Cloud Provider

Local Intranet

Cloud KMS

Cloud

DB

Component 2

Consuming Payment API

Exposed API

DMZ

ZONE

AD

Component 1

SSO

**High Level Design and Functionalities**

1. Component-1 is communicating with AD using LDAP Services in order to perform the Authentication and Authorization.
2. Component-1 is exposing Payment API to extract payment data.
3. Component-2 is running on cloud, supporting Single Sign on.
4. Component-2 is consuming Payment API from Component-1 to perform Payment transaction data generation.

**Assumptions:**

Component-2 support SSO and compatible with Industry specific standards such SAML and OAuth.

Component-1 will be issuing token upon successful user authentication.

**Risk Assessment:**

**Component-1 Security Requirements:**

1. Should provide OAuth 2.0/SAML 2.0 to access the protected resources (API).
2. Should expose only GET API(that means only read only operation)

**Risk**

If the POST has no business use case then it should be restricted for Coponent-2. Exposing POST API can provide the backdoor entry for Bad Actors.

1. Should connect with AD using TLS 1.2 Protocol.

**Risk**

AD contains sensitive information and communicating on secure channel will provider confidentiality.

1. Should bind AD Server using service account. Service account username and password must be kept in configuration file.
2. Should use TLS 1.2 to connect with component-2
3. Should validate the token received from client.

**Risk**

Not validating user token can cause un-authorized access on Application Data. So received token from the client need to be validated by Provider.

1. Should provide the end point to revoking the token.

**Risk**

User may want to unlink his identity from component-2, this end point will help him to un-link his account.

1. Should be protected against TOP OWASP Attack such as Injection, Broken Access Control, Broken Authentication and Server Misconfiguration.

**Risk**

Not protecting against basic attack can compromise the user data and could also affect the integrity of the whole system.

1. Authenticated user must have least privileges.

**Risk**

Following the principle of least privileges. If one of user credential got compromised then bad actor should not have access on entire application data.

1. A user who needs high privileges must have different mechanism of login.
2. Should maintain the audit logs in database for accessing the resource as well as any authorized access calls.
3. Access tokens should not be printed in logs.
4. Following Security Headers must be in place to mitigate the risks:
   1. X-XSS-Protection
      1. Prevent for XSS attack
   2. X-Frame-Options: will prevent from click jacking and prevent the login form to embed in attackers Iframe
   3. Cookies should be set as HTTP only and secure flag should be present

**Comppnent-2 Security Requirements:**

1. Component-2 should use Token to get Payment API response.
2. Component-2 should encrypt the token if storing it in database.

**Risk:**

Keeping token in plain-text format is not recommended as it may affect the confidentiality of the system.

1. Encryption should be performed using AES-256(or Above) Key

**Risk:**

Key with fewer length than 256 are already proven insecure.

1. Data Encryption key need to be available in KMS system.

**Risk:**

Compromise DEK can impact the system confidentiality and user privacy.

1. Key needs to be rotated on periodic basis.

**Risk:**

This is more like a compliance requirement.

1. Generated Payments data might contains sensitive information such as First Name, Last Name, personal identifier (like govt. ID card), age, phone number, email, account number and holder name. These information are user specific and leaking can cause user privacy issue. Sensitive information need to be encrypted as mentioned above.

**Risk:**

If database got compromise and user information are available in plain text then it will impact on user privacy and reputation of organization

1. Component-2 is deployed on cloud and hence need to apply cloud security policy such as IP whitelisting, review IAM role policy, turn on logging, auditing and monitoring.
2. Adhering OWASP top-10 and Security Headers

**Active Directory Security Requirements:**

1. Limit the number of LDAP client connection on AD Server, this will prevent Denial of Service attack.
2. Do not allow anonymous client connection.
3. AD Server must be running as non-root user.

**Acceptance Criteria:**

1. Application will be tested based on the provided requirements, in-order to get the security sign-off security requirements should meet.
2. In order to get the security sign-off application should not have any Critical, Blocker and Major issues.
3. Risk raised as medium should be provided timeline to fix.