



Client Identifiers - Encryption Key Management Information for IIROC Dealer Members

Version 1.0

August 19, 2020

All Rights Reserved. No part of this document may be photocopied, reproduced, stored in a retrieval system, or transmitted, in any form or by any means whether, electronic, mechanical, or otherwise without the prior written permission of IIROC.

Table of Contents:

TABLE OF CONTENTS:..... 2
OVERVIEW: 2
DEALER MEMBER ENROLLMENT: 3
ENCRYPTION KEY INFORMATION AND DISTRIBUTION: 4
ENCRYPTION KEY ACKNOWLEDGEMENT:..... 7

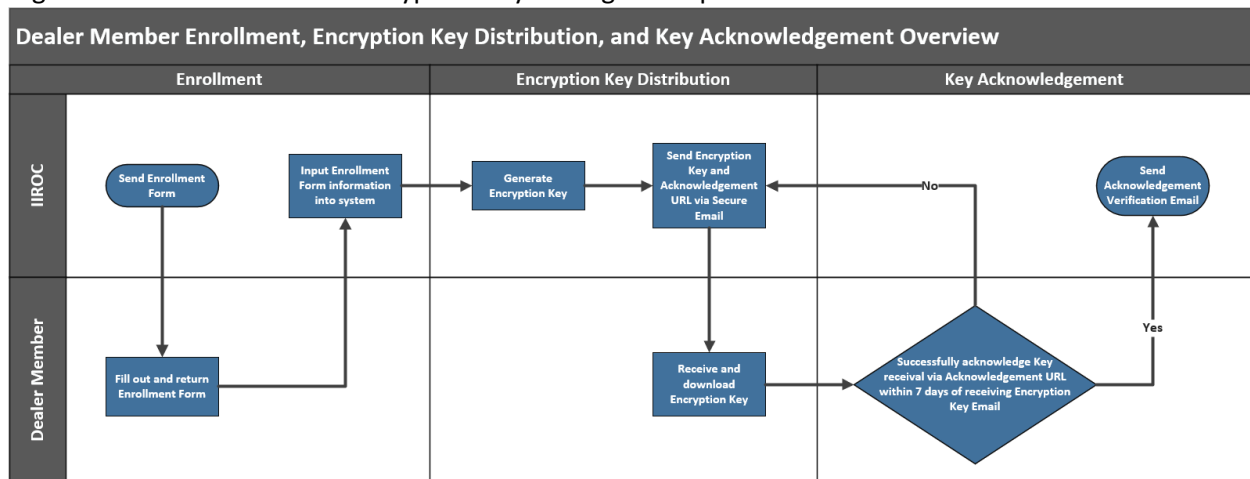
Overview:

IIROC is the pan-Canadian self-regulatory organization that oversees all investment dealers and their trading activity in Canada’s debt and equity markets. IIROC sets high quality regulatory and investment industry standards, protects investors and strengthens market integrity while supporting healthy Canadian capital markets. IIROC carries out its regulatory responsibilities through setting and enforcing rules regarding the proficiency, business and financial conduct of 175 Canadian investment dealer firms and their nearly 30,000 registered employees, the majority of whom are commonly referred to as investment advisors. IIROC also sets and enforces market integrity rules regarding trading activity on Canadian debt and equity marketplaces.

On April 15, 2019, the applicable securities regulatory authorities approved amendments to the Universal Market Integrity Rules and the Dealer Member Rules to include Client Identifiers.

Encryption Key Management is an essential piece of the Client Identifier project; this document illustrates the Dealer Member Enrollment process, Encryption Key Distribution process, and Encryption Key Receipt Acknowledgement process.

High-level overview of the 3 Encryption Key Management processes covered in this document:



Dealer Member Enrollment:

IIROC initiates the process by sending the Enrollment Form the Dealer Member CCO via email. The Dealer Member must fill out and return the Enrollment Form to IIROC (clientidentifiers@iiroc.ca) no later than 14 calendar days after receipt of the email. Returning the completed Enrollment Form is a prerequisite for generating the Dealer Member's Encryption Key; all fields on the Enrollment Form are mandatory. The Dealer Member is responsible for maintaining and updating the Encryption Key Distribution Email specified on the Enrollment Form (this distribution list is where the Dealer Member's Encryption Key is sent).

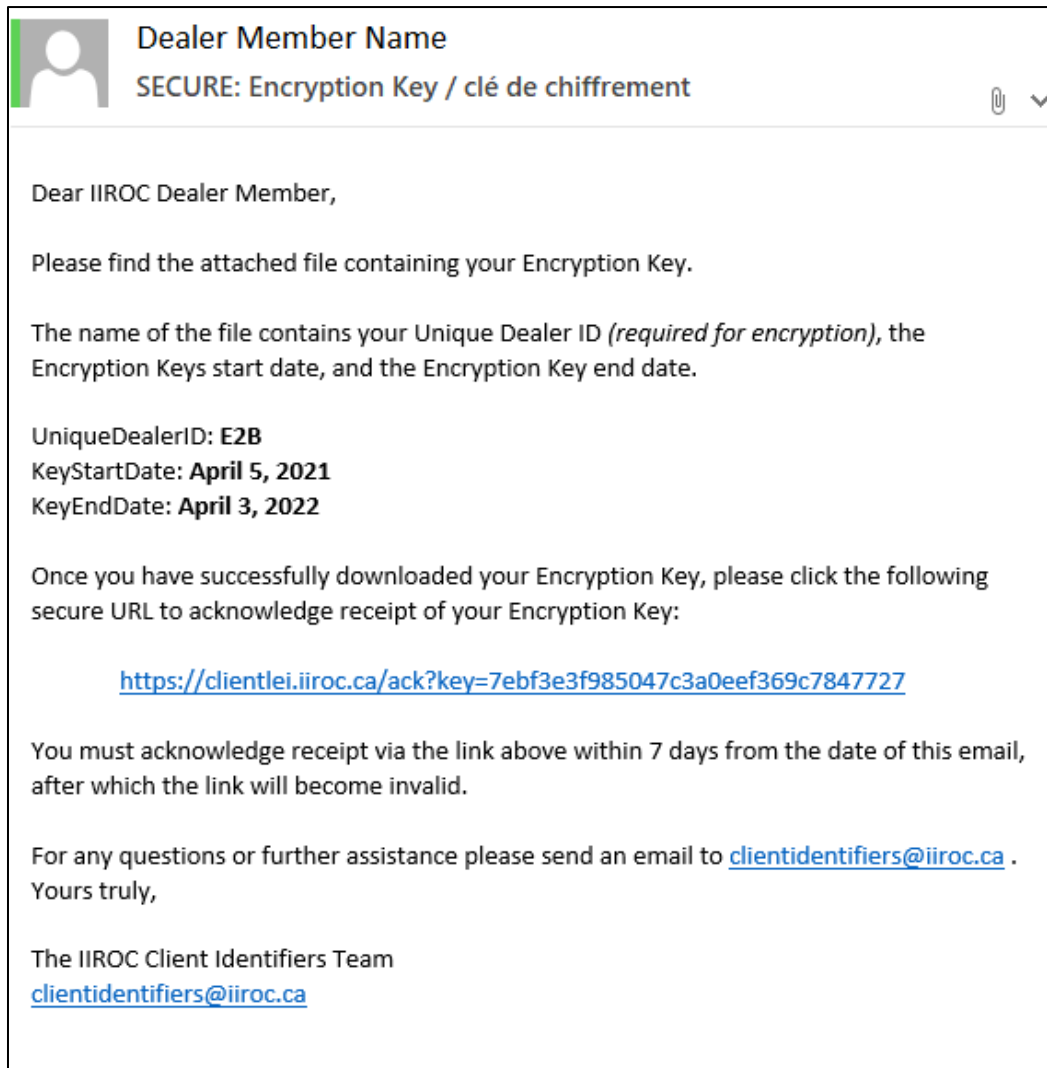
Encryption Key Management for Client Identifier Amendments Dealer Member Enrollment

Dealer Member Information Legal Name of Dealer Member Entity: _____ Legal Entity Identifier (LEI) or Participant Number: _____ Address: _____ City: _____ Province: _____ Postal Code: _____
Primary Contact Name: _____ Phone: _____ Email: _____
Backup Contact Name: _____ Phone: _____ Email: _____
Key Recipients Encryption Key Distribution Email: _____
Dealer Member Authorization Name: _____ Title: _____ Signature: _____ Phone: _____

Encryption Key Information and Distribution:

IIROC distributes the Dealer Member's Encryption Key (as a text file attachment) to the Encryption Key Distribution Email specified on the Enrollment Form, via secure email.

Sample Encryption Key Email:



Encryption Key File Attachment Information:

Encryption Key Filename Format: UniqueDealerID_StartDate_EndDate.key
e.g. E2B_20210405_20220403.key
Encryption Key File Content: 24-character Base64 Encoded Encryption Key
e.g. 3JpUwHDS0ZJHhWiJS5HPBg==

The Encryption Key is sent along with the Dealer Member's Unique Dealer ID (this ID is required when encrypting the client LEI information), the Encryption Key Start Date, the Encryption Key End Date, as well as a Secure URL that allows the Dealer Member to acknowledge receipt of their Encryption Key.

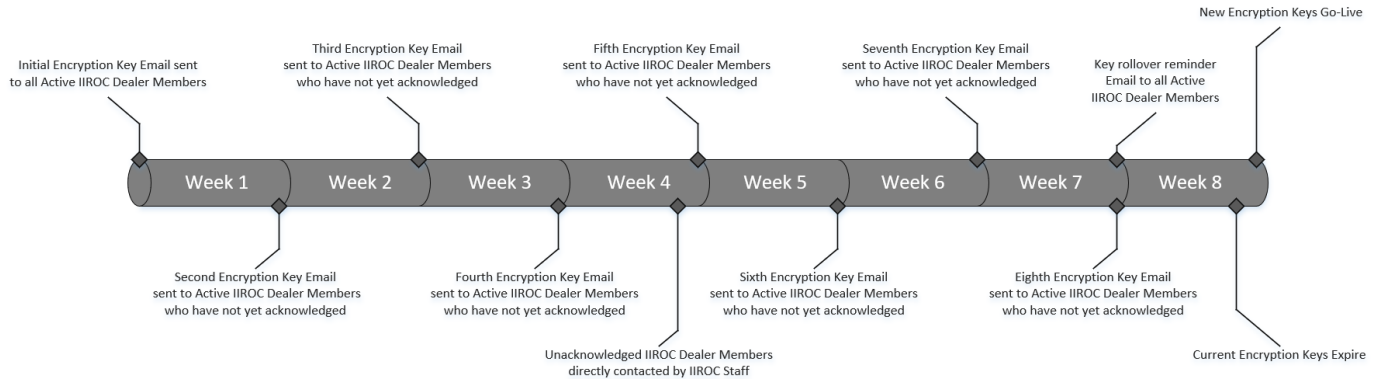
The Encryption Key format is Base64 encoded 128 Bit Key (24 ASCII characters) and is essential to encrypt the client LEI information before transmission. The Encryption Key is renewed on an annual basis.

The Unique Dealer ID is a 3-Character alphanumeric ID that IIROC has generated for the Dealer Member (this ID is permanent; it will not change yearly like the Encryption Key). The Unique Dealer ID is contained within the email body as well as in the filename of the Encryption Key file attached to the email. The Dealer Member is required to stamp their Unique Dealer ID on the encrypted client information, this allows IIROC to identify which Dealer Member has encrypted the information. IIROC can then decrypt using the Dealer Member's corresponding Encryption Key (for more information on the encryption process please refer to the Strategy for Encryption of Client Identifiers section on the IIROC Website: <https://www.iroc.ca/industry/Client-Identifiers/Pages/Technical-Specifications.aspx>).

The Encryption Key Start Date and End Date are also contained within the email body as well as the filename. The format for the Start and End Dates in the filename is "YYYYMMDD", and in the email body is "Month, Day, Year". For the initial distribution (Production Launch) as well as the Key Rollover Process (yearly process for sending the new Encryption Keys), the new Encryption Keys are generated and sent out 8 weeks prior to the current Encryption Key's End Date (for Production Launch this date is the Go-Live date). These new Encryption Keys last exactly 12 months with the Encryption Key Start Date set to the first Monday of April of the current year.

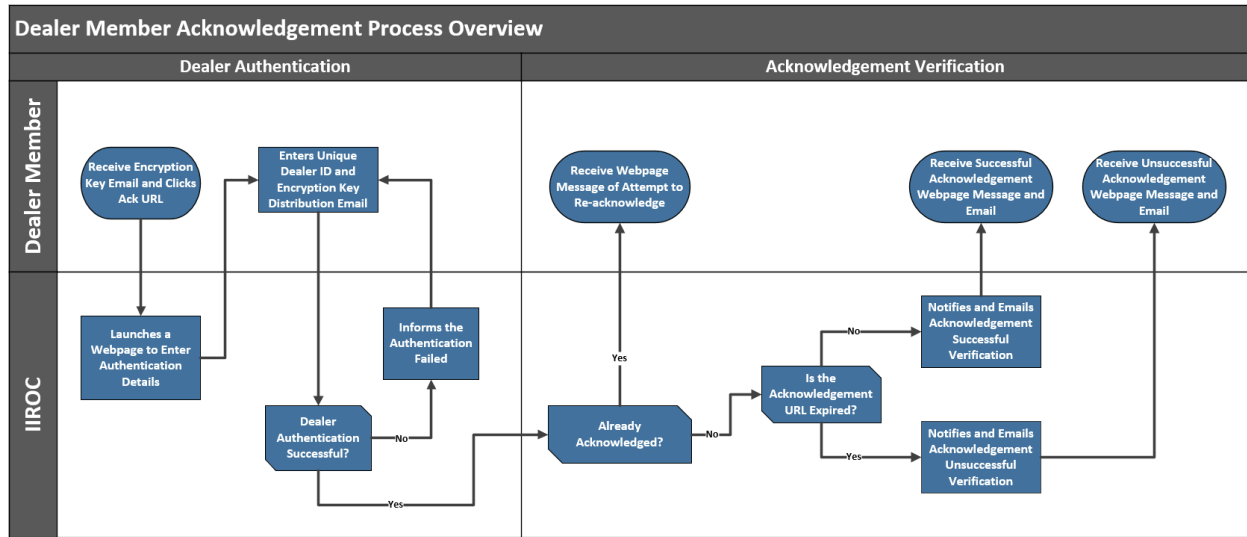
The Secure Acknowledgement URL is the concluding component contained within the Secure Encryption Key Email. The URL allows the Dealer Member to acknowledge receipt of their Encryption Key. The Secure Acknowledgement URL expires after 7 calendar days, consequently if the Dealer Member does not acknowledge receipt of their Encryption Key within 7 calendar days of receiving the email, IIROC will send a new secure email (with an updated Secure Acknowledgement URL for the Dealer Member to acknowledge key receipt). IIROC sends up to 8 Secure Encryption Key Emails, if the Dealer Member does not acknowledge key receipt by the 8th Email, they will not receive further Emails from IIROC requesting to acknowledge receipt of their Encryption Key. After the 4th Secure Encryption Key Email is sent to the Dealer Member, if they still have not acknowledged key receipt via the Secure Acknowledgement URL, IIROC directly contacts the Dealer Member. IIROC also sends a Reminder Email 1 week before the new Encryption Keys go-live, this serves as a reminder for Dealer Members to implement their new Encryption Key.

Key Rollover Timeline



Date	Outcome
8 Weeks Prior to First Monday of April	8 weeks prior to the current Encryption Key's End Date (for the Production Launch the End Date is the Go-Live date), IIROC generates new Encryption Keys for Active Dealer Members and sends the initial Encryption Key Email via Secure Email (containing the Encryption Key and a Secure URL to acknowledge key receipt). The Secure Acknowledgement URL is valid for 7 calendar days.
7 Weeks Prior to First Monday of April	For unacknowledged Active Dealer Members with an expired Acknowledgement URL, a new URL is generated, and the second Encryption Key Emails are sent via Secure Email (containing the Encryption Key and an updated Secure URL to acknowledge key receipt).
6 Weeks Prior to First Monday of April	For unacknowledged Active Dealer Members with an expired Acknowledgement URL, a new URL is generated, and the third Encryption Key Emails are sent via Secure Email (containing the Encryption Key and an updated Secure URL to acknowledge key receipt).
5 Weeks Prior to First Monday of April	For unacknowledged Active Dealer Members with an expired Acknowledgement URL, a new URL is generated, and the fourth Encryption Key Emails are sent via Secure Email (containing the Encryption Key and an updated Secure URL to acknowledge key receipt).
4 Weeks + 1 Day Prior to First Monday of April	Unacknowledged Dealer Members are directly contacted by IIROC Staff.
4 Weeks Prior to First Monday of April	For unacknowledged Active Dealer Members with an expired Acknowledgement URL, a new URL is generated, and the fifth Encryption Key Emails are sent via Secure Email (containing the Encryption Key and an updated Secure URL to acknowledge key receipt).
3 Weeks Prior to First Monday of April	For unacknowledged Active Dealer Members with an expired Acknowledgement URL, a new URL is generated, and the sixth Encryption Key Emails are sent via Secure Email (containing the Encryption Key and an updated Secure URL to acknowledge key receipt).
2 Weeks Prior to First Monday of April	For unacknowledged Active Dealer Members with an expired Acknowledgement URL, a new URL is generated, and the seventh Encryption Key Emails are sent via Secure Email (containing the Encryption Key and an updated Secure URL to acknowledge key receipt).
1 Week Prior to First Monday of April	For unacknowledged Active Dealer Members with an expired Acknowledgement URL, a new URL is generated, and the eighth and final Encryption Key Emails are sent via Secure Email (containing the Encryption Key and an updated Secure URL to acknowledge key receipt). A Reminder Email is sent to all Active Dealer Members with expiring Encryption Keys.
1 Day Prior to First Monday of April	Encryption Keys Expire/ Project Go-Live Date.
First Monday of April	New Encryption Keys Go-Live.

Encryption Key Acknowledgement:



Once the Dealer Member receives their Secure Encryption Key Email from IIROC, they have the ability to acknowledge Encryption Key receipt via the Secure Acknowledgement URL in the email. The Dealer Member must acknowledge using the most recent Encryption Key Email sent by IIROC (less than 7 calendar days old, as the Secure Acknowledgement URL expires after 7 calendar days). Clicking the URL launches a webpage that prompts the Dealer Member to enter in their Unique Dealer ID and Dealer Email (in order for IIROC to authenticate the Dealer Member). The Unique Dealer ID and Dealer Email can both be found on the Secure Encryption Key Email sent.

Once the Dealer Member has been authenticated successfully, IIROC confirms if the Dealer Member has already successfully acknowledged receipt of their Encryption Key (since the Encryption Key Email is sent to a distribution list, multiple recipients can attempt to acknowledge receipt of the Encryption Key). If there has already been successful Encryption Key receipt acknowledgment, IIROC notifies the Dealer Member (via webpage message). If there has not been successful Encryption Key receipt acknowledgment, the Secure Acknowledgement URL is validated (IIROC checks if the URL has expired). If the URL is valid the Dealer Member is notified via webpage message and secure email that the Encryption Key receipt acknowledgment is successful. If the URL is not valid the Dealer Member is notified via webpage message and secure email that the Encryption Key receipt acknowledgment is unsuccessful (unsuccessful validation only occurs if the URL clicked is from an Encryption Key Email more than 7 calendar days old).