Bucket Protector

Introduction to Encryption Consulting's Bucket Protector Cloud Utility Function.

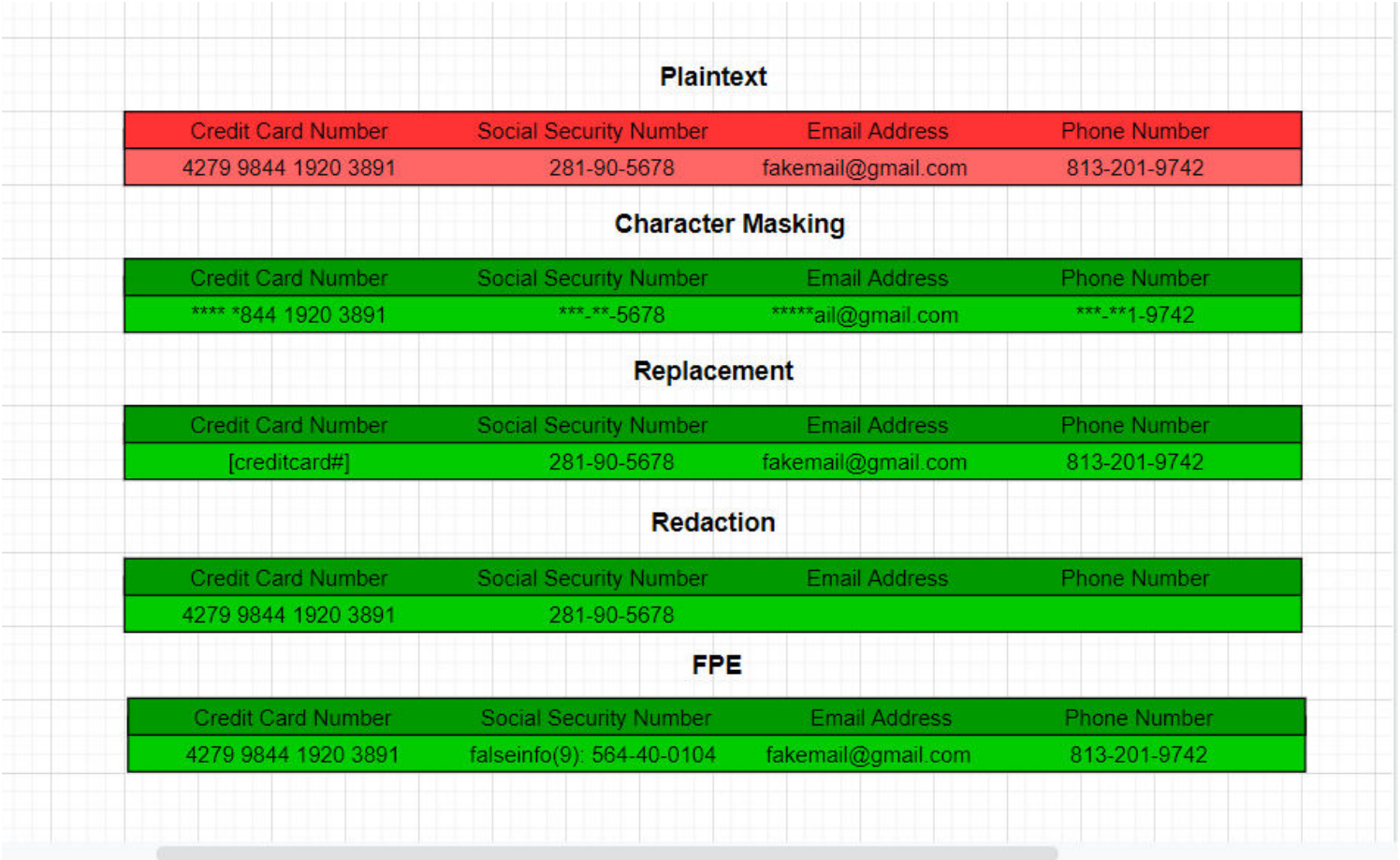
ENCRYPTION CONSULTING

What is Bucket Protector?

Bucket Protector is a Google Cloud Utility Function that utilizes the KMS, DLP, and Cloud Build APIs. The Data Loss Prevention (DLP) API works to encrypt or deidentify data that is passed to the API. The Key Management Services (KMS) API works with the DLP API to manage keys for any Format Preserving Encryption (FPE) that occurs. The Cloud Build API is how the Google Cloud Function can be built and run.

How do the different methods of deidentification and encryption work?

The user can select from character masking, replacement, redaction as methods of deidentification, or they can use FPE to allow their data to maintain the same length and alphabet as the value encrypted. Below are images displaying each type of deidentification and encryption with a short description of what is occurring.

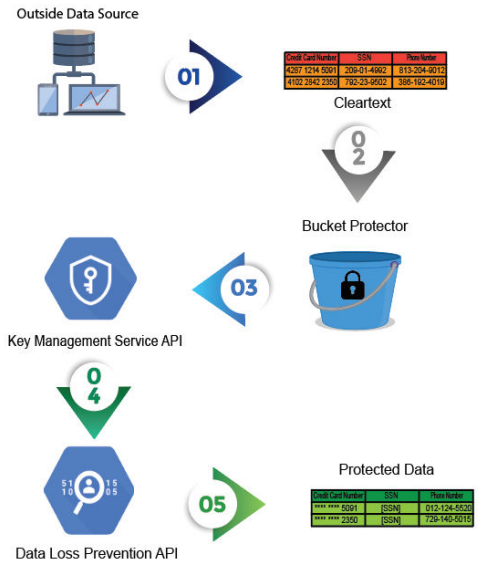


The first green box in the above image shows how character masking deidentification works. The user supplies a masking character, the infotype(s) to be deidentified, and the number of characters to be masked. The second

green box in the above image shows how replacement deidentification works. The user supplies the infotype(s) to be deidentified as well as a phrase to replace the infotype(s) with. The third green box in the above image shows how redaction deidentification works. The user supplies the infotype(s) to be deidentified and the values are redacted. The final green box in the above image shows how format preserving encryption works. The user supplies the infotype(s) to be encrypted, the names of the wrapping key and key ring in Google Cloud used to wrap the AES key used for FPE, and the surrogate infotype name the infotype(s) should be called. The surrogate infotype is used for decryption purposes.

Bucket Protector Overview

Bucket Protector is a Google Cloud Function that runs on a Google Cloud Storage bucket whenever a file is uploaded to the bucket, or a new version of a file is uploaded to replace the original. Prior to uploading the file to be protected, a JSON file named cloudFuncConfig.json is uploaded to the triggering bucket. This file contains data on what methods of deidentification/encryption are to be used on what info types. The below image goes over each portion of the Bucket Protector dataflow step by step.



1. The data is initially uploaded to the triggering Google Cloud Storage Bucket from another Cloud Storage Bucket on another account or from another project.
2. The data is uploaded to the Google Cloud Storage Bucket that triggers the Google Cloud Function.

3. The Cloud Function is triggered, calling the Cloud Identity Access Management (IAM) service.
4. The IAM service ensures the user has permissions to access both the Cloud KMS and DLP APIs.
5. The Cloud KMS API accesses any keys needed for Format Preserving Encryption, if the user has selected this method of encryption.

Finally, the DLP API is called and the encryption or deidentification methods are used and the now encrypted data is sent to the bucket that will hold any protected datasets created by Bucket Protector.

About Encryption Consulting

Encryption Consulting is a customer-focused cyber-consulting firm providing an array of services in all aspects of Encryption. Our areas of expertise include Public Key Infrastructure, enterprise key management, cloud key management, code-signing, hardware security modules, transparent data encryption, element level format preserving encryption, homomorphic encryption, and tokenization.

Our Expertise

Our knowledge and experience put experts on your team to deploy the industry's best, proven encryption technologies. Our people and services enable organizations to successfully achieve their data security goals in Confidentiality, Integrity, and Availability.

Our solutions will secure your sensitive data throughout its entire lifecycle.

The Problem We Solve

Our specialty is delivering Assessments, Strategies, and Implementations for organizations who either lack the specialized resources or who simply value having a trusted advisor to assist them to upgrade their data security posture.

At Encryption Consulting, we have created a custom framework based on NIST 800-57, NIST 800-53 standards, FIPS and industry best practices to accelerate our client's data protection projects.