OCF "Fargo" – Clarification of Link Parameters – Core Technology WG CR 1915

Legal Disclaimer

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.

[... Existing Text Unchanged...]

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 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 8288, *Web Linking*, October 2017
https://www.rfc-editor.org/info/rfc8288

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

3. Terms, definitions, and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

– ISO Online browsing platform: available at https://www.iso.org/obp.

– IEC Electropedia: available at http://www.electropedia.org/.

[... Existing Text Unchanged...]

3.1.21
Introspection Device Data (IDD)
data that describes the payloads per implemented method of the Resources (3.1.22) that make up the Device (3.1.14)

Note 1 to entry: See 11.8 for all requirements and exceptions.

3.1.22
Links
extends typed web links according to IETF RFC 8288

3.1.23
Non-Discoverable Resource
a Resource (3.1.32) that is not listed in "/oic/res"

Note 1 to entry: The Resource (3.1.32) can be reached by a Link (3.1.22) which is conveyed by another Resource (3.1.32). For example a Resource (3.1.32) linked in a Collection (3.1.8) does not have to be listed in "/oic/res", since traversing the Collection (3.1.8) would discover the Resource (3.1.32) implemented on the Device (3.1.14).

[... Existing Text Unchanged...]

7.8 Structure

7.8.1 Introduction

In many scenarios and contexts, the Resources may have either an implicit or explicit structure between them. This may be achieved through the use of Collection (7.8.6) and Atomic Measurement (7.8.7) Resources.

7.8.2 Resource relationships (Links)

7.8.2.1 Introduction

Resource relationships are expressed as Links. A Link is a hyperlink, which defines a typed connection between two Resources. Hyperlinks, or web links, have the following components as defined in IETF RFC 8288:

– Link context (URI reference) as defined in 7.8.2.2
– Link relation type as defined in 7.8.2.3
– Link target (URI reference) as defined in 7.8.2.4
– Link target attributes as defined in 7.8.2.5

The Link context is the Resource with which the Link is associated. A Link is viewed as a statement of the form "(Link context) has a (Link relation type) to a Resource at (Link target), which has (Link target attributes)" as per IETF RFC 8288 clause 2.

To paraphrase, the Link target is related to the Link context according to the Link relation type. Additionally, the Link target attributes make semantic statements about the Link target, to identify the content type, physical location, etc.

Links conform to the definitions in IETF RFC 8288, with an example JSON serialization with associated Link Parameters as illustrated:

```
{
  "anchor": "/some/ocf/resource",     // Link context, optional
  "rel": ["hosts"],                   // Link relation Type, optional
  "href": "/some/other/ocf/resource", // Link target, required
  "p": {"bm": 3},                     // Link target attributes, optional
  "if": ["oic.if.baseline"],          // Link target attributes, required
  "rt": ["oic.r.sensor"]              // Link target attributes, required
}
```

Additional items in the Link may be made mandatory based on the use of the Links in different contexts (e.g. in Collections, in discovery, in bridging etc.). The OpenAPI 2.0 file for the Link payload is detailed in Annex D.

Another example of a Link is as illustrated:

```
{"href": "/switch", "rt": ["oic.r.switch.binary"], "if": ["oic.if.a",
"oic.if.baseline"], "p": {"bm": 3}, "rel": "item"}
```

7.8.2.2 Link context

The Link context is defined in the Link using the "anchor" Parameter. If the Link doesn't contain an "anchor" Parameter, the Link context shall be the Resource from which the Link was retrieved.

7.8.2.3 Link relation type

The Link relation type conveys the semantics of the Link. The Link relation type is defined in the Link using the "rel" Parameter. If the Link doesn't contain a "rel" Parameter, the Link relation type shall be assumed to have the default value "hosts", which means that the Resource at the Link target is "hosted" by the Resource at the Link context. The set of Link relation types to be used to describe various relationships between Resources are as listed:

- "hosts"
  - The Link target points to a Resource that is hosted at the Link context. This Link relation type indicates that the Resource is allowed to be included in the batch representations of the Link target. This Link relation type is defined by IETF RFC 6690.
- "self"
  - The Link refers to the Link context, which allows a Link to describe the Resource at the Link context, which is to say that the Link can describe the Collection or Atomic Measurement Resource that the Link is retrieved from. The Link target points to the Link context, and the Link target attributes describe the Link context. This Link relation type is defined by IETF RFC 4287.
- "item"
  - The Link target points to a Resource that is a member of the Collection or Atomic Measurement at the Link context, which might not specifically be hosted by the Collection or Atomic Measurement Resource, and is allowed to be contained in batch representations of the Collection or Atomic Measurement. An example is using "rel": "item" to declare that the Properties of the Collection or Atomic Measurement Resource itself should be included in a batch representation of the Collection or Atomic Measurement. This Link relation type is defined by IETF RFC 6573.

All of these Link relation types are registered in the IANA Registry for Link relations types defined in IANA Link Relations. Other Link relation types may be included in Links, provided that they conform to the requirements in IETF RFC 8288. Other Link relation types may be defined for features contained in other specifications and may not be included in what is defined in this clause. The presence of Link relation types not defined in this document does not affect the processing of Link relation types defined in this document.

When there is more than one Link relation type value in a Link, all of the values apply to describe the relationship between the Link context and the Link target. A Link with multiple Link relation type values is equivalent to a set of Links having the same Link context and Link target, each having one of the Link relation values.

7.8.2.4 Link target

The Link target is a URI reference to a Resource using the "href" Parameter.

7.8.2.5 Parameters for Link target attributes

7.8.2.5.1 Introduction

Link target attributes are specialisations of Link Parameters. Table 1 lists all the Link target attributes defined in this document.

Table 1 – Link target attributes list

Parameter title	Parameter name	Mandatory	Description
Device ID	"di"	No	Defined in clause 7.8.2.5.5

OCF Endpoint information	"eps"	No	Defined in clause 7.8.2.5.6
OCF Interface	"if"	Yes	Defined in clause 7.6
Link instance	"ins"	No	Defined in clause 7.8.2.5.2
Policy	"p"	No	Defined in clause 7.8.2.5.3
Resource Type	"rt"	Yes	Defined in clause 7.4
Media type	"type"	No	Defined in clause 7.8.2.5.4

Note: Other Link target attributes may to defined for features in other specifications and may not be included in this table.

7.8.2.5.2 "ins" or Link instance Parameter

The "ins" Parameter identifies a particular Link instance in a list of Links. The "ins" Parameter may be used to modify or delete a specific Link in a list of Links. The value of the "ins" Parameter is set at instantiation of the Link by the OCF Device (Server) that is hosting the list of Links – once it has been set, the "ins" Parameter shall not be modified for as long as the Link is a member of that list.

7.8.2.5.3 "p" or policy Parameter

The policy Parameter defines various rules for correctly accessing a Resource referenced by a target URI. The policy rules are configured by a set of key-value pairs.

The policy Parameter "p" is defined by:

– "bm" key: The "bm" key corresponds to an integer value that is interpreted as an 8-bit bitmask. Each bit in the bitmask corresponds to a specific policy rule. The rules are specified for "bm" in Table 2:

Table 2 – "bm" Property definition

Bit Position	Policy rule	Comment
Bit 0 (the LSB)	discoverable	The discoverable rule defines whether the Link is to be included in the Resource discovery message via "/oic/res". If the Link is to be included in the Resource discovery message, then "p" shall include the "bm" key and set the discoverable bit to value 1. If the Link is NOT to be included in the Resource discovery message, then "p" shall either include the "bm" key and set the discoverable bit to value 0 or omit the "bm" key entirely.
Bit 1 (2nd LSB)	observable	The Observable rule defines whether the Resource referenced by the target URI supports the NOTIFY operation. With the self-link, i.e. the Link with "rel" value of "self", "/oic/res" can have a Link with the target URI of "/oic/res" and indicate itself Observable. The "self" is defined by IETF RFC 4287 and registered in the IANA Registry for "rel" value defined at IANA Link Relations. If the Resource supports the NOTIFY operation, then "p" shall include the "bm" key and set the Observable bit to value 1. If the Resource does NOT support the NOTIFY operation, then "p" shall either include the "bm" key and set the Observable bit to value 0 or omit the "bm" key entirely.
Bits 2-7	--	Reserved for future use. All reserved bits in "bm" shall be set to value 0.

NOTE If all the bits in "bm" are defined to value 0, then the "bm" key may be omitted entirely from "p" as an efficiency measure. However, if any bit is set to value 1, then "bm" shall be included in "p" and all the bits shall be defined appropriately.

- "sec" and "port" in the remaining bullets shall be used only in a response payload when the request does not include an OCF-Accept-Content-Format-Version option as defined in 12.2.5. In a payload sent in response to a request that includes an OCF-Accept-Content-Format-Version option "sec" and "port" shall not be used and instead the "eps" Parameter shall provide the information for an encrypted connection. See Annex E for the schema for the "p" Parameter that includes "sec" and "port".
- "sec" key: The "sec" key corresponds to a Boolean value that indicates whether the Resource referenced by the target URI is accessed via an encrypted connection. If "sec" is true, the Resource is accessed via an encrypted connection, using the "port" specified. If "sec" is false, the Resource is accessed via an unencrypted connection, or via an encrypted connection (if such a connection is made using the "port" settings for another Resource, for which "sec" is true).
- "port" key: The "port" key corresponds to an integer value that is used to indicate the port number where the Resource referenced by the target URI may be accessed via an encrypted connection.
- If the Resource is only available via an encrypted connection (i.e. DTLS over IP), then
  - "p" shall include the "sec" key and its value shall be true.
  - "p" shall include the "port" key and its value shall be the port number where the encrypted connection may be established.
- If the Resource is only available via an unencrypted connection, then
  - "p" shall include the "sec" key and its value shall be false or "p" shall omit the "sec" key; the default value of "sec" is false.
  - "p" shall omit the "port" key.
- If the Resource is available via both an encrypted and unencrypted connection, then
  - "p" shall include the "sec" key and its value shall be false or "p" shall omit the "sec" key; the default value of "sec" is false.
  - "p" may omit the "port" key. If the "port" key is omitted, the Resource shall be available using the same "port" information as another Resource on the Device for which "sec" is true.
- Access to the Resource on the port specified by the "port" key shall be made by an encrypted connection (e.g. "coaps://"). (Note that unencrypted connection to the Resource may be possible on a separate port discovered thru multicast discovery).
- Note that access to the Resource is controlled by the ACL for the Resource. A successful encrypted connection does not ensure that the requested action will succeed. See ISO/IEC 30118-2:2018 clause 12 for more information.

Example 1: This shows the policy Parameter for a Resource that is discoverable but not Observable, and for which authenticated accesses shall be done via CoAPS port 33275.

```
"p": {"bm": 1}
```

Example 2: This shows a self-link, i.e. the "/oic/res" Link in itself that is discoverable and Observable.

```
{
  "href": "/oic/res",
  "rel": "self",
  "rt": ["oic.wk.res"],
```

```
  "if": ["oic.if.ll", "oic.if.baseline"],
  "p": {"bm": 3}
}
```

7.8.2.5.4 "type" or media type Parameter

The "type" Parameter may be used to specify the various media types that are supported by a specific target Resource. The default type of "application/vnd.ocf+cbor" shall be used when the "type" element is omitted. Once a Client discovers this information for each Resource, it may use one of the available representations in the appropriate header field of the Request or Response.

7.8.2.5.5 "di" or Device ID Parameter

The "di" Parameter specifies the Device ID of the Device that hosts the target Resource defined in the in the "href" Parameter.

The Device ID may be used to qualify a relative reference used in the "href" or to lookup OCF Endpoint information for the relative reference.

7.8.2.5.6 "eps" Parameter

The "eps" Parameter indicates the OCF Endpoint information of the target Resource.

"eps" shall have as its value an array of items and each item represents OCF Endpoint information with "ep" and "pri" as specified in 10.2. "ep" is mandatory but "pri" is optional.

This is an example of "eps" with multiple OCF Endpoints.

```
"eps": [
  {"ep": "coap://[fe80::b1d6]:1111", "pri": 2},
  {"ep": "coaps://[fe80::b1d6]:1122"},
  {"ep": "coap+tcp://[2001:db8:a::123]:2222", "pri": 3}
]
```

When "eps" is present in a link, the OCF Endpoint information in "eps" can be used to access the target Resource referred by the "href" Parameter.

Note that the type of OCF Endpoint – Secure or Unsecure – that a Resource exposes merely determines the connection type(s) guaranteed to be available for sending requests to the Resource. For example, if a Resource only exposes a single CoAP "ep", it does not guarantee that the Resource cannot also be accessed via a Secure OCF Endpoint (e.g. via a CoAPS "ep" from another Resource's "eps information). Nor does exposing a given type of OCF Endpoint ensure that access to the Resource will be granted using the "ep" information. Whether requests to the Resource are granted or denied by the Access Control layer is separate from the "eps" information, and is determined by the configuration of the /acl2 Resource (see ISO/IEC 30118-2:2018 clause 13.5.3 for details).

When present, max-age information (e.g. Max-Age option for CoAP defined in IETF RFC 7252) determines the maximum time "eps" values may be cached before they are considered stale.

[... Existing Text Unchanged in Remaining Subclauses...]