|  |
| --- |
| i |

|  |  |
| --- | --- |
| CHANGE REQUEST | |
| Meeting ID:\* | SDS #49 |
| Source:\* | Andreas Kraft, DT, [Andreas.Kraft@t-systems.com](mailto:Andreas.Kraft@t-systems.com)  Andreas Neubacher, DT, [Andreas.Neubacher@magenta.at](mailto:Andreas.Neubacher@magenta.at) |
| Date:\* | 2021-01-07 |
| Reason for Change/s:\* | Editorial corrections for TS-0001 |
| CR against: Release\* | Release 4 |
| CR against: WI\* | Active WI-xxxx  MNT maintenance / < Work Item number(optional)>  Is this a mirror CR? Yes  No  mirror CR number: (Note to Rapporteur - use latest agreed revision)  STE Small Technical Enhancements / < Work Item number (optional)>  Only ONE of the above shall be ticked |
| CR against: TS/TR\* | TS-0001, V4.8.0 |
| Clauses \* | 9.6.1.3.2, 9.6.2.4, 9.6.24, 9.6.43 |
| Type of change: \* | Editorial change  Bug Fix or Correction  Change to existing feature or functionality  New feature or functionality  Only ONE of the above shall be ticked |
| Impacted other TS/TR(s) |  |
| Post Freeze checking:\* | This CR contains only essential changes and corrections? YES  NO  This CR may break backwards compatibility with the last approved version of the TS? YES  NO |
| Template Version: January 2017 (Do not modify) | |

**oneM2M Notice**

The document to which this cover statement is attached is submitted to oneM2M. Participation in, or attendance at, any activity of oneM2M, constitutes acceptance of and agreement to be bound by terms of the Working Procedures and the Partnership Agreement, including the Intellectual Property Rights (IPR) Principles Governing oneM2M Work found in Annex 1 of the Partnership Agreement.

GUIDELINES for Change Requests:

Provide an informative introduction containing the problem(s) being solved, and a summary list of proposals.

Each CR should contain changes related to only one particular issue/problem.

In case of a correction, and the change apply to previous releases, a separate “mirror CR” should be posted at the same time of this CR

Mirror CR: applies only when the text, including clause numbering are exactly the same.

Companion CR: applies when the change means the same but the baselines differ in some way (e.g. clause number).

Follow the principle of completeness, where all changes related to the issue or problem within a deliverable are simultaneously proposed to be made E.g. A change impacting 5 tables should not only include a proposal to change only 3 tables. Includes any changes to references, definitions, and acronyms in the same deliverable.

Follow the drafting rules.

All pictures must be editable.

Check spelling and grammar to the extent practicable.

Use Change bars for modifications.

The change should include the current and surrounding clauses to clearly show where a change is located and to provide technical context of the proposed change. Additions of complete clauses need not show surrounding clauses as long as the proposed clause number clearly shows where the new clause is proposed to be located.

Multiple changes in a single CR shall be clearly separated by horizontal lines with embedded text such as, start of change 1, end of change 1, start of new clause, end of new clause.

When subsequent changes are made to content of a CR, then the accepted version should not show changes over changes. The accepted version of the CR should only show changes relative to the baseline approved text.

Introduction

This CR proposes a couple of editorial corrections for TS-0001.

Change 1 - 3 : The attribute “owner” was renamed “holder”, but the attribute is still named “owner” in various places. This is corrected in these changes.

Change 4: in “Table 9.6.2.4-1: Types of Parameters in accessControlObjectDetails” the attribute “specialization” should be named “specializationType”. This would then be consistent with, for example, the definition in TS-0004, “Table 6.3.5.27 1: Type Definition of m2m:accessControlRule”. This is corrected in this change.

Change 5: in “Table 9.6.2.2-1: Types of Parameters in accessControlContexts” the attribute “accessControlIpAddress” should be named “accessControlIpAddresses”. This would then be consistent with, for example, the definition in TS-0004, “Table 6.3.5.27 1: Type Definition of m2m:accessControlRule”. This is corrected in this change.

### \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of Change 1 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

##### 9.6.1.3.2 Common attributes

The following attributes are commonly used in multiple, but not all, resource types which are normal, not virtual or announced. Common attributes for announced resource types are independently defined in clause 9.6.26.3.

NOTE: The list of attributes in table 9.6.1.3.2-1 is not exhaustive.

Table 9.6.1.3.2-1: Common Attributes

| Attribute Name | Description |
| --- | --- |
| *accessControlPolicyIDs* | The attribute contains a list of identifiers for *<accessControlPolicy>* resources. The privileges defined in the *<accessControlPolicy>* resources that are referenced determine who is allowed to access the resource containing this attribute for a specific purpose (e.g. Retrieve, Update, Delete, etc.).  For an Update operation to a resource, it is forbidden to change the *accessControlPolicyIDs* attribute in the same request to Update other attributes of the targeted resource, i.e a request to Update the *accessControlPolicyIDs* attribute shall be the only attribute in the UPDATE request.  To update the *accessControlPolicyIDs* attribute, a Hosting CSE shall check whether the Originator has Update privilege in any current *selfPrivileges* of the *<accessControlPolicy>* resources which this attribute references.  To update any attribute other than the *accessControlPolicyIDs* attribute, a Hosting CSE shall check whether the Originator has Update privilege in any *privileges,* of the *<accessControlPolicy>* resources which the *accessControlPolicyIDs* attribute references.  If a resource type does not have an *accessControlPolicyIDs* attribute definition, then the *accessControlPolicyIDs* for that resource is governed in a different way, for example, the *accessControlPolicy* associated with the parent may apply to a child resource that does not have an *accessControlPolicyIDs* attribute definition, or the privileges for access are fixed by the system. Refer to the corresponding resource type definitions and procedures to see how access control is handled in such cases.  If a resource type does have an *accessControlPolicyIDs* attribute definition, but the (optional) *accessControlPolicyIDs* attribute value is not set in a resource instance, then the Hosting CSE shall apply the concept of the default access policy. The Hosting CSE shall first check whether the resource has an *holder* attribute configured and if so, the default policy shall provide unrestricted access only to the holder. If the *holder* attribute is not configured, then the default policy shall provide unrestricted access only to the Originator of the successful resource creation request. All other entities shall be denied to access the resource. For that purpose, the Hosting CSE shall keep that Originator information of the resource. Note that how to keep that information is implementation specific. The default access policy is not applied to a resource which has a value assigned to the a*ccessControlPolicyIDs* attribute.  All resources are accessible if and only if the privileges (i.e. configured as *privileges* or *selfPrivileges* attribute of <accessControlPolicy> resource) allow it, therefore all resources shall have an associated *accessControlPolicyIDs* attribute, either explicitly (setting the attribute in the resource itself) or implicitly (either by using the parent privileges or the system default policies). Which means that the system shall provide default access privileges in case that the Originator does not provide a specific *accessControlPolicyIDs* during the creation of the resource. |
| *expirationTime* | Time/date after which the resource will be deleted by the Hosting CSE. This attribute can be provided by the Originator, and in such a case it will be regarded as a hint to the Hosting CSE on the lifetime of the resource. The Hosting CSE shall configure the *expirationTime* value. If the Hosting CSE configures the new *expirationTime* attribute value rather than the Originator suggested value, the new value can be sent back to the Originator depending on the ***Result Content*** value.  The lifetime of the resource can be extended by providing a new value for this attribute in an UPDATE operation. Or by deleting the attribute value, e.g. by updating the attribute with NULL when doing a full UPDATE, in which case the Hosting CSE can decide on a new value.  If the Originator does not provide a value in the CREATE operation the system shall assign an appropriate value depending on its local policies and/or M2M service subscription agreements.  A resource is known as 'obsolete' when the resource contains the attribute "expirationTime" and the lifetime of this resource has reached the value of this attribute. If the ‘obsolete’ resource had a reference to an Application Entity Resource ID, the Hosting CSE shall send a NOTIFY request to the IN-CSE, requesting to delete the entry from the <AEContactList> resource. |
| *stateTag* | An incremental counter of modification on the resource. When a resource is created, this counter is set to 0, and it will be incremented on every modification of the resource (see notes 1 and 2). |
| *announceTo* | This attribute may be included in a CREATE or UPDATE Request in which case it contains a list of addresses/CSE-IDs where the resource is to be announced. For the case that CSE-IDs are provided, the announced-to CSE shall decide the location of the announced resources based on the rules described in clause 9.6.26.  For the original resource, this attribute shall only be present if it has been successfully announced to other CSEs. This attribute maintains the list of the resource addresses to the successfully announced resources. Updates on this attribute will trigger new resource announcement or de-announcement.  If the *announceTo* attribute includes resource address(s), the present document does not provide any means for validating these address(s) for announcement purposes. It is the responsibility of the Hosting-CSE referenced by the resource address(s) to validate the access privileges of the originator of the Request that triggers the announcement. |
| *announcedAttribute* | This attributes shall only be present at the original resource if some Optional Announced **(OA)** type attributes have been announced to other CSEs. This attribute maintains the list of the announced Optional Attributes (**OA** type attributes) in the original resource. Updates to this attribute will trigger new attribute announcement if a new attribute is added or de-announcement if the existing attribute is removed. |
| *announceSyncType* | This attribute indicates the types of synchronization for resource announcement. Possible values are as follows:   * Uni-directional synchronization: Announced resource(s) is updated if the original resource is updated * Bi-directional synchronization: Announced resource(s) is updated if the original resource is updated and vice versa   This attribute is presented in both the original resource and the announced resource(s).  The absence of this attribute implies that uni-directional synchronization is the type of supported synchronization for resource announcement. |
| *labels* | Tokens used to add meta-information to resources.  This attribute is optional.  The value of the *labels* attribute is a list of individual labels, each of them being:   * Either a standalone label-key, used as a simple "tag", that can be used for example for discovery purposes when looking for particular resources that one can "tag" using that label-key * Or a composite element made of a label-key and a label-value, separated by a special character defined in [3].   The list of allowed characters in a label (and in label-keys and label-values) and separator characters is defined in [3], clause 6.3.3. |
| *e2eSecInfo* | Present in a resource representing an AE or CSE. Indicates the end-to-end security capabilities supported by the AE or CSE. May indicate supported end-to-end security frameworks. May also contains a certificate or credential identifier used by the AE or CSE. May include random values for use in end-to-end security protocols. The details of this attributes are described in oneM2M TS-0003 [2].  This attribute is optional and if not present it means that the represented entity does not support oneM2M end-to-end security procedures. |
| *dynamicAuthorizationConsultationIDs* | This attribute contains a list of identifiers of *<dynamicAuthorizationConsultation>* resources. The information defined in a *<dynamicAuthorizationConsultation>* resource is used by a CSE for initiating consultation-based dynamic authorization requests.  Consultation-based dynamic authorization is only performed for a targeted resource if and only if it is linked to an enabled *<dynamicAuthorizationConsultation>* resource.  If the attribute is not set or has a value that does not correspond to a valid *<dynamicAuthorizationConsultation>* resource(s), or it refers to an *<dynamicAuthorizationConsultation>* resource(s) that is not reachable, then the *dynamicAuthorizationConsultationIDs* associated with the parent may apply to the child resource if present, or a system default *<dynamicAuthorizationConsultation>* may apply if present. |
| *creator* | The AE-ID or CSE-ID of the entity which created the resource containing this attribute. |
| *location* | This attribute contains the geo-coordinates of entities or things represented by its resource types (e.g. AE, container). Longitude and Latitude are shall be included as a coordinate and optionally altitude may also be included. The representation format shall follow the definition in the GeoJSON format [16]. This attribute can be used for geo-query (Clause 10.2.6) with relevant filter conditions (Clause 8.1.2). |
| *resourceMappingRules* | This attribute contains a list of rules for mapping the resource and/or its attributes on a Registrar CSE to one or more corresponding resources/attributes hosted by a Registree AE. Each mapping rule contains various information elements as defined in table 9.6.1.3.2.1-1.  The mapping rule information stored in this attribute enables a Registrar CSE to receive a request from an Originator that targets the local resource hosted by the Registrar CSE and retarget this request to a Registree AE for processing. Once the Registree AE finishes processing the retargeted request and returns a response, the Registrar CSE uses the mapping rule information contained in this attribute to update the local resource with the contents of the response and to formulate a response that it returns back to the request Originator.  This attribute is applicable to a subset of content sharing resources (i.e. <container>, <flexContainer> and <timeSeries>) and the <mgmtObj> resource. |
| *holder* | The AE-ID, M2M-User-ID or CSE-ID of the entity which owns the resource containing this attribute. |
| NOTE 1: In order to enable detection of overflow, the counter needs to be capable of expressing sufficiently long numbers.  NOTE 2: This attribute has the scope to allow identifying changes in resources within a time interval that is lower than the one supported by the attribute *lastModifiedTime* (e.g. less than a second or millisecond). This attribute can also be used to avoid race conditions in case of competing modifications. | |

### \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of Change 1 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of Change 2 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 9.6.24 Resource Type *eventConfig*

*<eventConfig>* sub-resource shall be used to define events that trigger statistics collection. Below are some examples of events that can be generated:

* Collection based on a certain operation: collects any RETRIEVE operations on the data (i.e. resources) stored in the IN-CSE.
* Collection based on storage size: collects the size of storage when a "Content Sharing Resource" stored in the IN-CSE exceeds a quota.
* Combined configuration: collects all RETRIEVE operations on the data stored in the IN-CSE during a period of time.

The *<eventConfig>* resource shall contain the child resource specified in table 9.6.24-1.

Table 9.6.24-1: Child resources of *<eventConfig>* resource

| Child Resources of *<eventConfig>* | Child Resource Type | Multiplicity | Description |
| --- | --- | --- | --- |
| *[variable]* | *<subscription>* | 0..n | See clause 9.6.8 where this type of resource is described. |
| *[variable]* | *<transaction>* | 0..n | See clause 9.6.48 |

The *<eventConfig>* resource shall contain the attributes specified in table 9.6.24-2.

Table 9.6.24-2: Attributes of *<eventConfig>* resource

| Attributes of *<eventConfig>* | Multiplicity | RW/  RO/  WO | Description |
| --- | --- | --- | --- |
| *resourceType* | 1 | RO | See clause 9.6.1.3. |
| *resourceID* | 1 | RO | See clause 9.6.1.3. |
| *resourceName* | 1 | WO | See clause 9.6.1.3. |
| *parentID* | 1 | RO | See clause 9.6.1.3. |
| *accessControlPolicyIDs* | 0..1 (L) | RW | See clause 9.6.1.3. |
| *creationTime* | 1 | RO | See clause 9.6.1.3. |
| *expirationTime* | 1 | RW | See clause 9.6.1.3. |
| *lastModifiedTime* | 1 | RO | See clause 9.6.1.3. |
| *labels* | 0..1 (L) | RW | See clause 9.6.1.3. |
| *dynamicAuthorizationConsultationIDs* | 0..1 (L) | RW | See clause 9.6.1.3. |
| *creator* | 0..1 | RO | See clause 9.6.1.3. |
| *holder* | 0..1 | RW | See clause 9.6.1.3. |
| *eventID* | 1 | RO | This attribute uniquely identifies the event to be collected for statistics for AEs. |
| *eventType* | 1 | RW | This attribute indicates the type of the event: timer based, data operation, or storage based. |
| *eventStart* | 0..1 | RW | This attribute indicates the start time of the event. |
| *eventEnd* | 0..1 | RW | This attribute indicates the end time of the event |
| *operationType* | 0..1 (L) | RW | This attribute defines the type of the operation to be collected by statistics, such as CREATE, RETRIEVE. |
| *dataSize* | 0..1 | RW | This attribute defines the data size that will trigger a storage based event. For <container> and <timeSeries> *currentByteSize* is compared. For <contentInstance>, <flexContainer>, <timeSeriesInstance> *contentSize* is compared. An event is triggered when the compared data size exceeds *dataSize* size. |
| *eventResourceTypes* | 0..1 (L) | RW | This attribute indicates the list of resource types for which an event is to be captured and reported. This could be used to differentiate the same operation on different types of resources that triggers the charging activity. If this attribute is specified, then *eventResourceIDs* shall not be specified. |
| *eventResourceIDs* | 0..1 (L) | RW | This attribute indicates the list of resourceIDs for which the event is to be captured and reported. Whenever an operation is performed on the resourceIDs in this list, an event will be recorded provided other event criteria are met such as eventResourceType, locationRestriction and the event information based on the type of event. If this attribute is specified, then *eventResourceTypes* shall not be specified. |
| *eventResourceHolders* | 0..1 (L) | RW | This attribute indicates the list of resource *holders* for which the event is to be captured and reported. Whenever an operation is performed on a resource having an *holder* attribute that matches an AE-ID, M2M-User-ID or CSE-ID specified in this list, an event will be recorded, provided any other specified event criteria have also been met. |

### \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of Change 2 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of Change 3 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 9.6.43 Resource Type *authorizationInformation*

The <*authorizationInformation*> resource represents an access control information retrieval point that is responsible for retrieving access control information. <*authorizationInformation*> resources are the child resources of a <*CSEBase*> resource. When an UPDATE request addresses an <*authorizationInformation*> resource, the Hosting CSE acts as a Policy Information Point (PIP) as defined in TS-0003 [2]. The PIP shall retrieve the required access control information according to the access control information request and provide the access control information in the UPDATE response.

The resource specific attributes and child resources of <*authorizationInformation*> resource type are classed into two categories according to their usage. The <*role*> and <*token*> resources and *status* attribute are used for describing access control information responses. The others are used for describing access control information requests.

An access control information request shall be provided to a PIP through an UPDATE operation on an <*authorizationInformation*> resource that represents the PIP, and the updated resource attributes shall be the attributes used for describing access control information request parameters. The mandatory and optional parameters used for describing an access control information request are specified in oneM2M TS-0003 [2]. When an UPDATE request that represents a valid access control information request addresses an <*authorizationInformation*> resource, the PIP procedure bound to the <*authorizationInformation*> resource shall be triggered. The PIP procedure shall retrieve required access control information and then create corresponding <*role*> and/or <*token*> child resources and/or update *status* attributes. The <*role*> and/or <*token*> child resources and/or *status* attributes that represents an access control information response shall be returned to the requester in the UPDATE response. An UPDATE request that does not represent a valid access control information request shall not trigger the bound PIP procedure. Before triggering a PIP procedure, accessing an <*authorizationInformation*> resource is governed by the access control policies assigned to this resource.

For the lifecycle management of <*authorizationInformation*> resources, see oneM2M TS-0003 [2].

The <*authorizationInformation*> resource shall contain the child resources specified in table 9.6.43-1.

Table 9.6.43-1: Child resources of <*authorizationInformation*> resource

| Child Resources of *<role>* | Child Resource Type | Multiplicity | Description |
| --- | --- | --- | --- |
| *[variable]* | *<role>* | 0..n | See clause 9.6.38 |
| *[variable]* | *<token>* | 0..n | See clause 9.6.39 |
| *[variable]* | *<subscription>* | 0..n | See clause 9.6.8 |
| *[variable]* | *<transaction>* | 0..n | See clause 9.6.48 |

The <*authorizationInformation*> resource shall contain the attributes specified in table 9.6.43-2

Table 9.6.43-2: Attributes of *<authorizationInformation>* resource

| Attributes of *<role>* | Multiplicity | RW/  RO/  WO | Description |
| --- | --- | --- | --- |
| *resourceType* | 1 | RO | See clause 9.6.1.3. |
| *resourceID* | 1 | RO | See clause 9.6.1.3. |
| *resourceName* | 1 | WO | See clause 9.6.1.3. |
| *parentID* | 1 | RO | See clause 9.6.1.3. |
| *expirationTime* | 1 | RW | See clause 9.6.1.3. |
| *accessControlPolicyIDs* | 0..1 (L) | RW | See clause 9.6.1.3. |
| *dynamicAuthorizationConsultationIDs* | 0..1 (L) | RW | See clause 9.6.1.3. |
| *holder* | 0..1 | RW | See clause 9.6.1.3. |
| *creationTime* | 1 | RO | See clause 9.6.1.3. |
| *labels* | 0..1 (L) | RW | See clause 9.6.1.3. |
| *lastModifiedTime* | 1 | RO | See clause 9.6.1.3. |
| *status* | 0..1 | RO | Status of retrieving access control information. See clause 7 in oneM2M TS-0003 [2]. |
| *from* | 0..1 | RW | Same as the *From* parameter in the request. See clause 7 in oneM2M TS-0003 [2]. |
| *roleIDs* | 0..1 (L) | RW | Same as the *Role IDs* parameter in the request. See clause 7 in oneM2M TS-0003 [2]. |
| *tokenIDs* | 0..1 (L) | RW | Same as the *Token IDs* parameter in the request. See clause 7 in oneM2M TS-0003 [2]. |

### \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of Change 3 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of Change 4 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

#### 9.6.2.4 accessControlObjectDetails

The *accessControlObjectDetails* is an optional parameter of an access control rule. It specifies a subset of child resource types of the targeted resource to which the access control rule applies. If an access control rule includes *accessControlObjectDetails*, then *childResourceType* shall be specified. An access control rule which does not include any *accessControlObjectDetails* parameters applies to the child resource types of the target resource. The *accessControlObjectDetails* parameter shall consist of the elements listed in table 9.6.2.4-1. Child resource types listed in the *childResourceType* component are subject of access control for the Create operation only. Once a child resource is created, the Access Control Policies assigned directly to it apply. The *resourceType* and *specializationType* element are optional. If either the *resourceType* or *specializationType* element is present in *accessControlObjectDetails*, the CSE shall match the type of resource or specialization of the targeted resource with the value specified in the *resourceType* or *specializationType* element. Further checking of *childResourceType* shall be done only if the *resourceType* or *specializationType* match occurs. However, if the *resourceType* and *specializationType* elements are not provided, only *childResourceType* match shall be performed.

Table 9.6.2.4-1: Types of Parameters in *accessControlObjectDetails*

| **Name** | **Description** |
| --- | --- |
| *resourceType* | Identifier of the resource type to which this access control rule applies |
| *specializationType* | When the *resourceType* is *mgmtObj* or *flexContainer*, the identifier of the specialization as defined by *mgmtDefinition* or *containerDefinition* attribute, respectively, shall be specified. |
| *childResourceType* | List of child resource types and/or the identifier of the specialization. The identifier of the specialization shall be specified when the *resourceType* is *mgmtObj* or *flexContainer*. |

### \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of Change 4 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of Change 5 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

#### 9.6.2.2 *accessControlContexts*

The *accessControlContexts* is an optional parameter in an access-control-rule-tuple that contains a list, where each element of the list, when present, represents a context that is permitted to use this access control rule. Each request context is described by a set of parameters, where the types of the parameters can vary within the set. Table 9.6.2.2-1 describes the supported types of parameters in *accessControlContexts*.

The following Originator *accessControlContexts* shall be considered for access control policy check by the CSE.

Table 9.6.2.2-1: Types of Parameters in *accessControlContexts*

| Name | Description |
| --- | --- |
| *accessControlTimeWindow* | Represents a time window constraint which is compared against the time that the request is received at the Hosting CSE. |
| *accessControlLocationRegion* | Represents a location region constraint which is compared against the location of the Originator of the request. |
| *accessControlIPAddresses* | Represents an IP address constraint or IP address block constraint which is compared against the IP address of the Originator of the request. |
| *accessControlUserIDs* | Represents a M2M Service User constraint which is compared against the ***M2M Service User*** parameter of the request. |
| *accessControlEvalCriteria* | This attribute provides the conditions determining if the request *operation* is to be allowed. It allows conditional access to the resource based on conditions not contained in the received request. The *accessControlEvalCriteria* parameter consists of a mandatory *subjectResourceID* attribute as defined in table 9.6.61-2 and the *evalCriteria* attribute described in table 9.6.61-3. NOTE: this uses the same definitions that are present in the <action> resource, but does not use the <action> resource. |
| *accessControlLimit* | Represents the number of times that the policy defined in this accessControlRule can allow authorization to the requested resource. This attribute maintains of the number of authorizations granted based on this policy. This value is decremented each time the evaluation grants access to the requested resource. If this value is greater than zero (0) then the request operation is allowed. If the *accessControlLimit* parameter is not present then the request operation is allowed (unlimited access). |

### \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of Change 5 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*