CIRO · OCRI

Canadian Investment Regulatory Organization

Organisme canadien de réglementation des investissements

Client Identifiers - Encryption Key Management Information for CIRO Dealer Members

Version 1.1

January 28, 2026

Table of Contents:

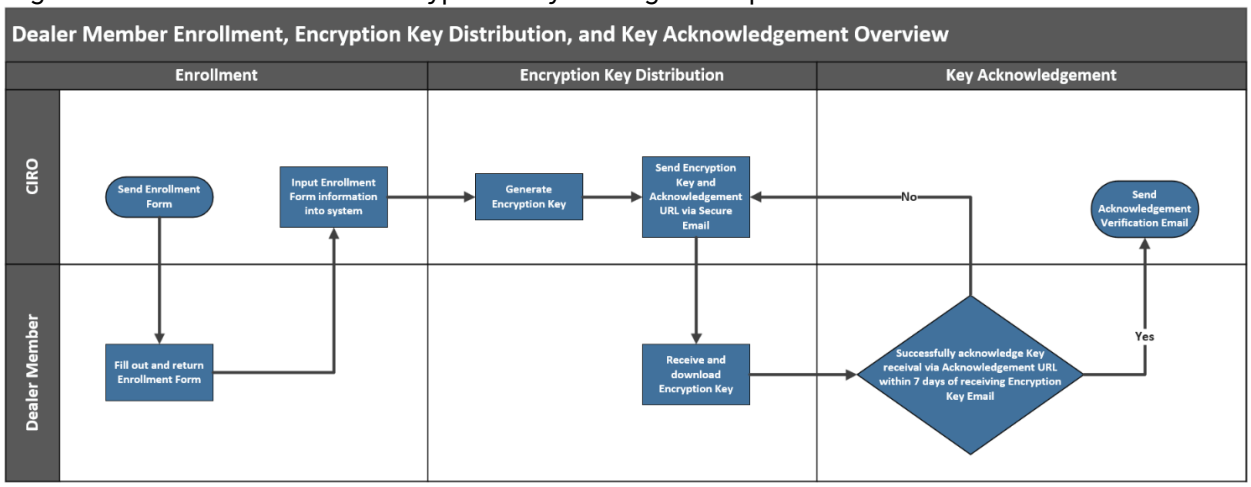
Overview:

The Canadian Investment Regulatory Organization (CIRO) is the national self-regulatory organization which oversees all investment dealers and trading activity on debt, derivative, and equity marketplaces in Canada. Created in 2023 through the consolidation of the Investment Industry Regulatory Organization of Canada (IIROC) and Mutual Funds Dealer Association (MFDA), CIRO sets high quality regulatory and investment industry standards, protects investors and strengthens market integrity while maintaining efficient and competitive capital markets. CIRO carries out its regulatory responsibilities through setting and enforcing rules regarding the proficiency, business and financial conduct of dealer firms and their registered employees and through setting and enforcing market integrity rules regarding trading activity on Canadian markets.

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 Receival Acknowledgement process.

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



Dealer Member Enrollment:

Enrollment Form to be sent to the Dealer Member CCO via email. The Dealer Member must fill out and return the Enrollment Form to CIRO (**clientidentifiers@ciro.ca**) no later then 14 days of receipt of the email. Returning the completed the Enrollment From is a prerequisite for generating the Dealer Members Encryption Key; all fields on the Enrollment Form are mandatory. The Dealer Member is responsible for maintaining the Encryption Key Distribution Email specified on the Enrollment Form (this distribution list is where the Dealer Members 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:

_____

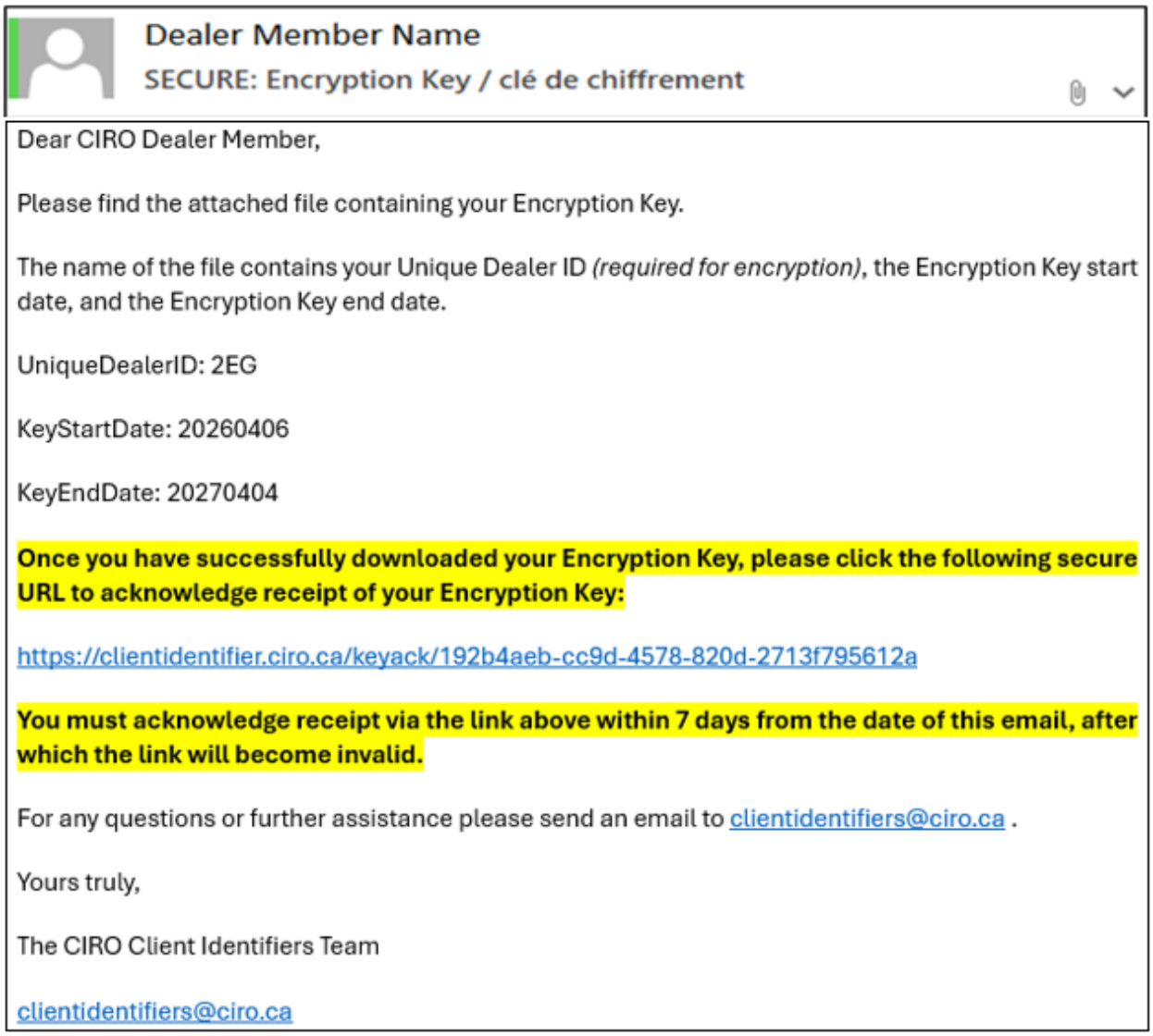
Phone:

_____

Encryption Key Information and Distribution:

CIRO distributes the Dealer Members 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:



Dealer Member Name

SECURE: Encryption Key / clé de chiffrement

Dear CIRO Dealer Member,

Please find the attached file containing your Encryption Key.

The name of the file contains your Unique Dealer ID *(required for encryption)*, the Encryption Key start date, and the Encryption Key end date.

UniqueDealerID: 2EG

KeyStartDate: 20260406

KeyEndDate: 20270404

Once you have successfully downloaded your Encryption Key, please click the following secure URL to acknowledge receipt of your Encryption Key:

https://clientidentifier.ciro.ca/keyack/192b4aeb-cc9d-4578-820d-2713f795612a

You must acknowledge receipt via the link above within 7 days from the date of this email, after which the link will become invalid.

For any questions or further assistance please send an email to clientidentifiers@ciro.ca .

Yours truly,

The CIRO Client Identifiers Team

clientidentifiers@ciro.ca

Encryption Key File Attachment Information:

Encryption Key Filename Format: UniqueDealerID_StartDate_EndDate.key e.g. E2G_20260406_20270404.key Encryption Key File Content: 24-character Base64 Encoded Encryption Key e.g. 3JpUwHDS0ZJHhWiJS5HPBg==

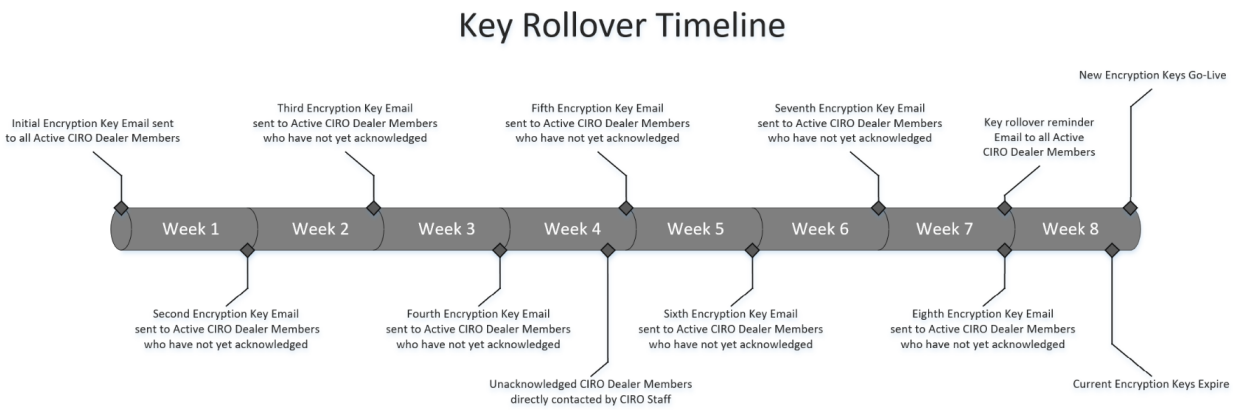
The Encryption Key is sent along with the Dealer Members Unique Dealer ID (this ID is required when encrypting the client information), the Encryption Keys Start Date, the Encryption Keys End Date, as well as a Secure URL that allows the Dealer Member to acknowledge receival of their Encryption Key.

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

The Unique Dealer ID is a 3-Character alphanumeric ID that CIRO has generated for the Dealer Member (this ID is permeant; it will not change yearly like the Encryption Key). The Unique Dealer ID is contained within the email body as well as 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 CIRO to identify which Dealer Member has encrypted the information. CIRO can then decrypt using the Dealer Members corresponding Encryption Key; for more information on the encryption process please refer to the **Strategy for Encryption of Client Identifiers** section on the CIRO Website.

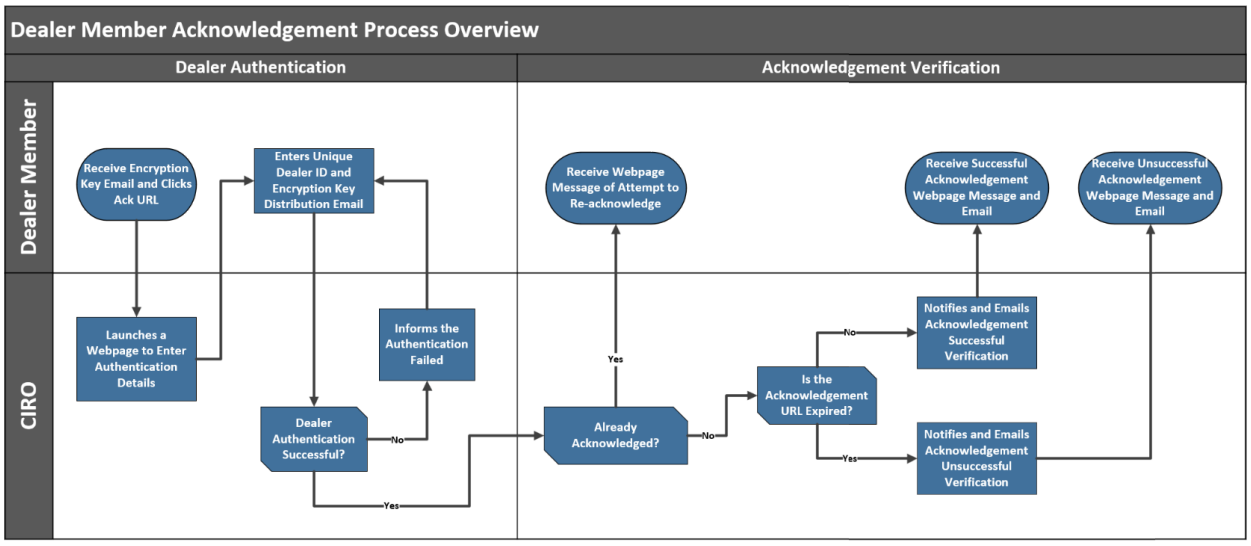
The Encryption Key Start Date and End Date are also contained within the email body as well as the filename. The format for the Start and End Dates in the filename is “YYYYMMDD”, and in the email body is “Month Day, Year”. For the initial distribution (Production Launch) as well as the Key Rollover Process (yearly process for sending the new Encryption Keys), the new Encryption Keys are generated and sent out 8 weeks prior to the current Encryption Keys 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 days, consequently if the Dealer Member does not acknowledge receival of their Encryption Key within 7 days of receiving the email, CIRO will send a new secure email (with an updated Secure Acknowledgement URL for the Dealer Member to acknowledge key receival). CIRO sends up to 8 Secure Encryption Key Emails, if the Dealer Member does not acknowledge key receival by the 8th Email, CIRO does not send further Emails. After the 4th Secure Encryption Key Email is sent to the Dealer Member, if they still have not acknowledged key receival via the Secure Acknowledgement URL, CIRO directly contacts the Dealer Member. CIRO 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 Keys.



Date	Outcome
8 Weeks Prior to First Monday of April	8 weeks prior to the current Encryption Keys End Date (for the Production Launch the End Date is the Go-Live date), CIRO generates new Encryption Keys for Active Dealer Members and send the initial Encryption Key Email via Secure Email (containing the Encryption Key and a Secure URL to acknowledge key receival). The Secure Acknowledgement URL is valid for 7 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 receival).
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 receival).
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 receival).
4 Weeks + 1 Day Prior to First Monday of April	Unacknowledged Dealer Members are directly contacted by CIRO 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 receival).
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 receival).
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 receival).
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 Encryption Key Emails are sent via Secure Email (containing the Encryption Key and an updated Secure URL to acknowledge key receival).
	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 CIRO, they have the ability to acknowledge Encryption Key receival via the Secure Acknowledgement URL in the email. The Dealer Members must acknowledge using the most recent Encryption Key Email sent by CIRO (less than 7 days old, the Secure Acknowledgement URL expires after 7 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 CIRO 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, CIRO confirms if the Dealer Member has already successfully acknowledged receival of their Encryption Key (since the Encryption Key Email is sent to a distribution list, multiple recipients can attempt to acknowledge receival of the Encryption Key). If there has already been successful Encryption Key receival acknowledgment, CIRO notifies the Dealer Member (via webpage message). If there has not been successful Encryption Key receival acknowledgment, the Secure Acknowledgement URL is validated (CIRO 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 receival acknowledgment is successful. If the URL is not valid the Dealer Member is notified via webpage message and secure email that the Encryption Key receival acknowledgment is unsuccessful (unsuccessful validation only occurs if the URL clicked is from an Encryption Key Email more then 7 days old).