**Threat Modeling of ….(Keystone)**

**1.1 System Overview**

|  |  |
| --- | --- |
| Application version | Keystone Havana Stable Release |
| Application  Description |  |
| Version | Havana Stable |
| Participants |  |
| Additional Info |  |

**1.2 Implementation Overview**

|  |  |
| --- | --- |
| Major Components |  |
| Dependent components |  |
| Description |  |

**1.3 System Assumptions (External Dependencies)**

|  |  |
| --- | --- |
| **ID** | **Description** |
| 1 |  |
| 2 |  |
| 3 |  |

**2. Security Objective**

|  |  |
| --- | --- |
| System Security objective |  |

**3. 1 Data Flow Diagrams**

**3.2 Entry points**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Name** | **Description** | **Accessible To** |
|  |  |  |  |
| 2 |  |  |  |

**3.3 Assets**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Name** | **Details** | | **Required Trust Levels** |
| 1 | User | | Assets related to a user |  |
| 1.1 | User auth credentials | |  | 9) User  7) System Admin |
| 1.1.1 | Tenant Admin auth credentials | |  | 3) Tenant admin  4) Keystone Identity Admin  7) System admin  8) DB User |
| 1.1.2 | Keystone Identity admin auth credentials | |  | 4) Keystone Identity Admin  7) System admin  8) DB User |
| 1.2 | User details | | Information related to a user e.g., email, |  |
| 1.4 | Project | |  |  |
| 1.4.1 | User to Project relation | |  |  |
| 1.5 | Group | |  |  |
| 1.5.1 | User to Group relation | |  |  |
| 1.6 | User-Project-Role relation | |  |  |
| 1.7 | domain | |  |  |
| 1.7.1 | User to domain relation | |  |  |
| 1.8 | Trust | |  |  |
|  |  | |  |  |
|  |  | |  |  |
| 1.9 | Catalog data related to user and tenant (endpoints) | |  | 9) user  3) Tenant admin  4) Keystone Identity Admin  7) System admin  8) DB User |
| 1.10 | domain | |  |  |
| 1.11 | Auth Token related to a user | |  | 9) User  7) System admin  8) DB User  11) Keystone Process user |
|  |  | |  |  |
| 2 | System | | Assets related to configuration and system |  |
| 2.1 | Audit data | |  | 7) System admin  11) Keystone Process user |
| 2.2 | PKI/SSL private key | |  | 7) System admin  11) Keystone Process user |
| 2.3 | PKI/SSL signing cert | |  | All |
| 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 |
| 2.7 | REMOTE\_USER set | |  | External Identity admin  11) Keystone Process user |
| 2.8 | Ability to manage users (account provisioning) | |  | 3) Tenant admin  4) Keystone Identity Admin |
| 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)