OCF 2.3 – Access control for batch interface requests to an OCF Collection Resource – remote references – Sec WG CR 2286/2332

****** Change to Section 5.1 ******

5.1 Access Control

The OCF framework assumes that Resources are hosted by a Server and are made available to Clients subject to access control and authorization mechanisms. The Resources at the end point are protected through implementation of access control, authentication and confidentiality protection. This section provides an overview of Access Control (AC) through the use of ACLs. However, AC in the OCF stack is expected to be transport and connectivity abstraction layer agnostic.

Implementation of access control relies on a-priori definition of a set of access policies for the Resource. The policies may be stored by a local ACL or an Access Management Service (AMS) in form of Access Control Entries (ACE). Two types of access control mechanisms can be applied:

- Subject-based access control (SBAC), where each ACE will match a subject (e.g. identity of requestor) of the requesting entity against the subject included in the policy defined for Resource. Asserting the identity of the requestor requires an authentication process.
- Role-based Access Control (RBAC), where each ACE will match a role identifier included in the policy for the Resource to a role identifier associated with the requestor

Some Resources, such as Collections, generate requests to linked Resources when appropriate Interfaces are used. In such cases, additional access control considerations are necessary. Additional access control considerations for Collections when using the batch OCF Interface are found in Section 12.6.3.

In the OCF access control model, access to a Resource instance requires an associated ACE. The lack of such an associated ACE results in the Resource being inaccessible.

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

****** Changes to Sections 12.2.6.2 and 12.2.6.3 ******

12.2.6.2 VOID

This section is intentionally left blank.

12.2.6.3 ACL considerations for a batch OCF Interface request to a Collection

This section addresses the additional authorization processes which take place when a Server receives a batch OCF Interface request from a Client to a Collection hosted on that Server, assuming there is an ACE matching the Collection which permits the original Client request. For the purposes of this section, the Server hosting this Collection is called the "Collection host". The additional authorization process is dependent on whether the linked Resource is hosted on the Collection host or the linked Resource is hosted on another Server:

- For each generated request to a linked Resource hosted on the Collection host, the Collection host shall apply the ACE2 matching algorithm in Section 12.2.6.1 to determine whether the linked Resource is permitted to process the generated request, with the following clarifications:
    - The requestor in Section 12.2.6.1 shall be the Client which sent the original Client request.
    - The requested Resource in Section 12.2.6.1shall be the linked Resource, which shall be matched using at least one of
        - a Resource Wildcard matching the linked Resource, or
        - an exact match of the local path of the linked Resource with a "href" Property in the "resources" array in the ACE2.
        - an exact match of the full URI of the linked Resource with a "href" Property in the "resources" array in the ACE2.

      NOTE: The full URI of a linked Resource is obtained by concatenating the "anchor" Property of the Link, if present, and the "href" Property of the Link. The local path can then be determined form the full URI.

  If the linked Resource is not permitted to process the generated request, then the Collection host shall treat such cases as a linked Resource which cannot process the request when composing the aggregated response to the original Client Request, as specified for the batch OCF Interface in the OCF Core Specification.

- For each generated request to a linked Resource hosted on another Server, the Collection host shall apply the ACE2 matching algorithm in Section 12.2.6.1 to determine whether sending the generated request to the OCF Server hosting the linked Resource is permitted, with the following clarifications:

- The requestor in Section 12.2.6.1 is the Client which sent the original Client request.
- The requested Resource is the linked Resource, which is matched using an exact match of the full URI of the linked Resource with a "href" Property in the "resources" array in the ACE2.

If sending the generated request is permitted and the Collection Host can establish a secure connection with the Server hosting the linked Resource, then the Collection Host shall send the generated request to that Server over the established secure connection.

If sending the generated request is not permitted, then the Collection Host shall not send the generated request to the Server hosting the linked Resource. When composing the aggregated response to the original Client Request, the Collection Host shall treat such cases as linked Resources which cannot process the request, as specified for the batch OCF Interface in the OCF Core Specification.

NOTE: As with ACE2 entries for Resources hosted on the Collection host, the AMS of the Collection Host configures the ACE2 entries to the Collection host for Resources hosted on another Server. There are no restrictions on the ACE2 entries which can be configured to the Collection host for Resources hosted on another Server. The AMS can configure ACE2 entries to the Collection host which are equally permissive as the ACE2 entries on the other Server, or which are more permissive than the ACE2 entries on the other Server or which are more restrictive than the ACE2 entries on the other Server. The choice is left to the person or organization controlling the AMS.

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