Secret Management Service

API Documentation:
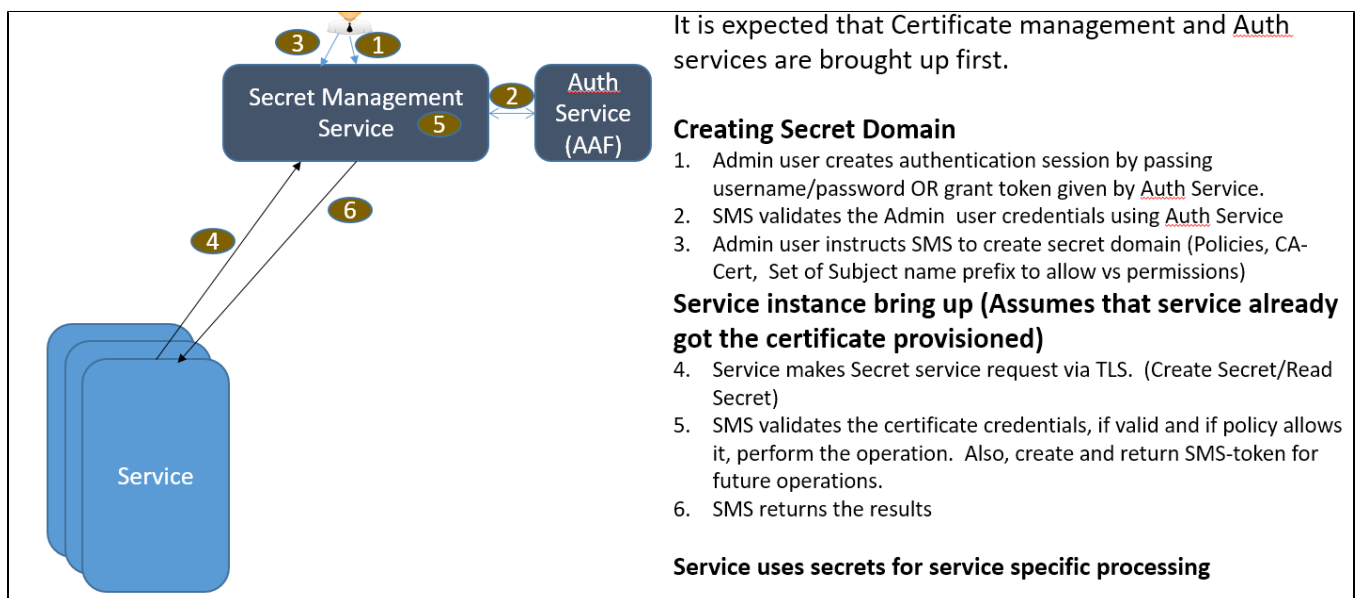

api_swagger.html

Link to Code Coverage Page

The project will provide a Secret Management Service with the following features and capabilities:

- Support multiple Secret domains
  - Each domain can be used to multiple secrets
  - Each domain is associated with various policies
- Each secret can have multiple key value pairs
- Certificate based authentication
- Authenticate users with AAF
- Token based authentication
- Securely store secrets using AES encryption
  - Use TPM/SGX for key storage if available
- RESTful API support for ADD, UPDATE, DELETE of secrets

The below diagram illustraces the Secret Service High Level Flow in an ONAP Context

It is expected that Certificate management and Auth services are brought up first.

Creating Secret Domain
1. Admin user creates authentication session by passing username/password OR grant token given by Auth Service.
2. SMS validates the Admin user credentials using Auth Service
3. Admin user instructs SMS to create secret domain (Policies, CA-Cert, Set of Subject name prefix to allow vs permissions)

Service instance bring up (Assumes that service already got the certificate provisioned)
4. Service makes Secret service request via TLS. (Create Secret/Read Secret)
5. SMS validates the certificate credentials, if valid and if policy allows it, perform the operation. Also, create and return SMS-token for future operations.
6. SMS returns the results

Service uses secrets for service specific processing

The below diagram illustrates how a micro service will use the Secret Client Agent to talk to the Secret Service to store or retrieve passwords.