IIROC OCRCVM
Investment Industry Regulatory Organization of Canada
Organisme canadien de réglementation du commerce des valeurs mobilières

Strategy for Encryption of Client Identifiers

Version 1.~~7~~8.~~0~~1
~~May~~ August ~~20~~11, 2020

Document History

Version	Description of Change	Date
1.0	• Document initiated. First draft complete.	Jun 5, 2019
1.1	• Minor edits	Jul 15, 2019
1.2	• Edits and clarifications based on feedback from implementation committee	Sep 2, 2019
1.3	• Expansion of key management process	Nov 5, 2019
1.4	• Revises 2.2 Encrypt FIX Value to add Base64 encoding • Updates Figure 2 Encrypt Value Structure • Adds Figure 3 Timeline for key rotation schedule	Dec 2, 2019
1.5	• Dealer ID could be 3 characters instead of 3-digit number • Randomization of counter block is not mandatory	Jan 20, 2019
1.6	• Update key management section	Mar 11, 2020

1.7	• Update 2.2 Encryption FIX Value to combine nonce and counter as initialization vector (IV)
	• Update 2.3 key management section
	  ○ Encryption key encoded into 24-character using base64 for delivery
	  ○ Key distributed via secure email
	  ○ Using URL link provided in email for acknowledgement of key receipt
		May 20, 2020

1.8	• Update Figure 2 Encrypted Value Structure to have the sample data in the figure as real data for implementation testing reference	Aug 11, 2020

Table of Contents

1. About this Document

1.1 Introduction

IIROC has amended to the Universal Market Integrity Rules (UMIR) which require client identifiers and/or certain designations to be included on all orders and trades for an equity security sent to a marketplace. The client identifiers will be encrypted by the originating Dealer Member such that they are visible by the regulator and not the marketplaces. This document provides the method of encryption and the attendant infrastructure required for its successful implementation (representation of the ciphertext on the FIX feed, key management, etc.)

1.2 Intended Audience

This document was initially written for the benefit of IIROC Client Identifiers Implementation Committee, but could be expanded at a later date for use by information security, business analysis, development and quality assurance staff involved in the implementation of client identifier encryption.

2. Method of Encryption

2.1 Advanced Encryption Standard

The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST). Now used internationally, it is the only publicly accessible cipher approved by the National Security Agency (NSA) and was adopted by the U.S. as a federal government standard in 2002.

The AES describes a 'block cipher' and is a symmetric-key algorithm (i.e. the same key is used for both encryption and decryption); key size may be 128, 192 or 256 bits. Using 128-bit keys would minimize impact to system performance while maintaining a sufficient level of information security.

2.1.1 Mode of Operation – AES-CTR

A mode of operation is an algorithm used in conjunction with a block cipher to enhance information security. There exists a wide range of modes that encompass varying guarantees of security and efficiency; the Counter (CTR) mode offers a number of efficiency advantages over other modes without weakening security (e.g. it is highly parallelizable, and securely transforms of a block cipher into a stream cipher (thereby removing the need for block padding)).

With the plaintext having been divided into blocks, the basic algorithm combines a 'nonce' (or 'initialization vector') – an arbitrary, unpredictable value such as a random or pseudo-random number – with a counter that increments with each block; this combination is then encrypted using the key and the result is XOR'd with the plaintext to generate the ciphertext. A simplified description of the process is illustrated in Figure 1.

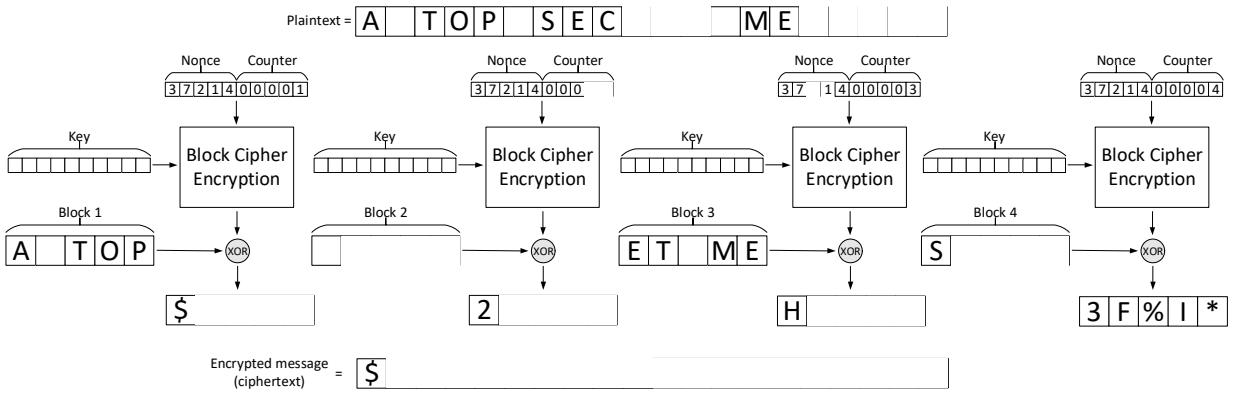

Figure 1: AES-CTR Encryption

2.2 Encryption of FIX Values

The relevant FIX tags should be populated with a string comprised of three concatenated elements:

- a 3-byte unique dealer ID identifying the encrypting Dealer Member
- a 16-byte initialization vector (IV) and
- a 20-byte encrypted LEI value;

The concatenated binary data will be then encoded with Base64 to a 52-character string value assigned to the relevant FIX tag as the figure 2 illustrated below:

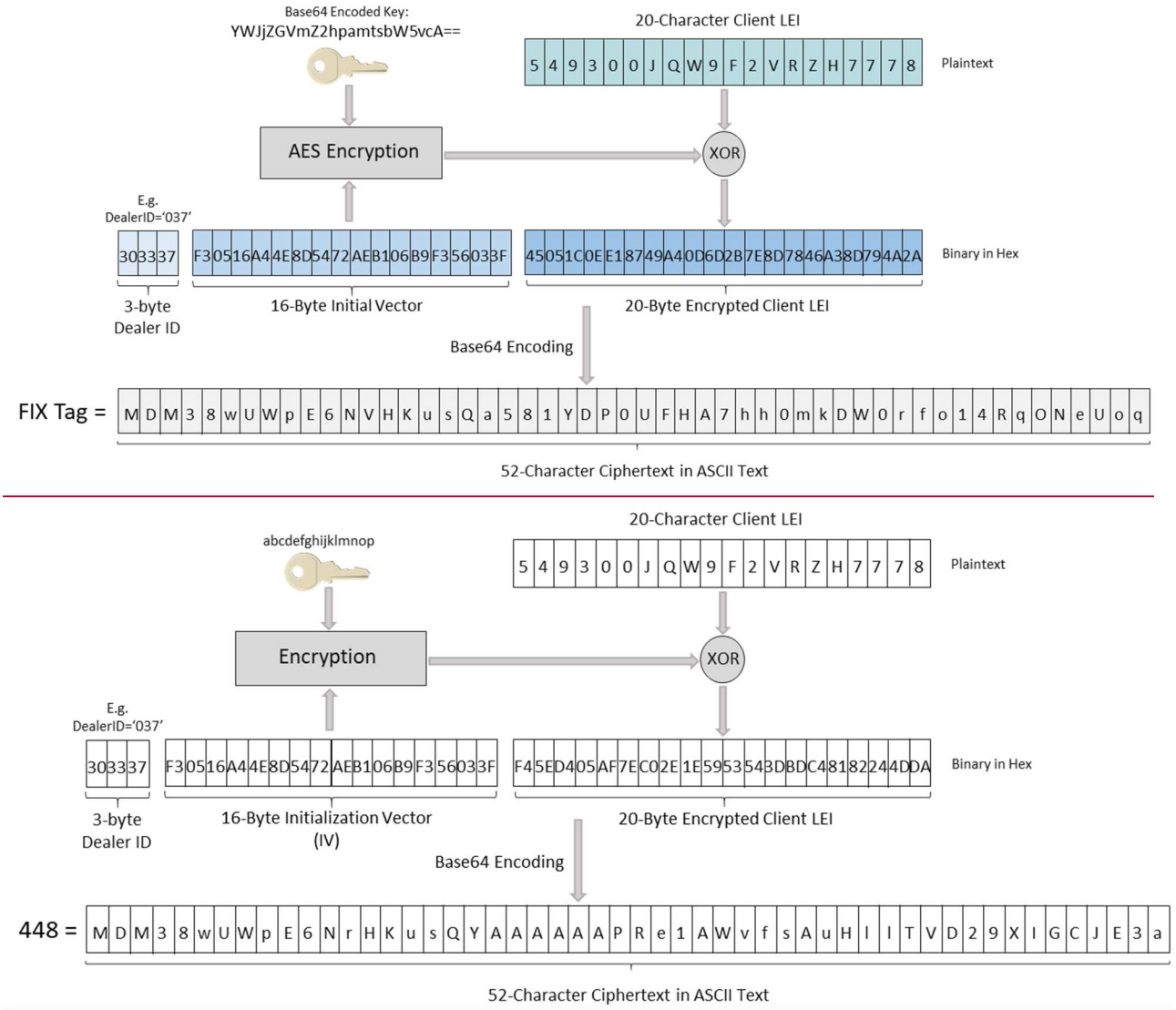

Figure 2: Encrypted Value Structure

- The encryption key is 16 bytes long and is distributed as Base64 encoded 24-character string.
- The Initialization Vector (IV) is a block of 128 bits (16 bytes) stored in Little Endian order.

- We recommend randomizing the IV so that a unique and unpredictable IV will be provided on each order message – this will produce distinct ciphertexts of same client LEI in different order messages since a key-IV pair is used only once.
- However this randomization of the IV value is not mandatory on each order message, they can be a fixed value used to encrypt a client LEI as long as the client understands that its encrypted LEI as seen by the marketplaces will have the same string value across all order messages.
- The encrypting dealer ID is required for IIROC to identify the appropriate key for decryption of a given LEI; this ID will be assigned when the initial encryption keys are disseminated.
- The concatenated dealer ID, IV block and encrypted client LEI is a 39-byte arbitrary binary data which shall be turned into a readable 52-character ASCII text using Base64 encoding.
- Where an executing Participant receives an order from a non-executing Dealer Member that is trading for its client and the client LEI is not encrypted, the executing Participant will use its own encryption key to encrypt the non-executing Dealer Member's client's LEI. An executing Participant can identify whether or not an LEI is encrypted (and therefore whether or not to initiate its own encryption) by examining the length of the LEI field in the message transmitted by the non-executing Dealer Member: if the field's value is longer than 20 characters (the length of an unencrypted LEI), the LEI can be assumed to have been already encrypted by the non-executing Dealer Member.

~~2.4~~2.3 Key Rotation Management

A different encryption key will be provided to each originating Dealer Member. The key is a 128-bit binary data and will be encoded into a 24-character ASCII text using Base64 encoding for delivery to the Dealer Member via encrypted email. Keys will be refreshed every 12 months; IIROC will generate and disseminate keys on an annual basis (as opposed to disseminating multiple years' keys at once) – it is believed that this approach will minimize potential uncertainty around when to refresh keys, which keys should be used etc.

The key rotation schedule will operate as Figure 3 illustrates:

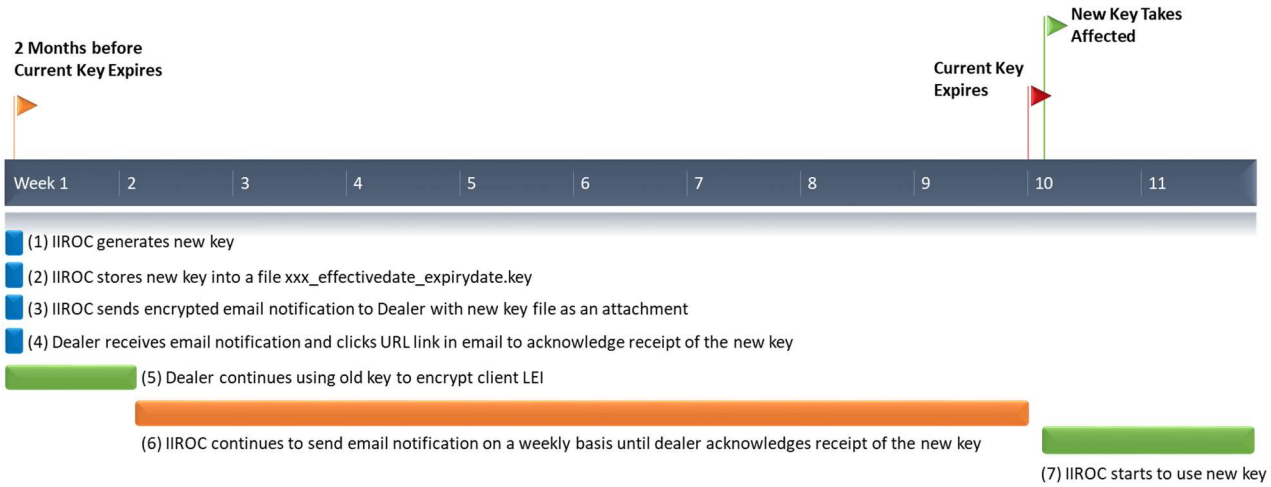

Figure 3: Key Rotation Schedule

1. Two months before the current key expires, IIROC will generate a new key for each active Dealer Member.
2. The new key is encoded into a 24-character ASCII text using Base64 encoding and stored into a text file with the file name pattern as xxx_yyyymmdd_yyyymmdd.key where:
    a) xxx is 3-character unique dealer ID
    b) 1st yyyymmdd is the effective date of the new key (inclusive)
    c) 2nd yyyymmdd is the expiry date of the new key (inclusive)
3. IIROC will send an e-mail with the above key file as an attachment via secure TLS email channel notifying the Dealer Member that a new key is available.
4. Each Dealer Member will receive an email containing a time-sensitive URL link (valid for a week) that is unique to each new dealer key. The key administrator at the Dealer Member must click the link in order to acknowledge the receipt of the new encryption key.
5. Once the receipt of the new key is acknowledged by Dealer Member, IIROC expects all trading by the Dealer Member must:
    a) continue to use the current key until it expires, and
    b) use the new key starting on its effective date.
6. If the Dealer Member fails to click the acknowledge URL link in the email within a week of notification, a new e-mail along with the encryption key in the attachment will be sent again via secure channel; further reminders will be sent for each subsequent week if the Dealer Member fails to click the acknowledge URL link in the notification email.
7. Starting from the new keys' effective date, IIROC will use the new keys to decrypt the Client LEI.