OCF “Gaborone-1” – New Resource Type for Event Logging – Security WG CR 3149

Legal Disclaimer

13.1 Security Resources General

The "/oic/sec/ael" Resource and its Properties are shown in Figure 30.

Figure 27 – OCF Security Resources

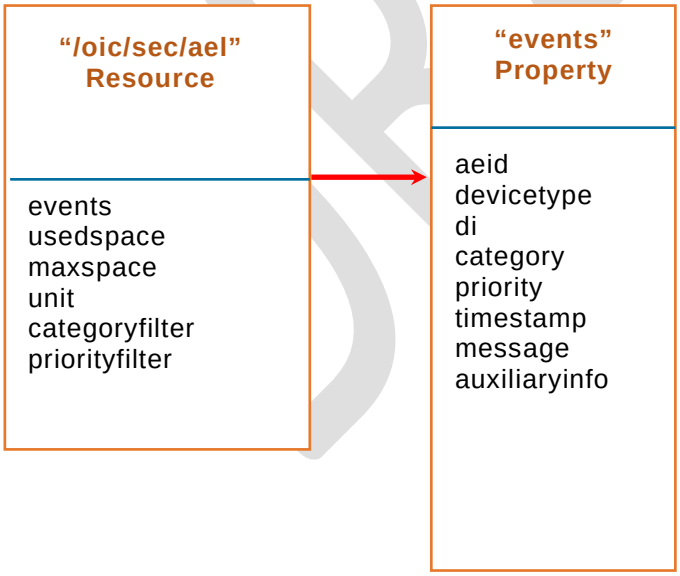

Figure 30 – "/oic/sec/ael" Resource and Properties

....

13.11 Auditable Events List Resource

13.11.1 Auditable Events List Resource General

The "/oic/sec/ael" Resource maintains a list of logged Auditable Events. Every OCF Device logs AEEs filtered according to the values of the "categoryfilter" and "priorityfilter" Properties of "/oic/sec/ael" Resource. All Devices shall have a "/oic/sec/ael" Resource to maintain AEEs. The new AEE shall be added to the "events" Property of "/oic/sec/ael" Resource as the last entry in the array. A Device shall store all AEEs of the "/oic/sec/ael" Resource in non-volatile memory. A Device shall be able to store at least 1 AEE.

The "categoryfilter" Property determines what categories of AEEs are to be logged. The "categoryfilter" Property is an integer value which is a composition of bitmasks. A Device shall log all AEEs filtered by this value. If the "categoryfilter" is either set to 0xff or is not set, then the Device shall log AEEs of all categories. Refer to Table 2 for more details.

The "priorityfilter" Property determines the lowest priority of AEE to be logged. A smaller value means higher priority. The AEEs whose "priority" Property values are equal to or smaller than this value shall be logged. If the "priorityfilter" Property is either set to the highest priority or is not set, then the Device shall log all AEEs. No matter what value is set to "priorityfilter", an AEE of CRIT (== 0) "priority" shall always be logged. Refer to Table 2 for more details.

When an AEE is added, the "usedspace" Property shall be updated to reflect the total storage used by all logged events. When the reserved storage for AEEs is full, the oldest AEE shall be purged.

A Device logs a new AEE as follows:

1) If a new AEE is not filtered by "categoryfilter" and "priorityfilter", then it is dropped.

```
/* c-like pseudo code */
If ((categoryfilter & new_aee->category) && (priorityfilter >=
new_aee->priority))
{
    addAEE(new_aee);
}
else
{
    free(new_aee);
}
```

2) If the value of "usedspace" Property is equal to, or the sum of the "usedspace" Property value and the size of the new AEE is bigger than the value of the "maxspace" Property of "/oic/sec/ael" Resource, then:

   a) Remove the oldest AEE continuously while the sum of the "usedspace" Property value and the size of the new AEE is bigger than the "maxspace" Property value.

```
/* c-like pseudo code */
Int addAEE(AEEtype *new_aee)
{

    While ((usespace + new_aee->size) > maxspace)
    {
        /* purgeAEE() returns the size of purged AEE */
        sizeOfPurgedAEE = purgeAEE();
        usedspace -= sizeOfPurgedAEE;
```

```
        }

        ...
        ...
    }
```

3) Add the new AEE to the "events" array Property of the "/oic/sec/ael" Resource as the last entry in the array.

4) Increase the value of the "usedspace" Property by the size of the new AEE.

In order to provide a mechanism which allows management of the "events" array Property, the RETRIEVE and UPDATE operations on the "/oic/sec/ael" Resource shall behave as follows:

1) A RETRIEVE operation shall return the full Resource representation.

2) An UPDATE operation may set the "categoryfilter" and/or "priorityfilter" Properties.

The "/oic/sec/ael" Resource is defined in Table 1.

Table 1 – Definition of the "/oic/sec/ael" Resource

Fixed URI	Resource Type Title	Resource Type ID ("rt" value)	OCF Interfaces	Description	Related Functional Interaction
/oic/sec/ael	Auditable Event List	oic.r.ael	oic.if.baseline, oic.if.rw	Resource for storing AEEs	Security

Table 2 defines the Properties of the "/oic/sec/ael" Resource.

Table 2 – Properties of the "/oic/sec/ael" Resource

Property Title	Property Name	Value Type	Value Rule	Mandatory	Device State	Access Mode	Description
AEE list	"events"	"array"	Array of "oic.sec.aee" entries	Yes	RESET	R	The Device clears
					RFOTM	R	This list stores AEEs whose "category" Property value is filtered by "categoryfilter" Property and "priority" Property value is equal or less than the value of "priorityfilter" Property.
					RFPRO		
					RFNOP		
					SRESET		
current used storage size	"usedspace"	"integer"	>= 0 (default: 0)	Yes	RESET	R	The Device sets to 0
					RFOTM	R	Current used space for logged AEEs. The Device updates this Property whenever new AEEs are logged.
					RFPRO		
					RFNOP		
					SRESET		
maximum allowed storage size for AEEs	"maxspace"	"integer"	> 0	Yes		R	This means the maximum allowable storage size for AEEs that can be stored in "events" list. The Manufacturer chooses this value.

unit for storage size	"unit"	"string"	enum ["Kbyte", "Byte"] (default: “Byte”)	No		R	The unit for "usedspace" and "maxspace" Properties. The Manufacturer chooses this value.
Categories of AEE to be logged	"categoryfilter"	"integer"	bitmask (default: 0xff)	No	RESET	R	The Device sets to the manufacturer default value
					RFOTM	RW	This value decides what categories of AEEs are to be logged. Meaning of each bit: • 0x01 (Access Control) • 0x02 (Onboarding) • 0x04 (Device) • 0x08 (Authentication) • 0x10 (SVR Modification) • 0x20 (Cloud) • 0x40 (Communication) • 0x80 (Reserved) e.g.) if "categoryfilter" == 0xff: log all events of all categories e.g.) if "categoryfilter" == 0x03: log all events of 'AC (== 0x01)' and 'OB (==0x02)' categories
					RFPRO		
					RFNOP	R	
					SRESET	RW	
Minimum priority of AEEs to be logged	"priorityfilter"	"integer"	enum [0, 1, 2, 3, 4] (default: 4)	No	RESET	R	Device sets to manufacturer default value
					RFOTM	RW	The AEEs whose "priority" values are equal to or smaller than this value are logged. A smaller value means a higher priority. Meaning of each value: • 0 (CRIT) • 1 (ERR) • 2 (WARN) • 3 (INFO) • 4 (DEBUG) e.g.) if "priorityfilter" is set to DEBUG (==4) all AEEs will be logged e.g.) if "priorityfilter" is set to 1, CRIT (==0) and ERR (==1) SEEs will be logged
					RFPRO		
					RFNOP	R	
					SRESET	RW	

Table 3 defines the Properties of the "oic.sec.aee" type.

Table 3 – "oic.sec.aee" data type definition

Property Title	Property Name	Value Type	Value Rule	Access Mode	Mandatory	Device State	Description
Auditable Event Identifier	"aeid"	“string”	N/A	R	Yes	-	Identity of the logged event
Value of "rt"	"devicetype"	"array"	Array of strings	R	No	-	The "rt" value of "/oic/d" of the Server which logged this AEE.
Device ID	"di"	"uuid"	N/A	R	No	-	The Device ID of the Server which logged this AEE.
Category of AEE	"category"	"integer"	enum [1, 2, 4, 8, 16, 32, 64, 128]	R	Yes	-	The category of this AEE: • 0x01 (Access Control) • 0x02 (Onboarding) • 0x04 (Device) • 0x08 (Authentication) • 0x10 (SVR Modification) • 0x20 (Cloud) • 0x40 (Communication) • 0x80 (Reserved)
Priority of AEE	"priority"	"integer"	enum [0, 1, 2, 3, 4]	R	Yes	-	The priority of this AEE: • 0 (CRIT) • 1 (ERR) • 2 (WARN) • 3 (INFO) • 4 (DEBUG)
Time stamp	"timestamp"	"string"	date-time (RFC3339 section 5.6)	R	Yes	-	The time when the AEE occured
Event message	"message"	"string"	N/A	R	No	-	The description of the logged AEE.
Auxiliary info	"auxiliaryinfo"	"array"	Array of strings	R	No	-	Supplementary information for the "message" Property e.g.) URI of specific Resource in ACE2

OCF-defined AEEs are listed in Table XX, and each such AEE has its own values for the "category" and "priority" Properties.

The "timestamp" Property follows a full-date and partial-time format of RFC3339. Every new AEE shall have a later timestamp than the latest previously logged AEE.

The "auxiliaryinfo" Property provides supplementary info which is not covered by the description in "message" Property. For example, the URI of specific Resource in ACE2 could be "auxiliaryinfo" for "Access Denied" AEE. Please see Table XX "List of Auditable Events".