ECKLER

espace™ where data lives

ingenius™ intuitive solutions

foreward™ insurance on demand

prevision™ foresee the potential

elegant™ pension management simplified

PENSION PILOT

Encryption Strategy for Eckler Financial Services Platforms

Encryption is a powerful tool that allows for an organization to protect data in scenarios when a breach or theft happens and the data can no longer be actively protected with access controls. Encryption can also be used to provide protection for client data from administrators. The technology and solutions utilizing encryption are continuously evolving as attacks and threats evolve. The primary goal with any encryption solution is to maintain separation of the key and the data protected by the key. If the key and the data are beside each other than using encryption is just a waste of resources. The separation can be in any form and it may depend on the data that is being protected. In this document we will outline the levels of encryption and protection employed on Eckler platforms to protect data of varying sensitivities as well as at different levels of storage.

Eckler Financial Services utilities Amazon Web Services (AWS) as the service provider for running our platforms. All our platforms maintain data within Canada. Where possible we utilize the Key Management Service (KMS) from AWS and the services ability to manage encryption with the KMS. This reduces the risk of improper implementation of encryption at rest within our platforms as well as utilizing AWS' best practices to protect the data.

DISCLAIMER: Encryption will never fully protect the data stored in it. All it does is buy enough time to make the data contained in the encryption no longer relevant or valuable once the encryption is broken if implemented correctly.

Key Management

All keys that are created within the Key Management Services (KMS) are created with the same configuration for all of our platforms. Each platform has one or more KMS keys used to protect data managed by that platform. The keys are created with permissions for administrators to administer the keys but do not have the ability to encrypt or decrypt data with the key. This ensure administrators are not able to inject or read data within the platform unless explicitly provided permission to do so. All keys are configured with key rotation which ensures new key material is generated annually to encrypt data with while maintaining all previous versions of key material so older data can be decrypted correctly.

AWS Services Utilized for Data Storage

The following services are utilized for storing data provided by users to our platforms:

- Simple Storage Service (S3)
- Elastic Block Storage (EBS)
- Relational Database Service (RDS)
- ElastiCache
- DynamoDB
- AWS Backup

All the services listed support encryption at rest with the key material managed by KMS. This ensures that data is encrypted at rest inline with industry best practices. These services also allow for the requirement that data is encrypted in transit so that the data is protected as it moves through the platform. Automation is utilized to ensure that any infrastructure created in these services are configured correctly to ensure client data is encrypted. Separate KMS keys are used for the different instances of the resources to ensure proper access controls based on the platform and use of the service and the resources within it.

In the event a particular configuration of a service does not allow for encryption at rest to be enforced by the service the platform will encrypt the client data before storing it with the service. The platform will use the KMS to manage the key material so that the configuration and management for key material is consistent across all platforms.

Password Storage

Password storage in our platforms is different from other data storage for the fact that passwords do not need to be fully decrypted to determine if the input matches. This allows the password to be stored in format that cannot be reversed to determine the plaintext version. The objective of this layer of protection is to render the password data unusable if the data was leaked via a breach or other means.

Passwords are stored using 3 layers of protection:

(1) Cryptographic hash using SHA512 and a unique key

(2) BCrypt hashing with a defined cost

(3) Encryption using a secret box with a derived key for each user

The first step allows us to take any size password and turn it into a consistently sized hash that has a very high probability of being unique per each unique input. The second step is similar to step 1, except it is meant to introduce work into the process. This makes it very difficult for an attacker to brute force guess a password for a particular user if the data was stolen and can no longer be actively protected. The third step is just an additional layer to slow down an attacker from accessing the underlying data.

Backups

The AWS Backup service is utilized to consistently store daily backups for all services that store client data. The service is configured with its own KMS key to ensure separate access controls to the backups. Configuration of the service is consistent across all AWS environments and accounts to ensure all utilize the same parameters and have the same life times.

Communication

Any data leaving our internal networks is encrypted directly to users accessing the platforms using the latest TLS standards. Internal network communication utilizes encryption were possible as well as security groups and access control lists to limit the how resources communicate with each other. Networking with our AWS environments is provided by the AWS Virtual Private Cloud (VPC) service which ensures that data within a VPC instance is protected and isolated similar to a physical internal networks utilizing switches and routers.

Handling Changes to Encryption Strategies

As encryption best practices and the AWS product suite evolve we will continuously review our current strategies and adjust to ensure we protect client data by any means necessary. In the event data needs to be encrypted again due to a strategy change automation will be utilized to ensure data consistency and validity is met before completing migrations and discarding the old data.

Technical Resources and References

Here are links to online resources to provide more in-depth knowledge on all the technologies referenced in this document:

- **AES256** https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
- **BCrypt** https://en.wikipedia.org/wiki/Bcrypt
- **SHA512** https://en.wikipedia.org/wiki/SHA-2
- **Simple Storage Service** https://aws.amazon.com/s3/
- **Elastic Block Storage** https://aws.amazon.com/ebs/
- **Relational Database Service** https://aws.amazon.com/rds/
- **DynamoDB** https://aws.amazon.com/dynamodb/
- **ElastiCache** https://aws.amazon.com/elasticache/
- **AWS Backup** https://aws.amazon.com/backup/
- **Amazon VPC** https://aws.amazon.com/vpc/

Questions about this document should be referred to Phillip Couto of Eckler Ltd., email: PCouto@Eckler.ca.

Latest revision to this document: July 2022