Case 1

CYBER Security

2020-04-01

Submitted by:

Group 15

Ranjana, Efstathios, Justas

# Encryption Key Management Policy

### Purpose

The Eastchange's Key Management Policy outlines the process for managing the encryption keys and the life cycle of the encryption keys at Eastchange.

### Scope

This assessment addresses the process of key management performed by Eastchange in order to ensure the keys used in Eastchange’s AB environment are under the well formulated process flow.

### Roles and Responsibilities

#### Separation of Duties

Regarding information security practices, the implementation of Separation of Duties is critical in the area of encryption key management. To prevent unwanted access to protected data, it is important that the person who manages encryption keys not have the ability to access protected data, and vice versa.

#### Dual Control

Dual control means that at least two or more people control a single process. In encryption key management, this means at least two people should be needed to authenticate the access of an encryption key, so that no one single person has access to an encryption key. Within Eastchange, the Information Technology manager and the Information Security Manager each know only a half of the pass phrase used to create encryption keys.

### Key Management Lifecycle

#### Creation

The key at Eastchange is generated using Advanced Encryption Standard, which produces a symmetric key. The generated random key is of length 32 , divided into 8-4-4-4-12 format and 256 bits. 256 -bit encryption is used for encryption and decryption of data which is among the secure encryption after 128 and 192-bit. AES protocol is used along with 256-bit encryption.

AES is short for Advanced Encryption Standard. It's a symmetric block cipher used to encrypt sensitive data and to lock away classified or otherwise valuable information. Advanced Encryption Standard is the default algorithm for encrypting classified information and also the first encryption algorithm approved by the National Security Agency made open for the general public. AES\_256 comprises 14 rounds of processing steps, which include permutation and substitution of the encrypted text which transforms into the encrypted form. The first step in the AES encryption process is substituting the information using a substitution table; the second transmutation changes data rows and the third shifts columns. The last transformation is a basic exclusive XOR process done on each column using a different part of the encryption key.

#### Backup/Storage

Before a new key is installed into environments, it is imperative that a backup be made. Once the key is generated and reviewed by Eastchange Information Technology manager, it is then stored in an encrypted location in which visible and accessible only to Eastchange Information technology manager, Information Security Manager and Eastchange system administrator. That location is then encrypted using bitlocker-key whose key is also only available to Information Technology manager, Information Security Manager and system administrator. The key and identifier of bitlocker is only accessible to the Information technology manager, Information Security Manager and system admin.

Whether keys are in the pre-operational or operational state, they are stored securely and, ideally, nowhere near the data that they protect. Pre-operational keys are stored in a drive with bitlocker encryption enabled. The key and identifier of bitlocker is only accessible to the Information technology manager, Information Security Manager and System Administrator. Operational keys on the other hand are accessible in real time, online, and are stored within live systems. The drives are encrypted using a key, but the key is not visible to users. The databases are encrypted using keys, which are defined using symmetric key tables and are constantly in use. The backups are encrypted using the same key as the database.

#### Deployment

At Eastchange, the key gets deployed in multiple locations. Following are the areas where encryption key is deployed:

* Database
* Backup of database
* Disk Drives
* Transaction between the Eastchange and clients
* Servers
* Data Center
* Data shared through FTP/SSH

#### Monitoring

There are three key aspects to monitoring that are followed from Eastchange:

* Unauthorized operation is handled by limiting the access to the required environments. Only the personnel from Eastchange who have security clearance with respective authentication can use the required materials in respective encrypted environments.
* The performance of cryptographic calculations tends to be CPU-intensive, which means that the Eastchange systems may be under significant load. Monitoring engine has been created to report the performance of the server.
* Monitoring the key in production is also important to ensure that the key has been created and deployed properly. If a corrupted key is deployed too quickly without proper vetting, the results could be catastrophic. Similarly, if a fault in the crypto system occurs, then the results could also interrupt service, with a negative impact to the business. As the key gets corrupted, it is configured to report it back to the system administrator and IT manager. As soon as the report is received, a new key is deployed using this same lifecycle.

#### Rotation

In rotating keys, the goal is to bring a new encryption key into active use by the crypto system, and to also convert all stored, encrypted data to the new key. This phase is discretely focused on the conversion activity, and less on the activation of the new key for future encryption requests. The rotation of the keys is done every year using this same lifecycle. In all the environments, the new keys are deployed and the old keys get archived/destroyed after deploying the new key.

#### Expiration

The expiration time of the certificates and keys used at Eastchange is configured to be one year. After the key gets expired, a new lifecycle is followed for key generation.The Expiration phase of key management represents the beginning of the depreciation period for the key.

#### Archival

The absolute last thing that Eastchange does when managing crypto systems is to destroy a key that still has data associated with it. The keys are archived for 10 years until it goes to the final stage, i.e., destruction.Following things are done in archival of key:

* The key and its associated data along with the respective environment is documented and indexed, should if needed to recover the data with an archived key, can be done so in as effective and efficient a manner as possible.
* The archived copy of key is insured in a drive which is encrypted using bitlocker. The key and identifier of this bitlocker is also available to Information Technology Manager, Information Security Manager and System Administrator.
* Before the archival of the key, Eastchange makes sure that the data which the key to be archived possess is capable to recover the encrypted data.

#### Destruction

The life of a key will end when it is destroyed. Key destruction follows secure deletion procedures so as to ensure that it is properly obliterated. Key destruction is not taken lightly, and only occurs after an adequately long Archival phase, i.e. 10 years, and after at least two reviews have been completed to ensure that loss of the key will not correspond to loss of data. The review is performed by the Information Technology Manager and Information Security Manager.

# Information Security Policy

### Purpose

The purpose of this Policy is to establish standards for protecting the information and assets of Eastchange and its information system from various threats and to ensure business continuity, minimize damage, maximum return on investment, legal compliance and improve the image.

### Scope

This Policy applies to all employees of Eastchange. It also applies to Eastchange's stakeholders as contractors, consultants, temporaries, third parties, further appointed in this document as Eastchange cooperators.This Policy applies to all equipment that is owned or leased by Eastchange.

### Information Security Policy

Information regardless of the form in which it is (written, spoken, printed, and electronic) is a primary asset for the business that has its value and therefore it is necessary to adequately protect it. Information together with other components makes up the information system of Eastchange.

In order to protect the information and assets of Eastchange or its information system from various threats and to ensure business continuity, minimize damage, maximum return on investment, legal compliance and improve the image, the Management Board of Eastchange should approve the security policy that sets goals and fundamental principles for establishing effective information system security.

The Management Board will be directly responsible to provide clear and concrete support in the implementation of security policy and monitor its application in daily operations by delegating responsibilities and establishing an appropriate organizational structure.

To achieve the goals, the Management Board will appoint a person responsible for information security, the Information Security Manager. His role and duties are governed by a special act, Information Security Manager Responsibilities.

The Information security manager is the owner of the Information Security Policy.

By protecting and securing the principles of information security, Eastchange:

* Will ensure compliance with criminal and civil law, statutory, legal or contractual obligations that have established safety requirements.
* Will educate all users of information systems for security awareness of threats to business, how to protect information and also how to care for the information system and to uphold its objectives and principles in everyday work.
* Will implement appropriate checks for every new employment according to Human Resources Manual.
* Has inventory of all equipment and other assets and regularly updates each change in order to prevent unauthorized dealing, theft, appropriation, misuse or removal of funds from Eastchange.
* Will analyze the risks associated with information system assets and measure the impact on the operations of Eastchange whenever necessary.
* Will establish a system of classification, labeling, storage and use of information in order to prevent unauthorized access, theft, misuse, destruction or alteration of their contents.
* Will not allow entry or use of unverified or illegal equipment and software in computer information systems, unauthorized access to information and information assets, loss, damage or unauthorized modification of information, interruption of business processes, theft or misuse of the information and assets of processing information
* Will provide an appropriate level of security of information and information resources in all parts of the organization by establishing security zones and limited physical access.
* Through regular monitoring and reporting of human errors, defects, damage, security incidents or unauthorized activities, Eastchange constantly learns and improves and thus decreases the effects of isolated and hidden threats to security of information and information assets.
* Will ensure continuity of critical business processes in case of unavailability of information systems in a reasonable and acceptable time frame, through the development, implementation and testing of Business continuity plans.
* Regular annual internal and external audits ensure compliance of the information system with security policy and international standards ISO / IEC 27001 and perform its constant improvement.
* Will ensure full management control for:
* Electronic Communication
* Acceptable Usage of Electronic Communication facilities
* Use of Email
* Use of Internet Access
* Data Privacy
* Physical Security
* Protection of Customer information
* Use of social Media
* Use of Electronic equipment
* Remote Access to your Company's network
* Reporting policy violation and security incident
* Access Control
* Information Classification
* Personnel Security and termination of employment
* Maintenance of Security policies
* Business continuity
* Supplier Relationship
* Compliance
* ICT securityDevelopment

The above principles represent the direction and support to establish a system for managing information system security, in accordance with the requirements of standards.

## Group 1 Review from Group 15

## Case 1 Policy

You have done a good job in following the pattern of policy as well as the look of the content you created. Every policy was explicitly described and motivated. However, we were supposed to write only 2 policies, but the first policy contains multiple sub-policies, which qualify as different policies. For example: Access control and cryptography should be separate policies.

Questions:

1. Why did you choose these policies as the most important ones for Eastchange AB?
2. Your encryption policy highlights the key creation, however encryption has multiple stages and each of them must be well maintained. For example: how the keys should be used, what to do after the key is decommissioned. Can you please elaborate why only key generation was focused on encryption policy?
3. We had to write about an overarching policy, but the policies you mentioned have sub policies, which qualify as different policies. Was there a specific reason for including main policies as sub sections?

Answers to Group 11 questions:

Hi, thank you for the review. Before we answer your questions, we would like to highlight that we were supposed to write any two most relevant policies we thought are the most important, not all of them.

1- There's no mention of PCIDSS in your policy, considering the company deals with alot transactions especially online through credit cards, how do you ensure the privacy and security of customers in that area

For the technical part, we went with encryption policy rather than a “Application policy”, where PCI/DSS would fall under, as we thought it would be more relevant since Eastchange work with bitcoins. It is clearly stated in the document that bitcoin transactions are made through asymmetric encryption and that is a crucial element of such a company. As a result, we thought that an encryption policy would fit better.

2- what are the the access controls for different levels of users

We have not mentioned access control in our two policies as we went with Information Security Policy and Encryption Policy, therefore this question is not relevant to the policies we chose.

3- Your policy doesn't mention any key exchange methods, how are keys exchanged between different branches or sites.

Our policy is for encryption key management rather than encryption key implementation, as implementation would fall under different topics. It would be implemented not just on sharing among parties but also how they are implemented including application, FTP, SSH and on servers. We only wanted to stick with the idea of how keys are managed so we went with encryption key management policy.

Regards,

Group 15