OCF "Essen" – ACEs for Created Resources – Security WG CR 2827

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 © 2019 Open Connectivity Foundation, Inc. All rights reserved.

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

DRAFT

****** Changes to clause 12.2.7.1 ******

12.2.7.1 ACE2 matching algorithm

The OCF Server shall apply an ACE2 matching algorithm that matches in the following sequence:

1) If the "/oic/sec/sacl" Resource exists and if the signature verification is successful, these ACE2 entries contribute to the set of local ACE2 entries in step 3. The Server shall verify the signature, at least once, following update of the "/oic/sec/sacl" Resource.
1) The local "/oic/sec/acl2" Resource contributes its ACE2 entries for matching.
2) Access shall be granted when all these criteria are met:
   a) The requestor is matched by the ACE2 "subject" Property.
   b) The requested Resource is matched by the ACE2 resources Property and the requested Resource shall exist on the local Server.
   c) The "period" Property constraint shall be satisfied.
   d) The "permission" Property constraint shall be applied.

If multiple ACE2 entries match the Resource request, the union of permissions, for all matching ACEs, defines the *effective* permission granted. E.g. If Perm1=CR---; Perm2=--UDN; Then UNION (Perm1, Perm2)=CRUDN.

The Server shall enforce access based on the effective permissions granted.

Batch requests to Resource containing Links require additional considerations when accessing the linked Resources. ACL considerations for batch request to the Atomic Measurement Resource Type are provided in clause 12.2.7.2. ACL considerations for batch request to the Collection Resource Type are provided in clause 12.2.7.3.

Clause 12.2.7.4 provides ACL considerations when a new Resource is created on a Server in response to a CREATE request.

****** End of Change ******

****** New clause 12.2.7.4 ******

12.2.7.4 ACL Considerations on creation of a new Resource

When a new Resource is created on a Server in response to a CREATE request, there might be no ACEs permitting access to the newly created Resource. The present clause describes how the Server autonomously modifies the "/oic/sec/acl2" Resource to provide some initial authorizations for accessing the newly created Resource. The purpose of this autonomous modification is to avoid relying on the AMS update the "/oic/sec/acl2" Resource after every new Resource is created.

Subsequent to a Server creating a Collection inside another Collection in response to a CREATE request from a Client, and prior to sending a response to the Client:

- If there is an ACE with “subject” containing the UUID of the Client, and “permissions” exactly matching the CREATE, RETRIEVE, UPDATE and DELETE operations, then the Server shall autonomously add an “href” entry to “resources” with the URI of the newly created Collection.

DRAFT

- Otherwise, the Server shall autonomously add an ACE with “subject” containing the UUID of the Client, “resources” containing an “href” entry with the URI of the newly created Collection, and “permissions” exactly matching the CREATE, RETRIEVE, UPDATE and DELETE operations.

Subsequent to a Server creating a non-Collection Resource inside another Collection in response to a CREATE request from a Client, and prior to sending a response to the Client:

- If there is an ACE with “subject” containing the UUID of the Client, and “permissions” exactly matching the RETRIEVE, UPDATE and DELETE operations, then the Server shall autonomously add an “href” entry to “resources” with the URI of the newly created Resource.

- Otherwise, the Server shall autonomously add an ACE with “subject” containing the UUID of the Client, “resources” containing an “href” entry with the URI of the newly created, and “permissions” exactly matching the RETRIEVE, UPDATE and DELETE operations.

****** End of Change ******

DRAFT