CDNI Metadata Interface
## (draft-ma-cdni-metadata-01)

Kevin J. Ma

kevin.ma@azukisystems.com

CDNI Metadata Requirements

- Metadata Push (META-3, META-4)
- Metadata Modify/Remove (META-7, META-8)
- Hierarchical Metadata and Metadata Grouping (META-9, META-10, META-11, META-12)
- CDNI Defined Metadata (META-15)
  - Content Acquisition (META-5, META-6)
  - Delivery Restrictions (META-14)
  - Request Authorization (META-17)
- Opaque Metadata (META-16)
- Metadata Rejection (META-13)

Data Model and API
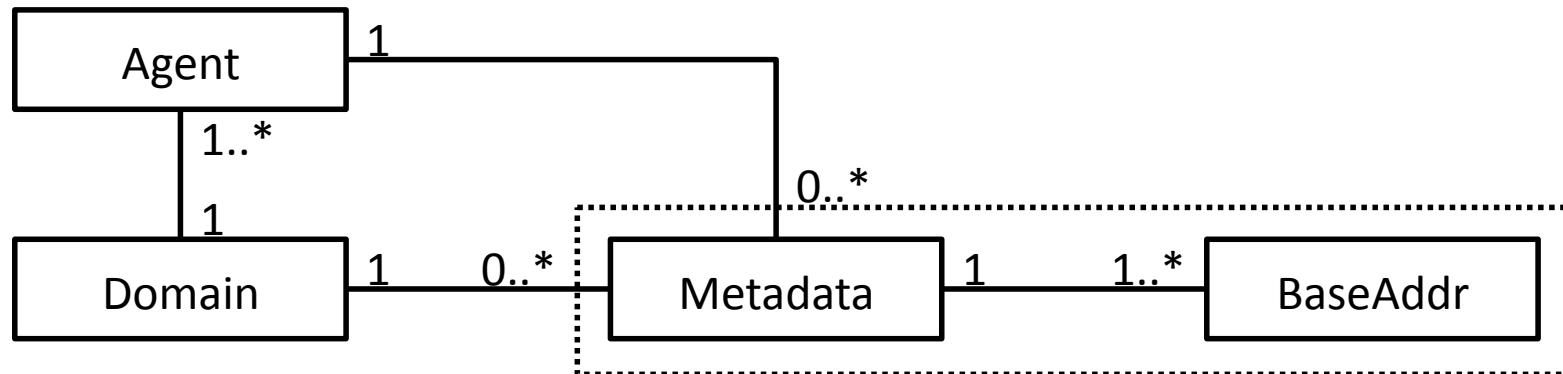
- Domain create/modify (POST), retrieval (GET), and removal (DELETE)
  - Domains provide information about and group Agents and Metadata.
- Agent create/modify (POST), retrieval (GET), and removal (DELETE)
  - Agents provide basic access control differentiation for Metadata.
- Metadata create/modify (POST), retrieval (GET), and removal (value="")
  - Metadata is stored as opaque name/value pairs, grouped by URI.
  - Metadata is indexed by domain, agent, and URL (BaseAddr + URI).
  - Metadata has a flag to force rejection of metadata that cannot be enforced.
  - Metadata values support any semantic representation.
  - Metadata is removed by clearing the value field.

Opaque Metadata Distribution

- Opaque representation in the data model provides support for both well-known and unknown metadata which may be encountered:
  - Opaque distribution does not prevent specifying rich semantics; nor does it increase complexity or workload for specifying individual metadata semantics; Opaque representation in the data model simply adds a layer of abstraction.
  - Opaque distribution supports extensibility for future metadata.
- Opaque representation in the data model separates metadata semantics from basic elements of generic metadata distribution:
  - Name/Value: The semantics of the metadata contained in 'value' are associated with the metadata 'name', but independent of the URI, Mandatory Flag, and TTL which apply to all metadata objects.
  - BaseAddr/URI: Metadata is associated with request URIs and BaseAddrs. URI wildcards define hierarchical sets of content.
  - Mandatory Flag: Handling of unenforceable metadata must be deterministic. The mandatory flag specifies when to reject unknown and/or unsupported metadata (i.e., mandatory metadata must either be enforced or rejected).
  - TTL: Metadata may be automatically invalidated via an optional TTL.

Opaque Metadata Examples

- Some metadata may only require simple string values:
  - Acquisition Base URL
    - `<value>http://origin.csp.com/</value>`
  - Content Activation Time:
    - `<value>2011-11-16T01:00:00.00Z</value>`
  - Content Deactivation Time:
    - `<value>2011-11-16T03:30:00.00Z</value>`
- Other metadata may require more complex object representations:
  - URL Hash:
    - ```
      <value>
          <hash_param_name>h</hash_param_name>
          <timestamp_param_name>e</timestamp_param_name>
          <timeout>5000</timeout>
          <timestamp_format>epoch</timestamp_format>
          <shared_secret>XXX</shared_secret>
          <secret_position>prepend</secret_position>
          <hash_algorithm>md5</hash_algorithm>
      </value>
      ```

Metadata Interface Security

- Attacks against the metadata interface poses risks to content delivery:
  - Inability to retrieve content acquisition metadata, or the altering of content acquisition metadata may prevent content acquisition and delivery.
  - Inability to distribute security metadata, or the altering of security metadata may allow content to be delivered insecurely or otherwise violate distribution licensing or media rights.
  - Insertion of bogus request filters or other mandatory metadata may prevent content delivery.
  - Insertion of bogus mandatory metadata may prevent request delegation.
  - Impersonation of a dCDN may allow unauthorized access to content.
- Spoofing of valid CDNs may be prevented using mutual authentication or host filtering, however, segregation of metadata between multiple valid dCDNs requires association of authentication credentials with metadata.
  - The agent associated with each metadata object provides this abstraction.
  - Only metadata intended for the requesting agent should be returned.
  - Only agents with proper credentials should be able to modify metadata.
  - Need to verify agent name relationship to authentication credentials.

Next Steps: WG Feedback

- There are multiple metadata interface drafts currently being discussed:
  - draft-ma-cdni-metadata focuses on the distribution aspects of the metadata interface.
  - draft-ma-cdni-metadata includes some basic metadata definitions, but does not contain the level of detail wrt core metadata as draft-caulfield-cdni-metadata-core or draft-jenkins-cdni-metadata.
  - Metadata distribution and the definition of core metadata are both important complementary components of the metadata interface.
- Questions for the Working Group:
  - Does the WG feel that this proposal meets the needs as defined in the requirements document and/or are those requirements sufficient?
  - Does the WG feel that there is merit in continuing to work on this particular proposal?
  - Does the WG feel that there are any particular aspects of this proposal that should be pursued and/or should be abandoned?