication required) that can be configured on the manager for use on Host Interface. If implemented, enablement of AuthNone shall be configurable, and the RoleId assumed by AuthNone requests shall be configurable as described by the Redfish schema.
 - In addition to standard credentials, implementations may optionally support auto-generation and delivery of HI-only credentials that may be used by the Firmware or OS to authenticate.
 - If supported, auto-generated host credentials shall be delivered using UEFI-based mechanism described in a later section of this document.
 - The permissions granted to any auto-generated credentials shall be configurable with a defined RoleId assigned.
- Services shall require HTTPS encryption for the Network Host Interface with same requirements as via out-of-band network interfaces:
 - Session Login POSTs shall use HTTPS
 - Patches that contain sensitive data shall use HTTPS
 - Basic Auth requests shall require HTTPS

- Implementations that support SMBIOS shall provide an SMBIOS Type 42 structure that describes each host interface as defined by the [SMBIOS](#) standard and the [SMBIOS Support](#) clause of this document.
- Implementations that support automatically generating and sending credentials to the host OS kernel and/or firmware using UEFI runtime variables shall be implemented as defined within the [Kernel Authentication](#) clause of this document..
 - If the Kernel Authentication Interface is implemented, the Redfish services shall implement a configuration option that allows customers to disable the Kernel Authentication as described by the Redfish schema.
 - If the Kernel Authentication Interface is implemented, the Redfish service shall implement a configurable role for the Kernel Authentication Interface as described by the Redfish schema.

8. SMBIOS Support

Information in the SMBIOS structure shall allow host software to discover the Redfish Service Entry Point supported and to initialize the host-side driver stack.

For Network Host interfaces, the mechanism that clients should use to discover/obtain the Redfish Service Entry Point IP address shall also be described in the structure.

8.1. SMBIOS Type 42 Struct General Layout

```

-----
Type 42 Header
-----
Interface Specific Data
- Device Description
- (1 of 3 types)
-----
Protocol Record Header
-----
- Protocol Specific Data
-----

```

8.2. Table-1: SMBIOS Type 42 Struct Definition for Redfish Host Interfaces

The following describes the SMBIOS Management Controller Host Interface (Type 42) structure. Offset 00h-04h is the Type 42 Header. Starting at Offset 05h is the Interface-specific Data.

Offset	Name	Length	Value	Description
00h	Type	BYTE	42	Management Controller Host Interface structure indicator
01h	Length	BYTE	Varies	Length of the structure, a minimum of 09h
02h	Handle	WORD	Varies	
04h	Interface Type	BYTE	Varies	Management Controller Interface Type. --Network Host Interface = 40h
05h	Interface Specific Data Length (n)	BYTE	Varies	Interface-specific Data as specified by the Interface type. if 0, there is no Interface specific data
06h	Interface Specific data	n BYTES	Varies	Defined by Interface Type. See Table-2 below.
06h+n	Protocol count	BYTE	Varies	number of protocols defined for the host interface (typically 1)
07h+n	Protocol Records	m Bytes	Varies	Include a Protocol Record for each protocol supported. See Table-4 below record format

8.3. Table-2: Interface Specific Data (for Interface Type 40h)

Interface Specific Data starts at offset 06h of the SMBIOS Type 42 struct. This table defines the Interface Specific data for Interface Type 40h. There are 3 types of Device Descriptor3 defined (see Table-3), however only 1 may be used in specific Tape 42 table.

Offset	Name	Length	Value	Description
X	Device Type	BYTE	Enum	USB Network Interface=02h, PCI/PCIe Network Interface=03h, OEM=80h-FFh other values reserved

Offset	Name	Length	Value	Description
X+1	Device Descriptors	n-1 Bytes	Varies	Device descriptor data formatted based on Device Type. See Table-3

8.4. Table-3: Device Descriptor Data

The following table defines the specific Device Descriptor data (referenced in Table-2) for each defined Device Type:

Device Type enum value	Device Type Name	Length	Value	Description
02h	USB Network Interface	Varies	Varies	Device Descriptors for USB Device Type: -idVendor(2-bytes), -idProduct(2-bytes), -iSerialNumber: --- bLength(1-Byte), --- bDescriptorType(1-Byte), --- bString(Varies))
03h	PCI/PCIe Network Interface	8-Bytes	Varies	Device Descriptors for PCI/PCIe Device Type: -VendorID(2-Bytes), -DeviceID(2-Bytes), - Subsystem_Vendor_ID(2-bytes), -Subsystem_ID(2-bytes)
80h-FFh	OEM	Varies	Varies	Device Descriptors for OEM Device Type: -vendor_IANA(4-bytes), -OEM defined data

8.5. Table-4: Protocol Records Data format:

The following table defines the general Protocol Record layout specific data for Redfish Over IP protocol follows:

Offset	Name	Length	Value	Description
X	Protocol Identifier	BYTE	Varies	The protocol identifier --"Redfish over IP" = 04h
X+1	Length	BYTE	varies	length of protocol specific data for Redfish Over IP protocol
X+2	Protocol specific record data	p Bytes	Varies	Defined by protocol. See Table-5 below for "Redfish over IP" protocol

8.6. Table-5: "Redfish Over IP" Protocol-specific Record Data

The following table defines the protocol-specific data for the "Redfish Over IP" protocol:

Offset	Name	Length	Value	Description
X+0	Service UUID	16BYTES	Varies	same as Redfish Service UUID in Redfish Service Root resource
X+16	Host IP Assignment Type	BYTE	Enum	Unknown=00h, Static=01h, DHCP=02h, AutoConfigure=03h, HostSelected=04h, other values reserved
X+17	Host IP Address Format	BYTE	Enum	Unknown=00h, Ipv4=01h, Ipv6=02h, other values reserved
X+18	Host IP Address	16BYTE	Varies	Used for Static and AutoConfigure. For IPV4, use the first 4 Bytes and zero fill the remaining bytes.
X+34	Host IP Mask	16BYTE	Varies	Used for Static and AutoConfigure. For IPV4, use the first 4 Bytes and zero fill the remaining bytes.
X+50	Redfish Service IP Discovery Type	BYTE	Enum	Unknown=00h, Static=01h, DHCP=02h,

Offset	Name	Length	Value	Description
				AutoConfigure=03h, HostSelected=04h, other values reserved
X+51	Redfish Service IP Address Format	BYTE	Enum	Unknown=00h, Ipv4=01h, Ipv6=02h, other values reserved
X+52	Redfish Service IP Address	16BYTE	Varies	Used for Static and AutoConfigure. For IPV4, use the first 4 Bytes and zero fill the remaining bytes.
X+68	Redfish Service IP Mask	16BYTE	Varies	Used for Static and AutoConfigure. For IPV4, use the first 4 Bytes and zero fill the remaining bytes.
X+84	Redfish Service IP Port	WORD	Varies	Used for Static and AutoConfigure.
X+86	Redfish Service VLAN ID	DWORD	Varies	Used for Static and AutoConfigure.
X+90	Redfish Service Hostname Length	BYTE	Varies	length of the following hostname string
X+91	Redfish Service Hostname	varies	Varies	hostname of Redfish Service

9. Delivery of Kernel Authentication Information via UEFI Runtime Variables

This section defines an optional mechanism for automatically generating and sending credentials to the host OS kernel and/or firmware using UEFI runtime variables. Services that implement the kernel authentication mechanism shall comply with the following sub-sections:

9.1. Credential Generation and Management for Use by Firmware and OS kernel

Opening a Redfish session on the Host Interface may be accomplished by use of any authorized Redfish credentials consisting of valid username and password. However in some situations it may be difficult to pre-provision the system with valid Redfish credentials for use by OS and Firmware clients of Redfish. Examples of this include (a) early provisioning of new systems and (b) systems where firmware does not have secure storage to hide the credentials.

To provide for situations of this type, systems supporting the Redfish service may optionally be configured to provide temporary logon credentials for use by Firmware Pre-boot elements and/or OS. If implemented, the credentials shall be implemented following the following requirements:

- The credentials shall be auto-generated by the Redfish Service and provided to firmware and OS using the UEFI variable interface variables described herein at the initiation of each system boot.
- The generation of both Firmware and OS credentials shall be user-configurable with the option to disable or enable generation of the credentials separately for both Firmware and OS kernel.
- The permissions of the resulting session shall be configurable through Manager configuration as described by the Redfish schema.
- The supplied credentials shall be in the form of a user id and password -- both auto-generated by the Redfish Service.
- Only one session using these auto-generated credentials shall be allowed at a time.
- The session associated with the auto-generated credentials shall not timeout or expire.
- The Redfish service may close the session if it resets or for other policy reasons in which case the host may re-open the session using the same credentials.
- Any open session started with firmware credentials shall be closed and the credentials invalidated at UEFI `ExitBootServices()` event.
- Any open session started with OS credentials shall be closed and new credential passwords generated when host restart is detected by manager.
- The Firmware Credentials shall be made available for any agent or driver that operates within the UEFI pre-boot prior to `ExitBootServices()` call. This may include local system ROM firmware or utility firmware applications downloaded from external sources.

9.2. Security Considerations for Protecting Auto-generated Credentials

It is recommended that system designers protect the credentials from unauthorized access. The use of UEFI Secure Boot to protect access to credentials is recommended. Because of the difficulty of defining a security procedure for Legacy-booting OS, delivery of credentials to Legacy OS is not described by this specification and any Legacy OS support for this feature is OEM specific.

The system OS is provided with a method of disabling further retrieval of the credentials after initial authorized retrieval. System designers are encouraged to implement such a scheme of retrieve, store, and disable to avoid unauthorized reading of the credential variables

9.3. UEFI Implementation

Implementations that present host interface for use by system firmware and OS shall use the UEFI Variables defined in this section to deliver credentials for the host interface.

The design of this delivery mechanism is compatible with any UEFI version starting with 2.3.1. Please refer to the specifications available at www.uefi.org for details on using the UEFI variable calls described here

9.3.1. Prototype

```
#define EFI_REDFISH_INFORMATION_GUID \
    {0x16faa37e, 0x4b6a, 0x4891, {0x90, 0x28, 0x24, 0x2d, 0xe6, 0x5a, 0x3b, 0x70 }}
#define EFI_REDFISH_INFORMATION_INDICATIONS    L"RedfishIndications"
#define EFI_REDFISH_INFORMATION_FW_CREDENTIALS    L"RedfishFWCredentials"
#define EFI_REDFISH_INFORMATION_OS_CREDENTIALS    L"RedfishOSCredentials"
```

9.3.2. Related Definitions

```
#define EFI_REDFISH_INDICATIONS_FW_CREDENTIALS    0x00000001
#define EFI_REDFISH_INDICATIONS_OS_CREDENTIALS    0x00000002
```

9.3.3. Description

This GUID and these variable names are used when calling the UEFI Runtime Service `GetVariable()`. See UEFI specification for details on use of this interface. As described below, the `SetVariable()` interface can be used to disable further access to the credential information.

The variables defined in this section have the following attributes:

- `EFI_REDFISH_INFORMATION_INDICATIONS` and `EFI_REDFISH_INFORMATION_OS_CREDENTIALS` have attributes `EFI_VARIABLE_BOOTSERVICE_ACCESS` and `EFI_VARIABLE_RUNTIME_ACCESS`.
- `EFI_REDFISH_INFORMATION_FW_CREDENTIALS` has attribute `EFI_VARIABLE_BOOTSERVICE_ACCESS`

The variable `EFI_REDFISH_INFORMATION_INDICATIONS` shall return a 32-bit value, and provides information if any credentials are provided for host software use. The bits defined with this variable shall be interpreted as follows:

- If `EFI_REDFISH_INDICATIONS_FW_CREDENTIALS` bit is 1, the Redfish host interface is configured to provide credentials for use by system firmware.
- If `EFI_REDFISH_INDICATIONS_OS_CREDENTIALS` bit is 1, the Redfish host interface is configured to provide a credentials for use by system OS.
- All other bits in `EFI_REDFISH_INDICATIONS_HOST_IF` are reserved.

When the Redfish implementation provides credentials for firmware use, the variable `EFI_REDFISH_INFORMATION_FW_CREDENTIALS` shall contain a UTF-8 character array formatted as described in the next section. If this session is not available as defined by current system policy, this variable shall return `EFI_NOT_FOUND`.

When the Redfish implementation provides a credentials for OS use, the variable `EFI_REDFISH_INFORMATION_OS_CREDENTIALS` a UTF-8 character array formatted as described in the next section. If these credentials are not available as defined by current system policy, this variable shall return `EFI_NOT_FOUND`.

The password contained in these variables shall be recalculated so as to be unique and not easily predicted on each boot.

If the variables `EFI_REDFISH_INFORMATION_FW_CREDENTIALS` or `EFI_REDFISH_INFORMATION_OS_CREDENTIALS` are accessed using the `SetVariable()` function with a *DataSize* of zero, the variable contents shall be hidden until the next system restart and not be available for retrieval by future `GetVariable()` calls. After such `SetVariable()` access any `GetVariable()` attempt shall return `EFI_NOT_FOUND` error. Calls to `SetVariable()` with non-zero *DataSize* shall be processed as if *DataSize* is zero

9.3.4. Variable Format

The UEFI variables for delivery of temporary credentials shall contain an array of UTF-8 characters in the format `Username:Password` where the `:` character shall act as separator. The final byte of the array shall be `0x00` as terminator and the size of the variable shall be length of `Username` plus length of `Password` plus 2. Characters shall be chosen from the set elsewhere defined as legal for Redfish `Username` and `Password` and neither field may contain the `:` character.

For convenience when identifying the auto-generated credentials when active and for the purpose of editing permissions, the following `Username` strings shall be used:

Usage	Username
Default Firmware Auto Username	HostAutoFW
Default OS Auto Username	HostAutoOS

10. ANNEX A (informative)

10.1. Change log

Version	Date	Description
1.0.0a	2016-12-07	Initial release