

**OCF “Gaborone-1” – List of Auditable Events – Security WG CR 3150**

Legal Disclaimer

THIS IS A DRAFT SPECIFICATION DOCUMENT ONLY AND HAS NOT BEEN ADOPTED BY THE OPEN CONNECTIVITY FOUNDATION. THIS DRAFT DOCUMENT MAY NOT BE RELIED UPON FOR ANY PURPOSE OTHER THAN REVIEW OF THE CURRENT STATE OF THE DEVELOPMENT OF THIS DRAFT DOCUMENT. THE OPEN CONNECTIVITY FOUNDATION AND ITS MEMBERS RESERVE THE RIGHT WITHOUT NOTICE TO YOU TO CHANGE ANY OR ALL PORTIONS HEREOF, DELETE PORTIONS HEREOF, MAKE ADDITIONS HERETO, DISCARD THIS DRAFT DOCUMENT IN ITS ENTIRETY OR OTHERWISE MODIFY THIS DRAFT DOCUMENT AT ANY TIME. YOU SHOULD NOT AND MAY NOT RELY UPON THIS DRAFT DOCUMENT IN ANY WAY, INCLUDING BUT NOT LIMITED TO THE DEVELOPMENT OF ANY PRODUCTS OR SERVICES. IMPLEMENTATION OF THIS DRAFT DOCUMENT IS DONE AT YOUR OWN RISK AMEND AND IT IS NOT SUBJECT TO ANY LICENSING GRANTS OR COMMITMENTS UNDER THE OPEN CONNECTIVITY FOUNDATION INTELLECTUAL PROPERTY RIGHTS POLICY OR OTHERWISE. IN CONSIDERATION OF THE OPEN CONNECTIVITY FOUNDATION GRANTING YOU ACCESS TO THIS DRAFT DOCUMENT, YOU DO HEREBY WAIVE ANY AND ALL CLAIMS ASSOCIATED HERewith INCLUDING BUT NOT LIMITED TO THOSE CLAIMS DISCUSSED BELOW, AS WELL AS CLAIMS OF DETRIMENTAL RELIANCE.

The OCF logo is a trademark of Open Connectivity Foundation, Inc. in the United States or other countries. \*Other names and brands may be claimed as the property of others.

Copyright © 2020 Open Connectivity Foundation, Inc. All rights reserved.

Copying or other form of reproduction and/or distribution of these works are strictly prohibited.

### 13.20 List of Auditable Events

Whenever a Device detects an occurrence of any of the Auditable Events in Table XX, then the Device **shall** log an AEE using the corresponding "category", "priority" and "auxiliaryinfo" Properties defined in Table XX. The "auxiliaryinfo" Property **shall** contain the entries in the "auxiliaryinfo" column of Table XX in the order specified in the table with each bullet contained in a separate array entry. The "auxiliaryinfo" Property **may** contain additional entries for further information following the entries for mandatory information. The "aeid" Property shall include the corresponding Auditable Event Identifier from Table XX.

**Table XX List of mandatory Auditable Events and corresponding Property values**

Auditable Event Identifier ("aeid")	Auditable Event Description	Example "message"	"category"	"priority"	"auxiliaryinfo"
<b>AC-1</b>	A Device received a request from an authenticated Client with valid URI path, valid interface and valid operation for that resource, but for which access was denied.	"Access Denied"	0x01 (Access Control)	2 (WARN)	<ul style="list-style-type: none"> <li>Client IP address &amp; port in format [xxxx:...xxxx]:xxxx</li> <li>Client UUID in UUID format (e.g. "00000000-0000-0000-0000-000000000000")</li> <li>Resource URI (e.g. "/oic/sec/ael")</li> <li>Requested CRUDN operation (e.g. "CREATE")</li> <li>Server security state (e.g. "RFNOP")</li> <li>Asserted roles by Client (e.g. "oic.role.owner"), or "No roles asserted" if there are none</li> </ul>
<b>AUTH-1</b>	The Device encountered an error during a DTLS handshaking procedure due to a credential validation failure.	"DTLS handshake failed due to a credential validation failure"	0x08 (Authentication)	1 (ERR)	<ul style="list-style-type: none"> <li>Client IP address &amp; port in format [xxxx:...xxxx]:xxxx</li> </ul>
<b>COMM-1</b>	The Device received a CoAP request which contained unexpected /unsupported CoAP header parameters or unexpected/unsupported CoAP options.	"Unexpected CoAP Command"	0x40 (COMM)	2 (WARN)	<ul style="list-style-type: none"> <li>Client IP address &amp; port in format [xxxx:...xxxx]:xxxx</li> <li>Hex-encoded CoAP header in format [xx:xx:xx:xx]</li> <li>Hex-encoded CoAP options except payload (empty if not present)</li> </ul>

Whenever a Device detects an occurrence of any of the Auditable Events in Table YY, then the Device **should** log an AEE using the corresponding "category", "priority" and "auxiliaryinfo" Properties defined in Table YY. The "auxiliaryinfo" Property **shall** contain the entries in the "auxiliaryinfo" column of Table YY in the order specified in the table with each bullet contained in a separate array entry. The "auxiliaryinfo" Property **may** contain additional entries for further information following the entries for mandatory information. The "aeid" Property shall include the corresponding Auditable Event Identifier from Table YY.

**Table YY List of recommended Auditable Events and corresponding Property values**

Auditable Event	Auditable Event Description	Example "message"	"category"	"priority"	"auxiliaryinfo"
-----------------	-----------------------------	-------------------	------------	------------	-----------------

Identifier					
<b>SVR-1</b>	The Device's attempted to use one of its credentials, and detected that the credential is expired	"My credential is expired"	0x10 (SVR Modification)	2 (WARN)	<ul style="list-style-type: none"> <li>• credid</li> <li>• Credential expiration value</li> </ul>
<b>SVR-2</b>	The Device could not validate the role certificate being asserted	"Role assertion failed"	0x10 (SVR Modification)	2 (WARN)	<ul style="list-style-type: none"> <li>• Client IP address &amp; port in format [xxxx:...:xxxx]:xxxx</li> </ul>

DRAFT