**Threat Modeling of Keystone Credential Service**

**1.1 System Overview**

|  |  |
| --- | --- |
| Application version | Keystone Havana Stable Release |
| Application  Description | The Keystone Credential Service falls under the Identity service. [**http://api.openstack.org/api-ref-identity.html**](http://api.openstack.org/api-ref-identity.html)  This document is in continuation with the Threat Modeling of Keystone Identity and Assignment Driver. |
| Document Version | 0.1 |
| Participants |  |
| Additional Info |  |

**1.2 Implementation Overview**

|  |  |
| --- | --- |
| Major Components | Keystone Credential Controller.  Credential Drivers (example SQL) |
| Dependent components | Keystone Policy Engine. |
| Description |  |

**1.3 System Assumptions (External Dependencies)**

|  |  |
| --- | --- |
| **ID** | **Description** |
| 1 | The default driver for Keystone Credential Service is SQL. |
| 2 | The path for policy.json file is rightly configured in the Keystone configuration file. In addition, it can be enforced. |

**2. Security Objective**

|  |  |
| --- | --- |
| 1. | Provide authentic CRUD operation for Credential Services. |

**3.1 Data Flow Diagrams**

**Credential API:** [**http://api.openstack.org/api-ref-identity.html**](http://api.openstack.org/api-ref-identity.html)

**I. CREDENTIAL OPERATIONS:**

**Context: Credential Related Operations**

**API: version 3**

**Controller: Controllers.CredentialV3()**

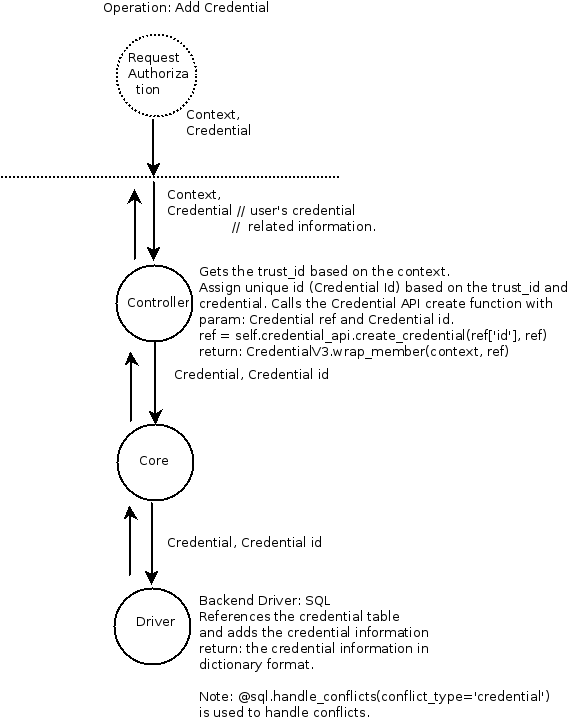
**1. Create Credentials:**

**Request Type: POST v3/credentials**

**Operation: Adds a Credential**

**Normal Response Code: 201**

**DFD:**

****

**2. Update Credentials:**

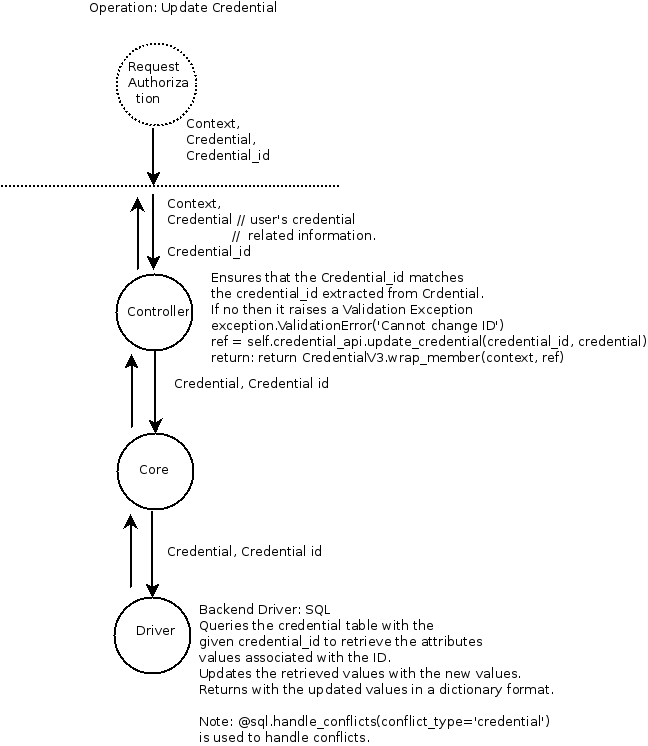
**Request Type: PATCH v3/credentials/ {credential\_id}**

**Operation: Updates a specified credential.**

**Normal Response Code: 200**

**NOTE: This operation does not require a request body.**

**DFD:**

****

**3. Delete Credentials:**

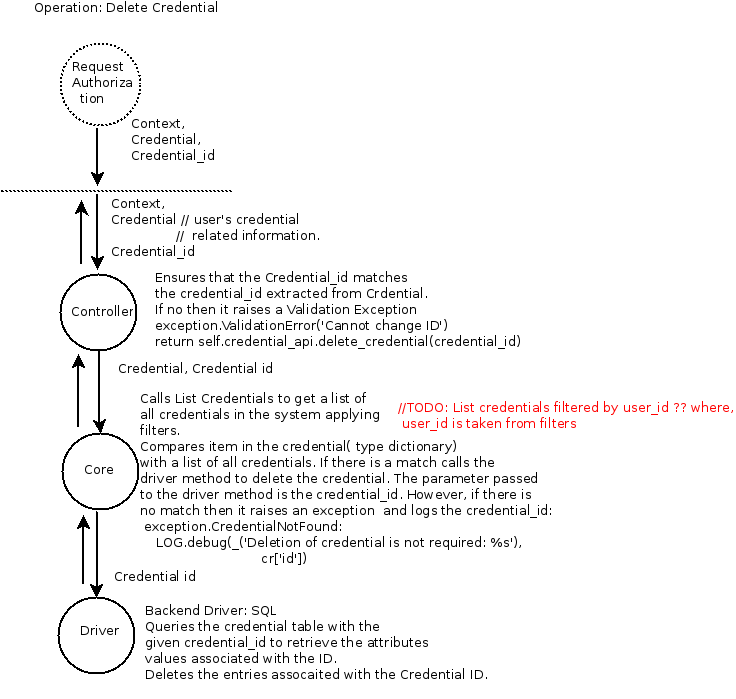
**Request Type: DELETE v3/credentials/ {credential\_id}**

**Operation: Deletes a specified credential.**

**Normal Response Code: 204**

**NOTE: This operation does not require a request body and does not return a response body.**

**DFD:**



**3.2 Entry points**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Name** | **Description** | **Accessible To** |
| 1 | Public port | SSL protected port, used to access the keystone server. External requests come and return through this port. Default 5000. If you plan to use SSL proxy, it could be different. |  |
| 4 | Interface towards persistence layer | Keystone server communicates with database backend. We only consider MySQL server. |  |

**3.3 Assets**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Name** | **Details** | **Accessible To** |
| 9. | Credentials (creds) | Includes:  Access key  Secret Key  User ID  Project ID  Type (example EC2) |  |
| 9.1 | Credential ID | ID of a specific credential. |  |

**3.4 (Existing Security Controls)**

**Not Done**

**4. Threat Identification and Analysis**

**// TODO:**