OCF "Ipanema" – Specify an Error Diagnostic Payload – Core Technology WG CR 2830

Legal Disclaimer

***** First Change *****

2. Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 8601, *Data elements and interchange formats – Information interchange –Representation of dates and times*, International Standards Organization, December 3, 2004

ISO/IEC DIS 20924, *Information Technology – Internet of Things – Vocabulary*, June 2018
https://www.iso.org/standard/69470.html

ISO/IEC 30118-2:2018, Information technology – Open Connectivity Foundation (OCF) Specification – Part 2: Security specification
https://www.iso.org/standard/74239.html
Latest version available at:
https://openconnectivity.org/specs/OCF_Security_Specification.pdf

ISO/IEC 30118-5:2018, Information technology – Open Connectivity Foundation (OCF) Specification – Part 5: Smart home device specification
https://www.iso.org/standard/74242.html
Latest version available at: https://openconnectivity.org/specs/OCF_Device_Specification.pdf

OCF Easy Wi-Fi Setup, Information technology – Open Connectivity Foundation (OCF) Specification – Part 7: Wi-Fi Easy Setup specification
Latest version available at: https://openconnectivity.org/specs/OCF_Wi-Fi_Easy_Setup_Specification_v2.0.1.pdf

IETF RFC 768, *User Datagram Protocol*, August 1980
https://www.rfc-editor.org/info/rfc768

IETF RFC 3339, *Date and Time on the Internet: Timestamps*, July 2002
https://www.rfc-editor.org/info/rfc3339

IETF RFC 3986, *Uniform Resource Identifier (URI): General Syntax, January 2005*
https://www.rfc-editor.org/info/rfc3986

IETF RFC 4122, *A Universally Unique IDentifier (UUID) URN Namespace*, July 2005
https://www.rfc-editor.org/info/rfcfse4122

IETF RFC 4287, *The Atom_Syndication Format*, December 2005
https://www.rfc-editor.org/info/rfc4287

IETF RFC 4941, *Privacy Extensions for Stateless Address Autoconfiguration in IPv6*, September 2007
https://www.rfc-editor.org/info/rfc4941

IETF RFC 5424, *The Syslog Protocol*, March 2009
https://tools.ietf.org/html/rfc5424IETF RFC 5646, *Tags for Identifying Languages*, September

2009
https://www.rfc-editor.org/info/rfc5646

IETF RFC 5988, *Web Linking: General Syntax, October 2010*
https://www.rfc-editor.org/info/rfc5988

IETF RFC 6347, *Datagram Transport Layer Security Version 1.2*, January 2012
https://www.rfc-editor.org/info/rfc6347

IETF RFC 6434, *IPv6 Node Requirements*, December 2011
https://www.rfc-editor.org/info/rfc6434

IETF RFC 6573, *The Item and Collection Link Relations*, April 2012
https://www.rfc-editor.org/info/rfc6573

IETF RFC 6690, *Constrained RESTful Environments (CoRE) Link Format*, August 2012
https://www.rfc-editor.org/info/rfc6690

IETF RFC 7049, *Concise Binary Object Representation (CBOR)*, October 2013
https://www.rfc-editor.org/info/rfc7049

IETF RFC 7084, *Basic Requirements for IPv6 Customer Edge Routers*, November 2013
https://www.rfc-editor.org/info/rfc7084

IETF RFC 7159, *The JavaScript Object Notation (JSON) Data Interchange Format*, March 2014
https://www.rfc-editor.org/info/rfc7159

IETF RFC 7252, *The Constrained Application Protocol (CoAP)*, June 2014
https://www.rfc-editor.org/info/rfc7252

IETF RFC 7301, *Transport Layer Security (TLS) Application-Layer Protocol Negotiation Extension*, July 2014
https://www.rfc-editor.org/info/rfc7301

IETF RFC 7595, *Guidelines and Registration Procedures for URI Schemes*, June 2015
https://www.rfc-editor.org/info/rfc7595

IETF RFC 7641, *Observing Resources in the Constrained Application Protocol (CoAP)*, September 2015
https://www.rfc-editor.org/info/rfc7641

IETF RFC 7721, *Security and Privacy Considerations for IPv6 Address Generation Mechanisms*, March 20016
https://www.rfc-editor.org/info/rfc7721

IETF RFC 7959, *Block-Wise Transfers in the Constrained Application Protocol (CoAP)*, August 2016
https://www.rfc-editor.org/info/rfc7959

IETF RFC 8075, *Guidelines for Mapping Implementations: HTTP to the Constrained Application Protocol (CoAP)*, February 2017
https://www.rfc-editor.org/info/rfc8075

IETF RFC 8323, *CoAP (Constrained Application Protocol) over TCP, TLS, and WebSockets*, February 2018
https://www.rfc-editor.org/info/rfc8323

IANA ifType-MIB Definitions
https://www.iana.org/assignments/ianaiftype-mib/ianaiftype-mib

IANA IPv6 Multicast Address Space Registry
http://www.iana.org/assignments/ipv6-multicast-addresses/ipv6-multicast-addresses.xhtml

IANA Media Types Assignment, March 2017
http://www.iana.org/assignments/media-types/media-types.xhtml

IANA Link Relations, October 2017
http://www.iana.org/assignments/link-relations/link-relations.xhtml

JSON Schema Validation, *JSON Schema: interactive and non-interactive validation*, January 2013
http://json-schema.org/draft-04/json-schema-validation.html

OpenAPI specification, *fka Swagger RESTful API Documentation Specification*, Version 2.0
https://github.com/OAI/OpenAPI-Specification/blob/master/versions/2.0.md

***** Second Change *****

7.11 Error response payload

7.11.1 Overview

Clause 7.11 describes a mechanism and payload to signal additional error information that may be provided in addition to the response code when an error response is sent. The transport specific response for a transport binding (e.g., CoAP) returns a status code that does not always provide enough information on what has gone wrong.

7.11.2 Error response payload content

The error response payload shall be an ASCII string that contains a brief, human-readable diagnostic description as a string describing the details of the transport specific error response code. Standardized messages for the error response payload are defined in Table 1. Vendors may use these standardized messages or define their own messages. The messages contained within an error response payload may be included with any transport specific response code. English text is the only language supported for the message. If the error response payload is not present in the response, a Client deals with the error based on only the transport specific response code.

Table 1 – Standardized error message

Category	Message
Error due to Client	"Invalid parameter"
	"The mandatory parameter is missing"
	"The parameter is not allowed"
	"The token syntax is invalid"
	"The message id syntax is invalid"
	"Invalid permission"
	"The service key is invalid"
	"The token is not issued"

	"The token user is not issued"
	"Terms of service are not agreed"
	"The API is not permitted"
	"The API call count is exceeded"
	"The country is not supported"
	"The Device is inaccessible"
	"The token is invalid"
	"The count of subscription has exceeded the limit"
	"Invalid resource access"
	"The admin is not registered"
	"The user is not registered"
	"The service is not registered"
	"The event is not subscribed"
	"The Device is not registered"
	"The admin is already registered.
	"Internal Server operation error"
	"Device profile error"
	"The model is not supported"
	"Undefined enumeration"
	"The value is out of range"
	"Feature is not supported in the model"
	"Integration Server error"
	"The product is not supported for interworking with other companies"
	"The Device status is abnormal"
	"The Device is not connected (offline)"
	"The Device control failed"
	"The request is required to retry"
	"Time out occurred"
Error due to Server	"Internal Server operation error"
	"Device profile error"
	"The model is not supported"
	"Undefined enumeration"
	"The value is out of range"
	"Feature is not supported in the model"
	"Integration Server error"
	"The product is not supported for interworking with other companies"
	"The Device status is abnormal"
	"The Device is not connected (offline)"
	"The Device control failed"
	"The request is required to retry"

	"Time out occurred"

7.11.3 Example of use

The following example shows an example message exchange for a RETRIEVE operation sent from a proximal Device to an OCF Cloud, with the target URI "coaps+tcp://exampleCloudEndPoint//deviceId_001/somehref".

Client request:

```
Target URI: /deviceId_001/somehref
Operation: RETRIEVE
Host: coaps://exampleCloudEndPoint
Accept: application/vnd.ocf+cbor
```

Server response:

```
Status code: 4.04 (Not Found)
Response Body: {
  "The device is not registered"
}
```

With the error response payload the Client can recognize that the Device it tried to discover is not registered on the OCF Cloud.

***** Third Change *****

12.2.9 Mapping the error response payload

The error response payload as defined in 7.11 shall be included as a diagnostic payload as described in IETF RFC 7252 clause 5.5.2. The diagnostic payload shall be encoded in ASCII.

***** Fourth Change *****

12.3.9 Mapping the error response payload

The mapping of the error response payload for CoAP serialization over TCP shall conform to 12.2.9.

***** C2C Spec Change *****

5.3 General OCF Cloud API for Cloud Services elements

Any responses that are sent by an OCF Cloud may include a diagnostic payload (see OCF Core Spec clause X.Y). If a diagnostic payload is included in a response, the response shall have a Content-Type header encoded as "text/plain", see also RFC 8075 clause 6.6.