**Threat Modeling of Trust (Keystone)**

**1.1 System Overview**

|  |  |
| --- | --- |
| Application version | Keystone Havana Stable Release |
| Application  Description | Trust provides project specific role delegation – i.e., a trustor delegates some roles on a project to the trustee. The trustee acquires the roles of the trustor for the specified amount of time defined in trust. Optionally, it allows impersonation – i.e., trustee takes the user\_id of the trustor. Trust is consumed by creating a token scoped under trust\_id. A trust\_token cannot be used to create another trust\_token.  https://github.com/openstack/identity-api/blob/master/openstack-identity-api/v3/src/markdown/identity-api-v3-os-trust-ext.md |
| Version | Havana Stable |
| Participants |  |
| Additional Info |  |

**1.2 Implementation Overview**

|  |  |
| --- | --- |
| Major Components | Trust/routers – routing of HTTP call  Trust/controller – associated controller for a HTTP call  Trust/core – stub/logic for backend  Trust/backends/sql - backend implementation  Trust/backends/kvs - backend |
| Dependent components | Token api  Identity api |
| Description |  |

**1.3 System Assumptions (External Dependencies)**

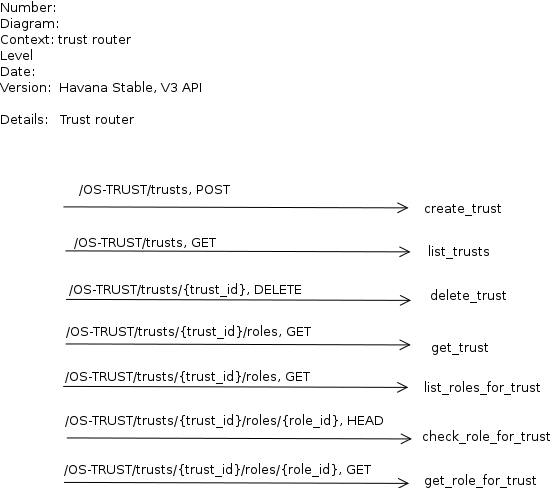
|  |  |
| --- | --- |
| **ID** | **Description** |
| 1 | Trust for V3 API is only considered |
| 2 |  |
| 3 |  |

**2. Security Objective**

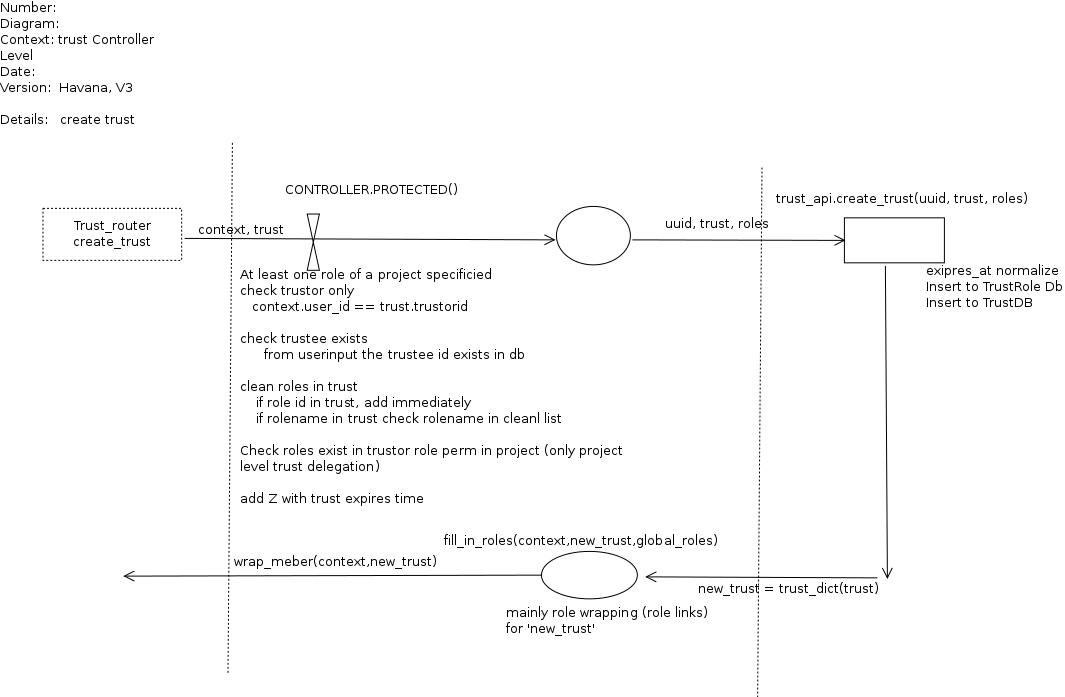
|  |  |
| --- | --- |
| System Security objective | 1. Delegated access (role) to resources (Project) |

**3. 1 Data Flow Diagrams**

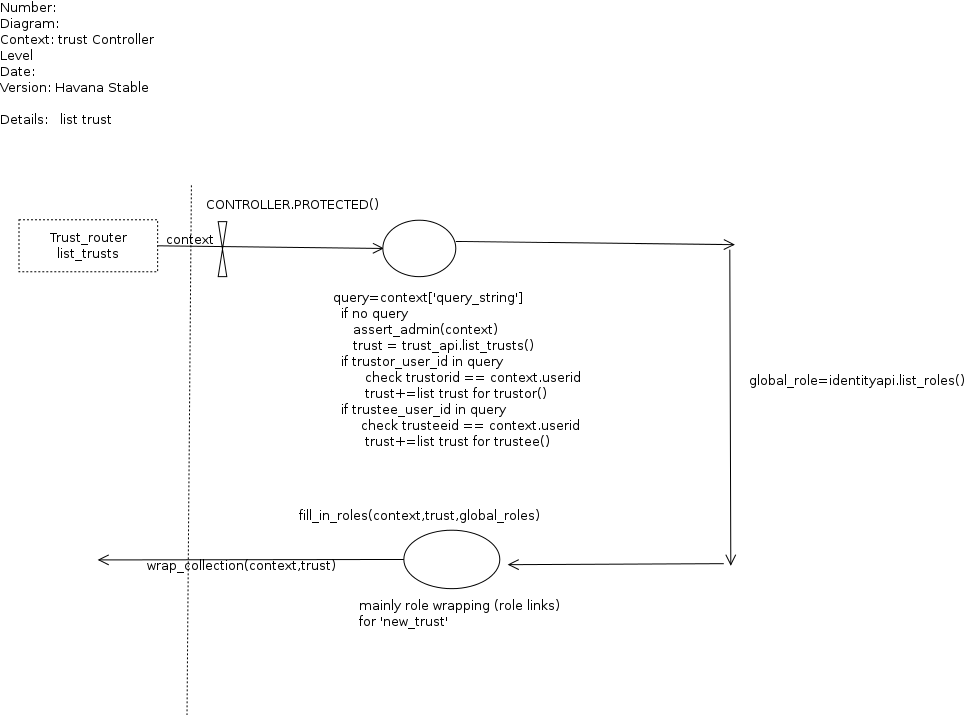
**TRUST ROUTER:**

****

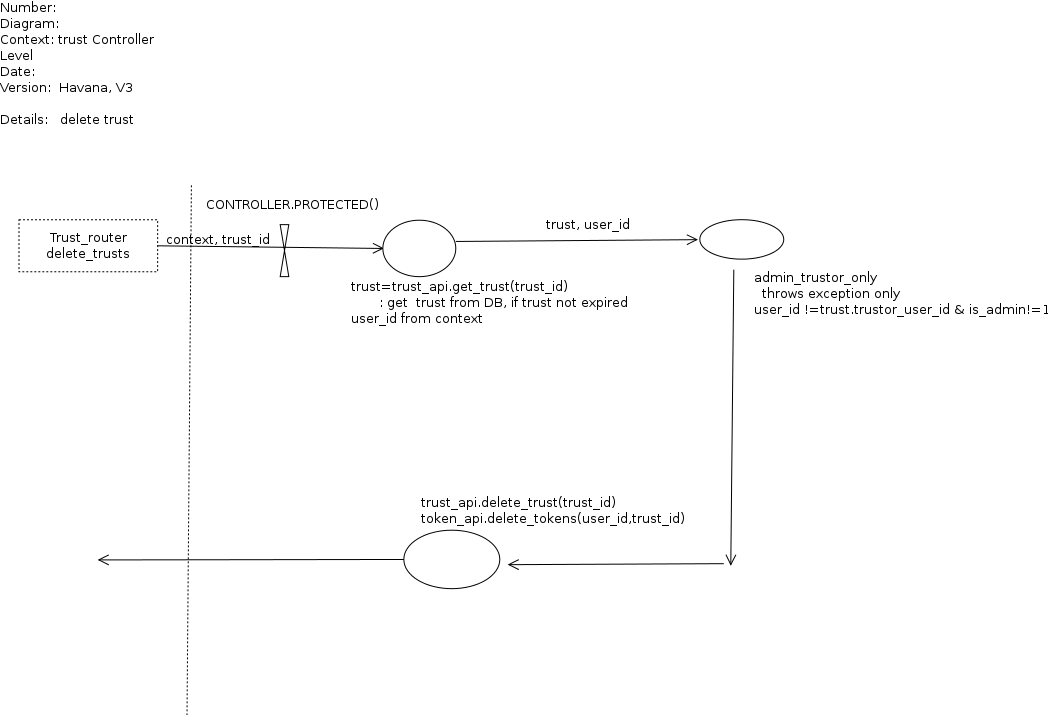
**CREATE TRUST:**

****

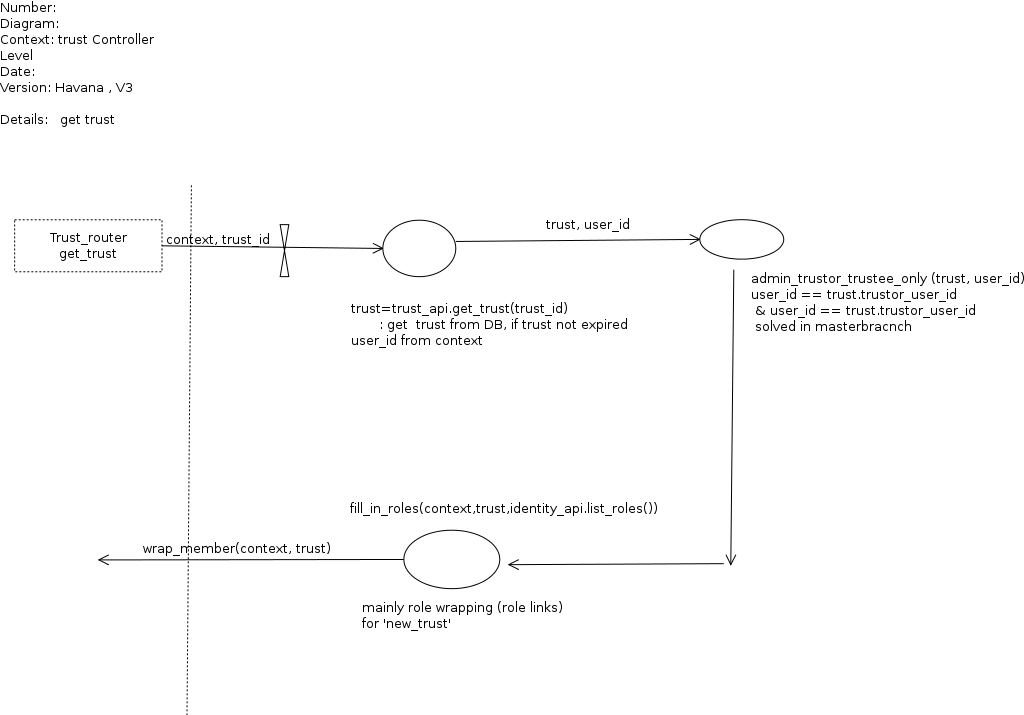
**LIST TRUST**

****

**DELETE TRUST**



GET TRUST



**3.2 Entry points**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Name** | **Description** | **Accessible To** |
|  | Public port |  |  |

**3.3 Assets**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Name** | **Details** | | **Required Trust Levels** |
| 1 | User | | Assets related to a user |  |
| 1.2 | User details | | Information related to a user e.g., email, |  |
| 1.4 | Project | |  |  |
| 1.4.1 | User to Project relation | |  |  |
| 1.6 | User-Project-Role relation | |  |  |
| 1.8 | Trust  Trust\_id  Trustor  Trustee | |  |  |
|  |  | |  |  |
|  |  | |  |  |
|  |  | |  |  |
| 2 | System | | Assets related to configuration and system |  |
| 2.1 | Audit data | |  | 7) System admin  11) Keystone Process user |
| 2.4 | Availability of keystone service | |  | 4) Keystone Identity Admin  7) System admin |
| 2.5 | Access & execute Query in DB | |  | 8) DB User |
| 2.6 | Configuration parameter set | |  | 7) System admin  11) Keystone Process user |
| 2.9 | UUID generator | |  | 7) System admin  4) Keystone Identity Admin |
| 2.10 | Authorization policy management within keystone | | Management of which user can access what (entitlement rules) i.e., policy definition file | 4) Keystone Identity Admin  7) System admin  11) Keystone Process user |
|  |  | |  |  |
| 3. | Web Application | | Dashboard to access Keystone service |  |
| 3.1 | Login session | |  | 9) Authenticated user  10) Dashboard Admin |

**3.4 (Existing Security Controls)**

**Not Done**

**4. Threat Identification and Analysis**

**Result-**

[**Link to Excel Sheet**](https://drive.google.com/file/d/0B1aEVfmQtqnobWFfTEZQTmZQZU0/edit?usp=sharing)