Authentication and Authorization

User Story	Acceptance Criteria
As a developer, **I want to** use OAuth 2.0 to securely authenticate my application with the Google Cloud Storage API, **in order to** ensure only authorized users can access my data.	The application successfully obtains an OAuth 2.0 access token from the Google Cloud Platform.
As a security administrator, **I want to** use IAM roles to assign granular permissions to different users and services, **in order to** ensure that only authorized individuals have access to specific data.	IAM roles are created and assigned to users and services based on their required permissions.

Data Encryption

User Story	Acceptance Criteria
As a data owner, **I want to** ensure that my data stored in Google Cloud Storage to be encrypted at rest using CMECK, **In order to** ensure that it is protected even if the storage infrastructure is compromised.	CMECK is configured for the Google Cloud Storage bucket containing the data.
As a user, **I want to** transmit my data securely over HTTPS between my application and the Google Cloud Storage API **In order to** prevent eavesdropping.	All data transfers between the application and the API use HTTPS.

Input Validation

User Story	Acceptance Criteria
As a developer, **I want to** validate and sanitize all user input, **In order to** prevent injection attacks and ensure the integrity of my data.	All user input is validated for correct format and content.
As a security administrator, **I want to** implement whitelisting rules to restrict the allowed characters and formats for user input, **In order to** further redyce the risk of injection attacks.	Whitelisting rules are defined for all user input fields.

XSS Prevention

User Story	Acceptance Criteria
As a user, **I want to** be protected from XSS attacks by ensuring that the API properly encodes output and implements CSP, **In order to** restrict the resources that can be loaded on web pages.	All output is properly encoded to prevent XSS attacks.

Rate Limiting

User Story	Acceptance Criteria
As a developer, **I want to** be able to set rate limits for my API usage, **In order to** prevent abuse and ensure fair access for other users.	Rate limits can be configured for different API endpoints or users.

Logging and Monitoring

User Story	Acceptance Criteria
As a security administrator, **I want to** enable audit logging, **In order to** track API usage and identify potential security incidents.	Audit logging is enabled for the Google Cloud Storage API.
As a developer, **I want to** be able to monitor the API for anomalies and suspicious activity, **In order to** detect and respond to security threats.	The developer can use monitoring tools to track API usage and performance.

Security Best Practices

User Story	Acceptance Criteria
As a developer, **I want to** keep the Google Cloud Storage API and its dependencies up-to-date with the latest security patches, **In order to** mitigate known vulnerabilities.	The API and its dependencies are regularly updated with the latest security patches.
As a security administrator, **I want to** conduct regular penetration testing, **In order to** identify potential security weaknesses in my API implementation.	Penetration testing is conducted regularly by qualified security professionals.
As a team leader, **I want to** ensure that all developers receive adequate security training **In order to** understand and implement best practices.	All developers receive security training that covers relevant topics, such as authentication, authorization, data encryption, and input validation.