Specification for Transfer of OpenC2 Messages via HTTPS Version 1.0

Working Draft 03

16 October 2018

Specification URIs

This Version:

http://docs.oasis-open.org/openc2/open-impl-https/v1.0/csd01/open-impl-https-v1.0-csd01.md (Authoritative)

http://docs.oasis-open.org/openc2/open-impl-https/v1.0/csd01/open-impl-https-v1.0-csd01.html

http://docs.oasis-open.org/openc2/open-impl-https/v1.0/csd01/open-impl-https-v1.0-csd01.pdf

Previous Version:

N/A

Latest Version:

http://docs.oasis-open.org/openc2/open-impl-https/v1.0/open-impl-https-v1.0.md (Authoritative)

http://docs.oasis-open.org/openc2/open-impl-https/v1.0/open-impl-https-v1.0.html

http://docs.oasis-open.org/openc2/open-impl-https/v1.0/open-impl-https-v1.0.pdf

Technical Committee:

OASIS Open Command and Control (OpenC2) TC

Chairs:

- Joe Brule (jmbrule@nsa.gov), National Security Agency
- Sounil Yu (sounil.yu@bankofamerica.com), Bank of America

Editor:

- David Lemire (dave.lemire@g2-inc.com), G2, Inc.

Related work:

This specification is related to:

- OpenC2 Language Specification
- Stateless Packet Filtering Application Profile

Abstract:

Open Command and Control (OpenC2) is a concise and extensible language to enable the command and control of cyber defense components, subsystems and/or systems in a manner that is agnostic of the underlying products, technologies, transport mechanisms or other aspects of the implementation. HTTP over TLS is a widely deployed transfer protocol that provides an authenticated, ordered, lossless delivery of uniquely-identified messages. This specification describes the use of HTTP over TLS as a transfer mechanism for OpenC2 messages.

Status:

This document was last revised or approved by the OASIS Open Command and Control (OpenC2) TC on the above date. The level of approval is also listed above. Check the "Latest version" location noted above for possible later revisions of this document. Any other numbered Versions and other technical work produced by the Technical Committee (TC) are listed at https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=openc2#technical.

TC members should send comments on this specification to the TC's email list. Others should send comments to the TC's public comment list, after subscribing to it by following the instructions at the "Send A Comment" button on the TC's web page at https://www.oasis-open.org/committees/openc2/.

This specification is provided under the Non-Assertion Mode of the OASIS IPR Policy, the mode chosen when the Technical Committee was established. For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the TC's web page (https://www.oasis-open.org/committees/openc2/ipr.php).

Note that any machine-readable content (Computer Language Definitions) declared Normative for this Work Product is provided in separate plain text files. In the event of a discrepancy between any such plain text file and display content in the Work Product's prose narrative document(s), the content in the separate plain text file prevails.

Citation format:

When referencing this specification the following citation format should be used:

[OpenC2-HTTPS-v1.0]

62 *Specification for Transfer of OpenC2 Messages via HTTPS Version 1.0*. Edited by David Lemire.
63 09 August 2018. OASIS Committee Specification Draft 02. http://docs.oasis-
64 open.org/openc2/open-impl-https/v1.0/csd02/open-impl-https-v1.0-csd02.html.

65 Latest version: http://docs.oasis-open.org/openc2/open-impl-https/v1.0/open-impl-https-
66 v1.0.html.

67 ---

68

Notices

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full Policy may be found at the OASIS website.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

OASIS requests that any OASIS Party or any other party that believes it has patent claims that would necessarily be infringed by implementations of this OASIS Committee Specification or OASIS Standard, to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification.

OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any patent claims that would necessarily be infringed by implementations of this specification by a patent holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification. OASIS may include such claims on its website, but disclaims any obligation to do so.

OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS' procedures with respect to rights in any document or deliverable produced by an OASIS Technical Committee can be found on the OASIS website. Copies of

claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this OASIS Committee Specification or OASIS Standard, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any information or list of intellectual property rights will at any time be complete, or that any claims in such list are, in fact, Essential Claims.

The name "OASIS" is a trademark of OASIS, the owner and developer of this specification, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, specifications, while reserving the right to enforce its marks against misleading uses. Please see https://www.oasis-open.org/policies-guidelines/trademark for above guidance.

Table of Contents

1 Introduction

OpenC2 is a suite of specifications to achieve command and control of cyber defense functions. These specifications include the OpenC2 Language Specification, Actuator Profiles, and Transfer Specifications. This transfer specification defines the procedures and conventions used when employing Hypertext Transfer Protocol (HTTP) and Transport Layer Security (TLS) for the transfer of OpenC2 command and response messages between OpenC2 Producers and Consumers. This specification is one of an expected portfolio of transfer specifications; implementers of OpenC2 should select one or more transfer specifications, consistent with the characteristics and requirements of their cyber ecosystem.

1.1 IPR Policy

This specification is provided under the Non-Assertion Mode of the OASIS IPR Policy, the mode chosen when the Technical Committee was established. For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the TC's web page (https://www.oasis-open.org/committees/openc2/ipr.php).

1.2 Terminology

A list of acronyms is provided in Annex A.

1.2.1 Requirement Keywords

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119] and [RFC8174] when, and only when, they appear in all capitals, as shown here.

1.3 Normative References

[RFC2119]

Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC2818]

Rescorla, E., "HTTP Over TLS", RFC 2818, DOI 10.17487/RFC2818, May 2000, <https://www.rfc-editor.org/info/rfc2818>.

[RFC5246]

Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008, <https://www.rfc-editor.org/info/rfc5246>.

[RFC5280]

Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>.

[RFC7230]

Fielding, R., Ed., and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing", RFC 7230, DOI 10.17487/RFC7230, June 2014, <https://www.rfc-editor.org/info/rfc7230>.

[RFC7231]

Fielding, R., Ed., and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content", RFC 7231, DOI 10.17487/RFC7231, June 2014, <https://www.rfc-editor.org/info/rfc7231>.

[RFC7235]

Fielding, R., Ed., and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Authentication", RFC 7235, DOI 10.17487/RFC7235, June 2014, <https://www.rfc-editor.org/info/rfc7235>.

[RFC7540]

Belshe, M., Peon, R., and Thompson, M., "Hypertext Transfer Protocol Version 2 (HTTP/2)", RFC 7540, DOI 10.17487/RFC7540, May 2015, <https://www.rfc-editor.org/info/rfc7540>.

[RFC8174]

Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <http://www.rfc-editor.org/info/rfc8174>.

[RFC8446]

Recorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <http://www.rfc-editor.org/info/rfc8446>

[OpenC2-Lang-v1.0]

Open Command and Control (OpenC2) Language Specification Version 1.0.

Edited by Jason Romano and Duncan Sparrell.

Latest version: http://docs.oasis-open.org/openc2/oc2ls/v1.0/oc2ls-v1.0.html.

1.4 Non-Normative References

[RFC3205]

Moore, K., "On the use of HTTP as a Substrate", BCP 56, RFC 3205, DOI 10.17487/RFC3205, February 2002, <https://www.rfc-editor.org/info/rfc3205>.

[RFC6546]

Trammell, B., "Transport of Real-time Inter-network Defense (RID) Messages over HTTP/TLS", RFC 6546, DOI 10.17487/RFC6546, April 2012, <https://www.rfc-editor.org/info/rfc6546>.

[RFC7525]

Sheffer, Y., Holz, R., and P. Saint-Andre, "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", BCP 195, RFC 7525, DOI 10.17487/RFC7525, May 2015, <https://www.rfc-editor.org/info/rfc7525>.

[SLPF]

Open Command and Control (OpenC2) Profile for Stateless Packet Filtering Version 1.0.

Edited by Joe Brule, Duncan Sparrell and Alex Everett.

Latest version: http://docs.oasis-open.org/openc2/oc2slpf/v1.0/oc2slpf-v1.0.html

1.5 Document Conventions

The following color, font and font style conventions are used in this document:

- All examples in this document are formatted in fixed font, with straight quotes, black text, a light grey background, and 4-space indentation.
- Parts of the example may be omitted for conciseness and clarity. These omitted parts are denoted with an ellipse (...).

Example:

```
HTTP/1.1 200 OK
Date: Day, DD Mon YYYY HH:MM:SS GMT
Content-type: application/openc2-cmd+json;version=1.0
X-Correlation-ID: bf5t2ttrsc8r

{
      "action": "query"
      "target": "command"
}
```

```

## 1.6 Overview

OpenC2 is a set of specifications to achieve command and control of cyber defense functions. These specifications include the OpenC2 Language Specification, Actuator Profiles, and Transfer Specifications. The OpenC2 Language Specification and Actuator Profile(s) specifications focus on the standard at the origin and destination of the command while the transfer specifications focus on the protocols for the commands and responses in transit.

- The OpenC2 Language Specification [OpenC2-Lang-v1.0] provides the semantics for the essential elements of the language, the structure for commands and responses, and the schema that defines the proper syntax for the language elements that represents the command or response.

- OpenC2 Actuator Profiles specify the subset of the OpenC2 language relevant in the context of specific actuator functions. Cyber defense components, devices, systems and/or instances may (in fact are likely) to implement multiple actuator profiles, such as Stateless Packet Filtering. Actuator profiles extend the language by defining specifiers that identify the actuator to the required level of precision and may define command arguments that are relevant and/or unique to those actuator functions.

- OpenC2 Transfer Specifications utilize existing protocols and standards to implement OpenC2 in specific environments. These standards are used for communications and security functions beyond the scope of the language, such as message transfer encoding, authentication, and end-to-end transport of OpenC2 messages.

[OpenC2-Lang-v1.0] defines a language used to compose messages for command and control of cyber defense systems and components. A message consists of a header (defined in this specification) and a payload (*defined* as a message body in the OpenC2 Language Specification Version 1.0 and *specified* in one or more actuator profiles). The language defines two payload structures:

1. **Command**: An instruction from one system known as the OpenC2 "Producer", to one or more systems, the OpenC2 "Consumer(s)", to act on the content of the command.

2. **Response**: Any information captured or necessary to send back to the OpenC2 Producer that issued the Command i.e., the OpenC2 Consumer's response to the OpenC2 Producer.

In general, there are two types of participants involved in the exchange of OpenC2 messages:

1. **OpenC2 Producers**: An OpenC2 Producer is an entity that creates commands to provide instruction to one or more systems to act in accordance with the content of the
```

command. An OpenC2 Producer may receive and process responses in conjunction with a command.

2. **OpenC2 Consumers**: An OpenC2 Consumer is an entity that receives and acts on an OpenC2 command. An OpenC2 Consumer may create responses that provide any information captured or necessary to send back to the OpenC2 Producer.

OpenC2 implementations integrate the related OpenC2 specifications described above with related industry specifications, protocols, and standards. Figure 1 depicts the relationships among OpenC2 specifications, and their relationships to other industry standards and environment-specific implementations of OpenC2. Note that the layering of implementation aspects in the diagram is notional, and not intended to preclude, e.g., the use of an application-layer message signature function to provide message source authentication and integrity.

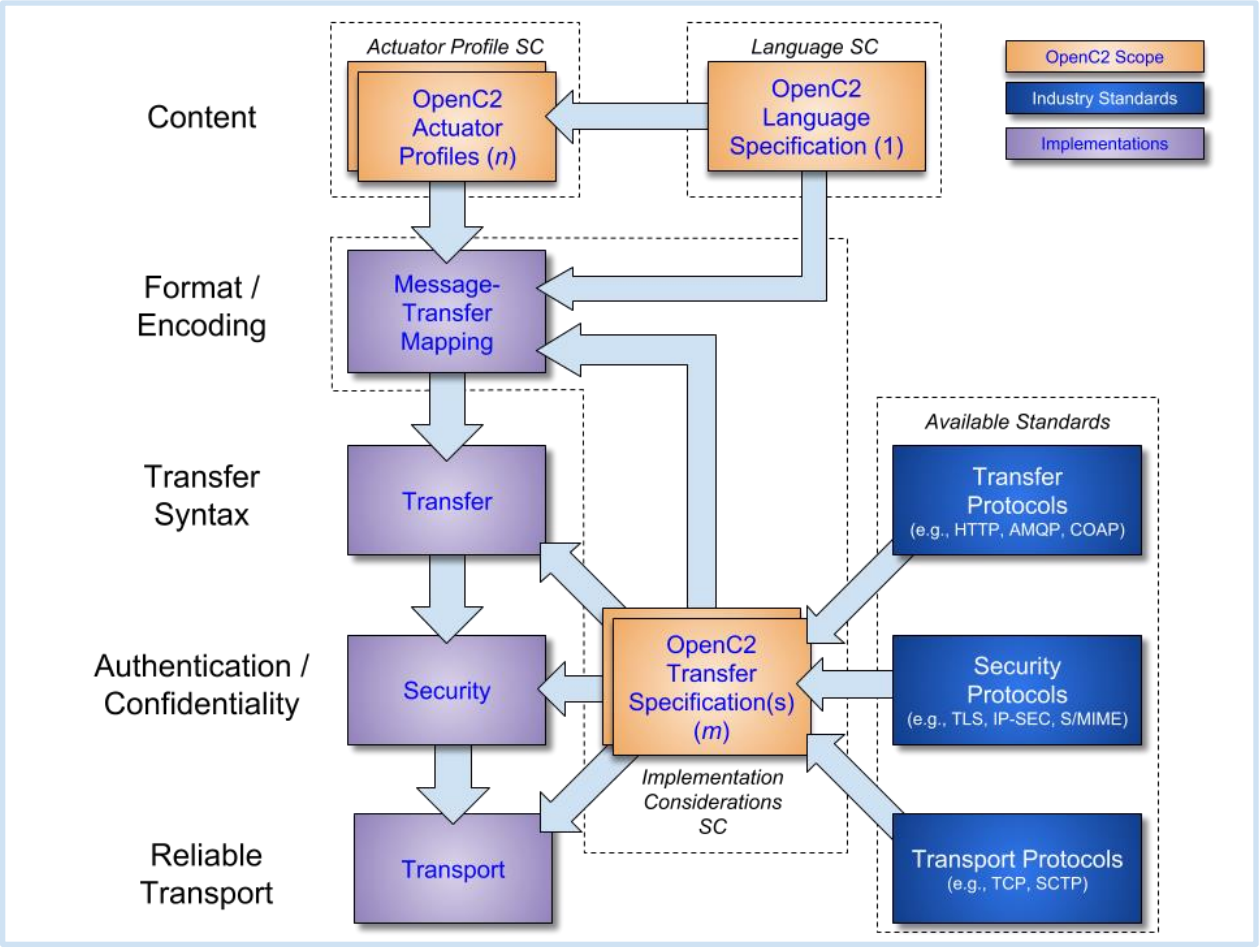

Figure 1 -- OpenC2 Documentation and Layering Model

This document specifies the use of Hypertext Transfer Protocol (HTTP) over Transport Layer Security (TLS) as a transport mechanism for OpenC2 messages; this HTTP/TLS layering is typically referred to as HTTPS [RFC2818]. As described in [RFC3205], HTTP has become a common "substrate" for information transfer for other application-level protocols. The broad

availability of HTTP makes it a useful option for OpenC2 message transport in support of prototyping, interoperability testing, and for operational use in environments where appropriate security protections can be provided. Similarly, TLS is a mature and widely-used protocol for securing information transfers in TCP/IP network environments. This specification provides guidance to the OpenC2 implementation community when utilizing HTTPS for OpenC2 message transport. It includes guidance for selection of TLS versions and options suitable for use with OpenC2.

1.7 Suitability

This OpenC2 over HTTPS transfer specification is suitable for operational environments where:

- Connectivity between OpenC2 producers and OpenC2 consumers is:
  - Highly available, with infrequent network outages
  - Of sufficient bandwidth that no appreciable message delays or dropped packets are experienced
- In-band negotiation of a connection initiated by either producer or consumer is possible without requiring an out-of-band signalling network.
- The overhead of HTTPS is acceptable (e.g., multiple OpenC2 command / response exchanges can be passed through a single HTTPS connection).

An additional application for this transfer specification is interoperability test environments.

2 Operating models

This section describes the operating models associated with the available assignments of endpoint roles with regard to OpenC2 and HTTP.

2.1 Endpoint Definitions

Each endpoint of an OpenC2-over-HTTPS interaction has both an OpenC2 role and an HTTP function. Ideally OpenC2 Consumers will be HTTP listeners so that they can accept connections and receive unsolicited commands from OpenC2 Producers. With this approach OpenC2 Producers act as 'HTTP clients' and transmit commands to Consumers.

In some environments, networking considerations may limit or preclude this configuration. For example, if the OpenC2 Consumer is located behind a router that performs network port and/or address translation, it may not be practicable for the Producer to contact an HTTP server listening on behalf of the Consumer. In these cases, each OpenC2 endpoint must act as both an HTTP client and a server.

One example of using HTTP as a substrate, [RFC6546], *Transport of Real-time Inter-network Defense (RID) Messages over HTTP/TLS*, addresses this situation by specifying an arrangement where each RID server is both an HTTP/TLS server and an HTTP/TLS client. Given the anticipated range of implementation environments for OpenC2, a more flexible approach appears justified, so this specification allows for three implementation configurations:

- The OpenC2 Consumer is the HTTP server
- The OpenC2 Producer is the HTTP server
- Both OpenC2 Producer and Consumer are HTTP servers

Where possible, the configuration where the OpenC2 Consumer is the HTTP server is preferred, as it aligns OpenC2 command / response messaging with HTTP's request / response structure.

The following sections briefly summarize each of these operating models. Specifications for how the models are implemented are provided in Section 3 and example interactions are described in Annex B.

2.2 OpenC2 Consumer as the HTTP server

Figure 2 illustrates the configuration where the OpenC2 Consumer operates an HTTP server. In this configuration, a Producer that needs to send OpenC2 commands initiates a TCP connection to the Consumer. Once the TCP connection is created, a TLS session is initiated to authenticate the endpoints and provide connection confidentiality. The Producer can then issue OpenC2 commands by sending HTTP requests using the POST method, with Consumer OpenC2 responses returned in the HTTP response.

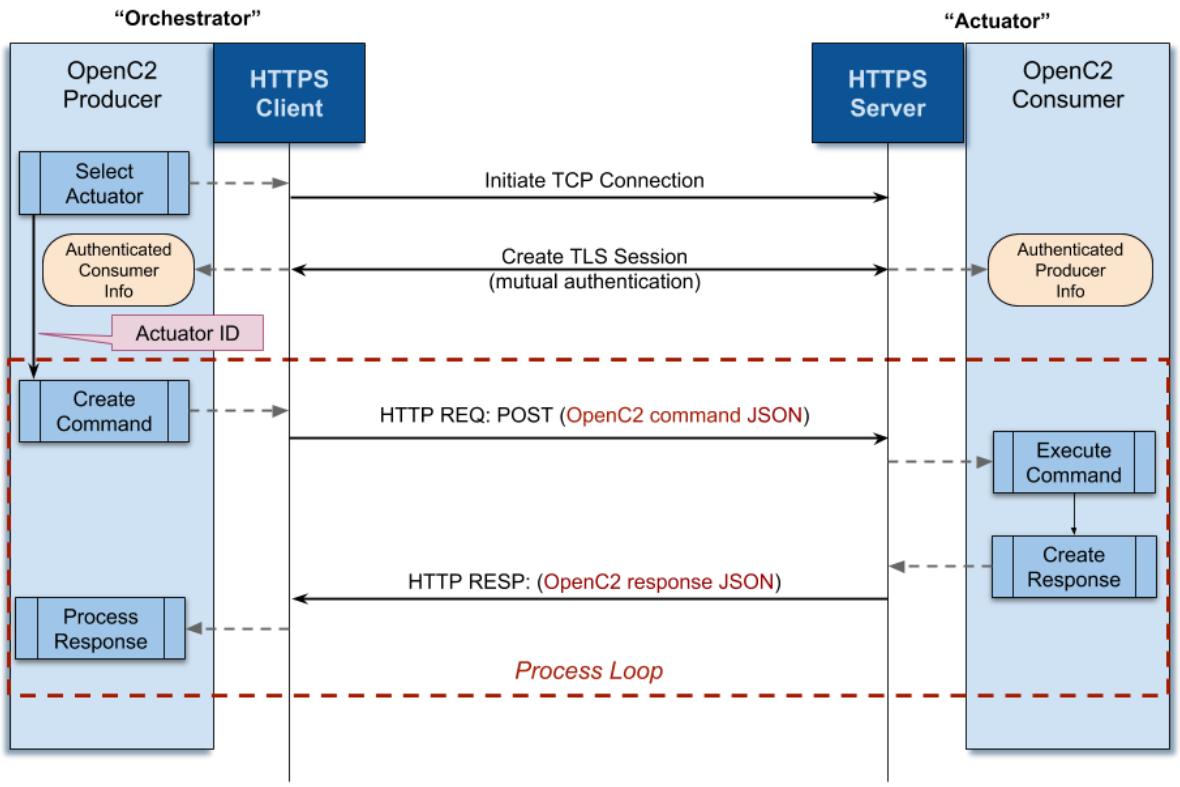

Figure 2 -- OpenC2 Consumer as HTTP Server

2.3 OpenC2 Producer as HTTP server

Figure 3 illustrates the configuration where the OpenC2 Producer operates an HTTP server. In this configuration, a Consumer that has been configured to request and accept OpenC2 commands from a particular Producer initiates a TCP connection to the Producer. Once the TCP connection is created, a TLS session is initiated to authenticate the endpoints and provide connection confidentiality. In this configuration, the exchange of OpenC2 commands and responses is driven by the Consumer using simple HTTP polling with the Producer.

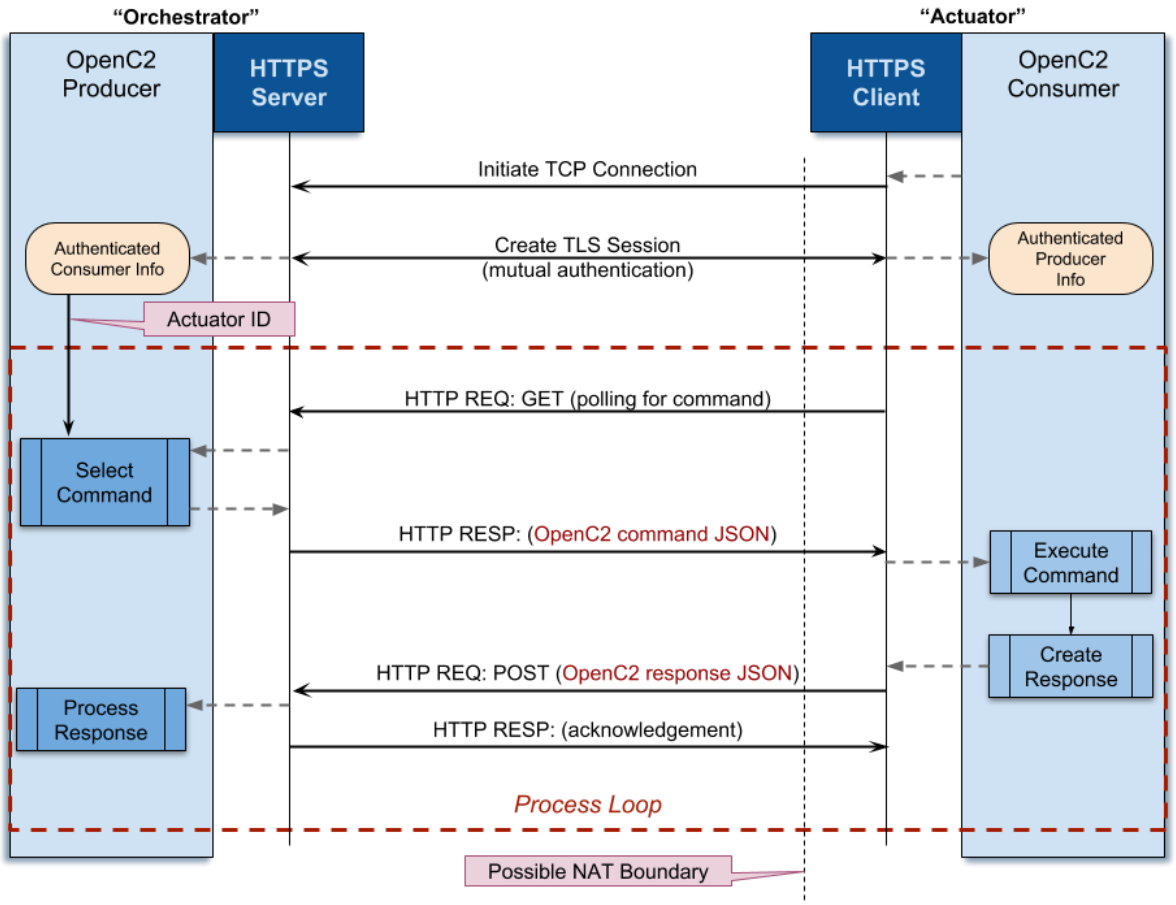

Figure 3 -- OpenC2 Producer as HTTP Server

2.4 Producer and Consumer as HTTP/TLS Servers

The configuration where both Producer and Consumer operate an HTTP server is operationally similar to the configuration where only the Consumer operates an HTTP server. In this configuration, a Producer that needs to send OpenC2 commands initiates a TCP connection to the Consumer. Once the TCP connection is created, a TLS session is initiated to authenticate the endpoints and provide connection confidentiality. The Producer can then issue OpenC2 commands by sending HTTP requests using the POST method, with Consumer OpenC2 responses returned in the HTTP response.

When the Consumer needs to send the Producer an OpenC2 response with updated status, it initiates a TCP connection to the Producer. Once the TCP connection is created, a TLS session is initiated to authenticate the endpoints and provide connection confidentiality. The Consumer can then transmit OpenC2 response messages using the HTTP POST method.

3 Protocol mappings

The section defines the requirements for using HTTP and TLS with OpenC2, including general requirements and protocol mappings for the three operating configurations described in Section 2.

3.1 Layering Overview

When using HTTPS for OpenC2 message transfer, the layering model is:

Layer	Description
OpenC2 Content	The OpenC2 Language Specification defines the overall OpenC2 language, and the Actuator Profile(s) implemented by any particular endpoint scopes the OpenC2 actions, targets, arguments, and specifiers that apply when commanding that type of Actuator.
Serialization	Serialization converts internal representations of OpenC2 content into a form that can be transmitted and received. The OpenC2 default serialization is JSON.
Message	The message layer provides a content- and transport-independent mechanism for conveying requests, responses and notifications. A message consists of content plus a set of meta items such as content type and version, sender, timestamp, and correlation id. This layer maps the transport-independent definition of each message element to its transport-specific on-the-wire representation. Note that notification messages are defined here for completeness even though OpenC2 does not currently define any notification content.
HTTP	The HTTP layer is responsible for conveying request, response, and notification messages, as described in this specification.
TLS	The TLS layer is responsible for authentication of connection endpoints and confidentiality and integrity of transferred messages.
Lower Layer Transport	The lower protocol layers are responsible for end-to-end delivery of messages. TCP/IP is the most common suite of lower layer protocols used with HTTPS.

3.2 General Requirements

This section defines serialization, HTTP, and TLS requirements that apply regardless of operating model.

3.2.1 Serialization and Content Types

While the OpenC2 language is agnostic of serialization, when transferring OpenC2 messages over HTTP/TLS as described in this specification, the default JSON verbose serialization described in [OpenC2-Lang-v1.0] MUST be used.

As described in [OpenC2-Lang-v1.0], transfer protocols must convey message elements. Two content types are defined here to support that requirement:

- OpenC2 Command:
  - msg_type: "request"
  - Content type: application/openc2-cmd+json;version=1.0
- OpenC2 Response:
  - Msg_type: "response"
  - Content type: application/openc2-rsp+json;version=1.0

OpenC2 command messages sent over HTTPS MUST use the content type "application/openc2-cmd+json;version=1.0".

OpenC2 response messages sent over HTTPS MUST use the content type "application/openc2-rsp+json;version=1.0".

3.2.2 HTTP Usage

OpenC2 Consumers MUST be HTTP listeners, to implement the operating model described in Section 2.2. OpenC2 Producers SHOULD be HTTP listeners, to support the operating models described in Sections 2.3 and 2.4. OpenC2 Producers and Consumers acting as HTTP listeners SHOULD listen on port 443, the registered port for HTTPS.

OpenC2 endpoints MUST implement all HTTP functionality required by this specification in accordance with HTTP/1.1 ([RFC7230], *et. al.*). As described in the Table 3-1, the only HTTP request methods utilized are GET and POST.

HTTP Method	Utilized
GET	Yes
HEAD	No
POST	Yes

PUT	No
DELETE	No
CONNECT	No
OPTIONS	No
TRACE	No

Table 3-1: HTTP Method Use

Each HTTP message body MUST contain only a single OpenC2 command or response message. This does not preclude a Producer and Consumer exchanging multiple OpenC2 command and response messages over time during a single HTTPS session. Depending on the set-up, a server and client can have multiple connections, but a sequence of OpenC2 interactions can spread over multiple connections. In some cases the connection may drop, but the session remains open (in an idle state).

All HTTP request and response messages containing OpenC2 payloads SHOULD include the "Cache-control:" header with a value of "no-cache".

3.2.3 TLS Usage

HTTPS, the transmission of HTTP over TLS, is specified in Section 2 of [RFC2818]. OpenC2 endpoints MUST accept TLS version 1.2 [RFC5246] connections or higher for confidentiality, identification, and authentication when sending OpenC2 messages over HTTPS, and SHOULD accept TLS Version 1.3 [RFC8446] or higher connections.

OpenC2 endpoints MUST NOT support any version of TLS prior to v1.2 and MUST NOT support any version of Secure Sockets Layer (SSL).

The implementation and use of TLS SHOULD align with the best currently available security guidance, such as that provided in [RFC7525]/BCP 195.

The TLS session MUST use non-NULL ciphersuites for authentication, integrity, and confidentiality. Sessions MAY be renegotiated within these constraints.

OpenC2 endpoints supporting TLS v1.2 MUST NOT use any of the blacklisted ciphersuites identified in Appendix A of [RFC7540].

OpenC2 endpoints supporting TLS 1.3 MUST NOT implement zero round trip time resumption (0-RTT).

When deployed in an operational environment, OpenC2 endpoints MUST support basic authentication and SHOULD support mutual authentication. When mutual authentication is

used, endpoints SHOULD support full path validation on each certificate, as defined in [RFC5280].

3.3 OpenC2 Consumer as HTTP/TLS Server

This section defines HTTP requirements that apply when the OpenC2 consumer is the HTTP server.

When the OpenC2 Consumer is the HTTP server, the Producer is able to initiate a connection to a specific Consumer and directly transmit OpenC2 messages containing commands; the HTTP POST method is used, with the OpenC2 command body contained in the POST body.

The contents of the X-Correlation-ID HTTP header MUST match the command-id in the OpenC2 message that is in the payload body, if one is present in the payload.

The following HTTP request headers MUST be populated when transferring OpenC2 commands:

- Host: host name of HTTP server:listening port number (if other than port 443)
- Content-type: application/openc2-cmd+json;version=1.0
- Date: date-time in HTTP-date format as defined by RFC 7231
- X-Correlation-ID: contains the OpenC2 command-id

The following HTTP response headers MUST be populated when transferring OpenC2 responses:

- Date: date-time in HTTP-date format as defined by RFC 7231
- Content-type: application/openc2-rsp+json;version=1.0
- X-Correlation-ID: contains the OpenC2 command-id

Example messages can be found in Annex B, section B.1.

3.4 OpenC2 Producer as HTTP/TLS Server

This section defines HTTP requirements that apply when the OpenC2 Producer is the HTTP server.

When the OpenC2 Producer is the HTTP server, the Consumer must poll for commands. The Consumer checks for commands by polling the Producer with the HTTP GET method. The polling interval is a matter of Consumer configuration. The interval SHOULD be short enough to meet latency requirements, but long enough to avoid excessive load on the server..

Since OpenC2 responses may not always be available immediately, the Producer may be in any of four states with respect to a particular Consumer when that Consumer polls:

- Producer has both commands and status queries
- Producer has commands but no status queries

- Producer has status queries but no commands
- Producer has neither commands nor status queries

The intent is that the Producer is able to transmit all commands and status queries to the Consumer and receive corresponding responses in a contiguous sequence of exchanges. To accomplish this, the Consumer MUST poll the Producer using the HTTP GET method to inquire whether the Producer has traffic for the Consumer. Polling messages sent by a Consumer MUST NOT contain an OpenC2 command-id and MUST NOT populate the HTTP X-Correlation-ID header field. Polling messages sent by a Consumer SHOULD populate the Accept: header with 'application/openc2-cmd+json;version=1.0'. The Producer will respond to each GET request with an HTTP response with code 200, OK, and a single command or status query in the response body, until the Producer's set of commands and queries is exhausted. The order in which the Producer sends multiple commands and/or status queries is undefined. After each exchange, the Consumer polls again without delay, until it receives an HTTP response with code 204, No Content.

The following HTTP request headers MUST be populated when a Producer responds to a Consumer's polling request with an OpenC2 command:

- Host: host name of HTTP server:listening port number (if other than port 443)
- Content-type: application/openc2-cmd+json;version=1.0
- Date: date-time in HTTP-date format as defined by RFC 7231
- X-Correlation-ID: contains the OpenC2 command-id

When the Producer sends a command in response to a Consumer poll, the Producer MUST populate the HTTP X-Correlation-ID field with the command-id value the Producer has assigned to the command. When the Producer sends a status query in response to a Consumer poll, the command-id in the X-Correlation-ID field MUST contain the command-id the Producer assigned when the command was originally sent.

The following HTTP response headers MUST be populated by a Consumer when transmitting OpenC2 responses:

- Date: date-time in HTTP-date format as defined by RFC 7231
- Content-type: application/openc2-rsp+json;version=1.0
- X-Correlation-ID: contains the OpenC2 command-id of the command to which this response applies

Example messages can be found in Annex B, section B.2.

3.5 OpenC2 Producer and OpenC2 Consumer as HTTP/TLS Servers

When both the Producer and the Consumer act as HTTP servers, the Producer contacts the Consumer to send commands and status queries as described in Section 3.3. If the Consumer needs to send an OpenC2 response to the Producer asynchronously, it uses the process

498 described in Section 3.4, initiating the connection and using the HTTP POST method to send the
499 OpenC2 response message.

500 Example messages for Producers sending OpenC2 commands can be found in Annex B, section
501 B.1. Example messages for Consumers asynchronously posting response messages can be found
502 in Annex B, section B.2.

4 Conformance

This specification defines a set of basic conformance requirements that all implementations must meet to claim conformance. An additional set of conformance requirements are defined for fully-authenticated implementations. Users of this specification deploying OpenC2 in an operational environment are strongly recommended to use fully-authenticated implementations in order to provide adequate security.

4.1 Basic Conformance

A conformant implementation of this transfer specification MUST:

1. Support JSON serialization as specified in Section 3.2.1
2. Transfer OpenC2 messages using the content types defined in Section 3.2.1 appropriately, as specified in Sections 3.3 and 3.4
3. Listen for HTTPS connections as specified in Section 3.2.2.
4. Use HTTP GET and POST methods as specified in Sections 3.2.2, 3.3, and 3.4, and no other HTTP methods
5. Ensure HTTP request and response messages only contain a single OpenC2 message, as specified in Section 3.2.2
6. Implement TLS in accordance with the requirements and restrictions specified in Sections 3.2.3 and 3.2.3.1
7. Employ HTTP methods to send and receive OpenC2 messages as specified in Sections 3.3 and 3.4
8. Employ only the HTTP response codes as specified in Sections 3.3 and 3.4
9. Instantiate the message elements defined in Table 3-1 of [OpenC2-Lang-v1.0] as follows:

Name	HTTPS Implementation
content	JSON verbose serialization of OpenC2 commands and responses carried in the HTTP message body
content_type / msg_type	Combined and carried in the HTTP Content-type and Accepted headers: Command: application/openc2-cmd+json;version=1.0 Response: application/openc2-rsp+json;version=1.0
status	Numeric status code supplied by OpenC2 Consumers is carried in the HTTP Response start line status code.
request_id	Valued supplied by OpenC2 Producers is carried in HTTP X-Correlation-ID header and delivered to recipient along with

	OpenC2 command.
created	Carried in the HTTP Date header
from	Populated with the authenticated identity of the peer entity, consistent with the configured authentication scheme.
to	Carried in the HTTP Host header

526 **Table 4-1 - Message Element Implementation**

527

528 4.2 Fully-Authentication Conformance

529 10. Fully-authenticated implementations of this transfer specification MUST support mutual
530 authentication using public key certificates with full path validation, as specified in
531 Section 3.2.3.
532

5 # Annex A. Acronyms

Term	Expansion
0-RTT	Zero Round Trip Time
API	Application Programming Interface
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP over TLS
IETF	Internet Engineering Task Force
IPR	Intellectual Property Rights
JSON	JavaScript Object Notation
RFC	Request For Comment
RID	Real-time Inter-network Defense
TC	Technical Committee
TCP	Transmission Control Protocol
TLS	Transport Layer Security

6 # Annex B. Examples

OpenC2 commands and responses need to be transmitted with certain relevant head information (i.e., metadata), as described in Section 3.2 of [OpenC2-Lang-v1.0]**.** When sending OpenC2 commands and responses over HTTP/TLS, the OpenC2 message elements are handled as described in Table 4-1.

A Request-URI ending in `/openc2` is used in all example HTTP requests.

B.1 HTTP Request / Response Examples: Consumer as HTTP Server

This section presents the HTTP message structures used when the OpenC2 Consumer acts as the HTTP listener.

B.1.1 Producer HTTP POST with OpenC2 Command

Example message:

```
```
POST /openc2 HTTP/1.1
Host: oc2consumer.company.net
Content-type: application/openc2-cmd+json;version=1.0
Date: Day, DD Mon YYYY HH:MM:SS GMT
X-Correlation-ID: shq5x2dmgayf

{
      "action": ...
      "target": …
      "args": ...
}
```
```

B.1.2 Consumer HTTP Response with OpenC2 Response

Example message:

```
```
HTTP/1.1 200 OK
Date: Day, DD Mon YYYY HH:MM:SS GMT
Content-type: application/openc2-rsp+json;version=1.0
X-Correlation-ID: shq5x2dmgayf

{
      "id_ref": ...
      "status": 200
      "status_text": ...
      "results": { ...
```
```

```
}
```

B.2 HTTP Request / Response Examples: Producer as HTTP Server

This section presents the HTTP message structures used when the OpenC2 Producer acts as the HTTP listener.

B.2.1 Consumer Polls Producer with HTTP GET

Consumers use the HTTP GET method to poll a Producer for available commands and status queries. No message body is required.

```
GET /openc2 HTTP/1.1
Host: oc2producer.company.net
Accept: application/openc2-cmd+json;version=1.0
Cache-control: no-cache
Date: Day, DD Mon YYYY HH:MM:SS GMT

```

B.2.2 Producer HTTP Response with OpenC2 Command

If the Producer has commands for the Consumer, the Producer returns HTTP 200, Success and places an OpenC2 message with a command body in the body of the HTTP response. This signals the Consumer to process the command, send an HTTP POST with its OpenC2 response message, and then poll again for additional messages from the Producer.

```
HTTP/1.1 200 OK
Date: Day, DD Mon YYYY HH:MM:SS GMT
Content-type: application/openc2-cmd+json;version=1.0
X-Correlation-ID: bf5t2ttrsc8r

{
      "action": ...
      "target": ...
      "actuator": ...
      "args": ...
}
```

B.2.3 Producer HTTP Response with OpenC2 Status Query

If the Producer has status queries for the Consumer, the Producer returns HTTP 200, Success and places an OpenC2 message with a command to query status in the body of the HTTP response. The `id` in the OpenC2 message header identifies the command for which updated status is requested. This signals the Consumer to process the status query, send an HTTP POST

with its OpenC2 response message, and then poll again for additional messages from the Producer.

```
HTTP/1.1 200 OK
Date: Day, DD Mon YYYY HH:MM:SS GMT
Content-type: application/openc2-cmd+json;version=1.0
X-Correlation-ID: bf5t2ttrsc8r

{
      "action": "query"
      "target": "command"
}
```

B.2.4 Producer HTTP Response with No Content

If the Producer has no commands or status queries for the Consumer, the Producer returns HTTP 204, No Content. This signals the Consumer to return to its default polling interval.

```
HTTP/1.1 204 OK
Date: Day, DD Mon YYYY HH:MM:SS GMT

```

B.2.5 Consumer HTTP POST with OpenC2 Response

Consumers use the HTTP POST method to send OpenC2 response messages to the Producer.

```
POST /openc2 HTTP/1.1
Host: oc2producer.company.net
Content-type: application/openc2-rsp+json;version=1.0
Date: Day, DD Mon YYYY HH:MM:SS GMT
X-Correlation-ID: bf5t2ttrsc8r

{
      "id_ref": ...
      "status": 200
      "status_text": ...
      "results": { …
      }
}
```

7 # Annex C. Acknowledgments

The Implementation Considerations Subcommittee was tasked by the OASIS Open Command and Control Technical Committee (OpenC2 TC) which at the time of this submission, had 132 members. The editor wishes to express their gratitude to the members of the OpenC2 TC.

The following individuals are acknowledged for providing comments, suggested text, and/or participation in CSD ballots or face-to-face meetings:

- Michelle Barry, AT&T
- Brian Berliner, Symantec
- Joe Brule, National Security Agency
- Trey Darley, New Context Services, Inc.
- David Darnell, Systrends
- Travis Farral, Anomali
- Andy Gray, ForeScout
- John-Mark Gurney, New Context Services, Inc.
- Pavel Gutin, G2, Inc.
- David Hamilton, AT&T
- April Jackson, Praxis Engineering
- Sridhar Jayanthi, Polylogyx LLC
- Bret Jordan, Symantec
- Takahiro Kakumaru, NEC Corporation
- David Kemp, National Security Agency
- Lauri Korts-Pärn, NECAM
- Anthony Librera, AT&T
- Danny Martinez, G2, Inc.
- Lisa Mathews, National Security Agency
- Jim Meck, Fireeye
- Efrain Ortiz, Symantec Corp.
- Daniel Riedel, New Context Services, Inc.
- Nirmal Rajarathnam, ForeScout
- Chris Ricard, FS-ISAC
- Jason Romano, National Security Agency
- Philip Royer, Splunk Inc.
- Duane Skeen, Northrop Grumman
- Duncan Sparrell, sFractal Consulting LLC
- Michael Stair, AT&T
- Andrew Storms, New Context Services, Inc.
- Gerald Stueve, Forenetix
- Allan Thomson, LookingGlass Cyber Solutions
- Bill Trost, AT&T
- Ryan Trost, ThreatQuotient

690 - Drew Varner, NineFX
691 - Jason Webb, LookingGlass Cyber Solutions
692 - Sounil Yu, Bank of America
693 - David Webber, Huawei

694 # 8 # Annex D. Revision History

Revision	Date	Editor	Changes Made
v1.0-wd01-wip	6/15/2018	Lemire	Initial working draft
v1.0-wd01-wip	6/29/2018	Lemire	Added Suitability section (1.6), responded to SC member comments
v1.0-wd01-wip	7/20/2018	Lemire	Additional responses to member comments; formatting clean-up for easier conversion to Markdown.
v1.0-wd01-wip	8/9/2018	Lemire	Implementing feedback from the July 2018 face-to-face meeting and resolving other comments to reach WD01 version to submit for CSD ballot.
v1.0-wd02-wip	8/24/2018	Lemire	Various edits to clarify interactions when the producer is HTTP listener; other edits and cleanup in response to document comments and Slack forum discussions.
v1.0-wd02-wip	8/29/2018	Lemire	1) Adjustments to content type definitions to distinguish commands and responses; 2) Made corresponding adjustments to message flow descriptions and sample messages. 3) Added acknowledgements.
v1.0-wd02-wip	8/30/2018	Lemire	Inserted proposed replacements for sequence diagrams (Figures 2 and 3).
v1.0-wd02-wip	8/31/2018	Lemire	1) Inserted initial draft conformance language (section 4). 2) Revised Section 1 content for greater consistency with related OpenC2 specifications. 3) Revised section 2.1 to merge proposed endpoint role descriptions 4) General edit for formatting, readability, consistency, etc.
v1.0-wd02-wip	9/11/2018	Lemire	1) Reviewed and accepted / rejected comments. 2) Added placeholders for addressing use of "From" field. 3) Added statements about using Cache-

			control
v1.0-wd02-wip	9/17/2018	Lemire	1) Added table to conformance section specifying mapping of Language Spec message elements. 2) Clarified certificate mutual authentication requirement. 3) Removed language about unsolicited responses from Consumers 4) Numbered the conformance items
v1.0-wd02-wip	9/17/2018	Lemire	1) Removed used of the HTTP "From:" field, and mapped the OpenC2 "from" message element to the authenticated identity of the peer entity 2) Updated examples to remove HTTP From:
v1.0-wd02-wip	9/19/2018	Lemire	1) Final clean-up of residual comments and edits to create WD02 package for CSD ballot. 2) Renamed document to WD03-wip
v1.0-wd03-wip	10/15/2018	Lemire	1) Reorganized section 1 to align with other OpenC2 specifications 2) Reworded section 3.2.1 to properly use MUST / SHALL language 3) Clarified requirements wording section 3.2.3 to better indicate TLS version requirements and preferences, and authentication requirements. 4) Updated Table 4-1 to align with changes to Language Specification Table 3-1.
v1.0-wd03-wip	10/16/2018	Lemire	1) Final clean-up of residual edits to create WD03 package for CSD approval and release for public review.

695