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

Identifiants des clients – Renseignements sur la gestion des clés de chiffrement à l'intention des courtiers membres de l'OCRCVM

Version 1.0

19 août 2020

Table des matières

TABLE DES MATIÈRES 2

APERÇU 2

INSCRIPTION DU COURTIER MEMBRE 3

DESCRIPTION ET DISTRIBUTION DES CLÉS DE CHIFFREMENT 4

ACCUSÉ DE RÉCEPTION DE LA CLÉ DE CHIFFREMENT 7

Aperçu

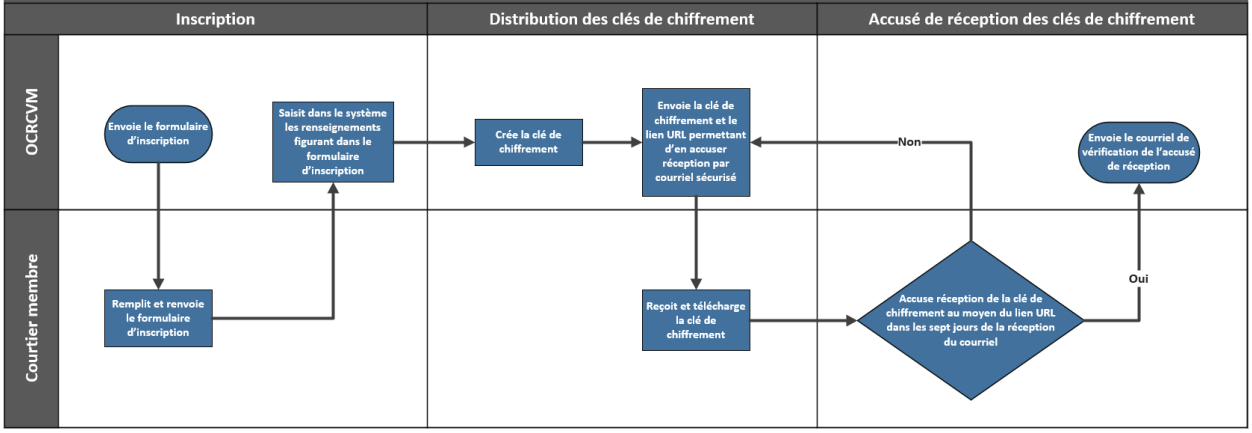
L'OCRCVM est l'organisme d'autoréglementation pancanadien qui surveille l'ensemble des courtiers en placement et toutes les opérations que ceux-ci effectuent sur les marchés des titres de capitaux propres et des titres de créance au Canada. L'OCRCVM établit la réglementation en matière de commerce des valeurs mobilières, veille à la protection des investisseurs et renforce l'intégrité des marchés tout en favorisant des marchés financiers sains au Canada. Il s'acquitte de ses responsabilités de réglementation en établissant et en faisant appliquer des règles qui régissent la compétence, les activités et la conduite financière de 175 courtiers en placement canadiens et des quelque 30 000 employés inscrits qui y travaillent, dont la plupart sont communément appelés conseillers en placement. L'OCRCVM établit et fait appliquer également des règles d'intégrité du marché qui régissent les opérations effectuées sur les marchés canadiens des titres de capitaux propres et des titres de créance.

Le 15 avril 2019, les autorités en valeurs mobilières compétentes ont approuvé les Modifications apportées aux Règles universelles d'intégrité du marché (RUIM) et aux Règles des courtiers membres afin d'exiger la mention de l'identifiant du client.

La gestion des clés de chiffrement est un volet essentiel du projet concernant les identifiants des clients. Le présent document décrit le processus d'inscription des courtiers membres, le processus de distribution des clés de chiffrement et le processus d'accusé de réception des clés de chiffrement.

Aperçu général des trois processus de gestion des clés de chiffrement traités dans le présent document :

Vue d'ensemble des processus d'inscription des courtiers membres, de distribution des clés de chiffrement et d'accusé de réception des clés de chiffrement



Inscription du courtier membre

L'OCRCVM entreprend le processus en envoyant le formulaire d'inscription au chef de la conformité du courtier membre par courriel. Le courtier membre doit remplir le formulaire d'inscription et le renvoyer à l'OCRCVM (à l'adresse clientidentifiers@iiroc.ca) dans les 14 jours civils suivant la réception du courriel. Le renvoi du formulaire d'inscription rempli constitue une condition préalable à l'émission de la clé de chiffrement du courtier membre; tous les champs du formulaire sont obligatoires. Le courtier membre doit tenir et mettre à jour l'adresse courriel correspondant à la liste de distribution utilisée pour l'envoi de la clé de chiffrement, laquelle figure sur le formulaire d'inscription (cette liste indique à qui la clé de chiffrement du courtier membre est envoyée).

Gestion des clés de chiffrement – Modifications concernant les identifiants des clients
Inscription du courtier membre

Renseignements sur le courtier membre

Dénomination sociale du courtier membre :

_____

Identifiant pour entité juridique (LEI) ou numéro de participant :

_____

Adresse :

_____

Ville : _____ Province : _____ Code postal : _____

Principale personne-ressource

Nom :

_____

Téléphone : _____ Courriel : _____

Autre personne-ressource

Nom :

_____

Téléphone : _____ Courriel : _____

Destinataires de la clé de chiffrement

Liste de distribution (adresse courriel) :

_____

Autorisation du courtier membre

Nom :

_____

Titre :

_____

Signature :

_____

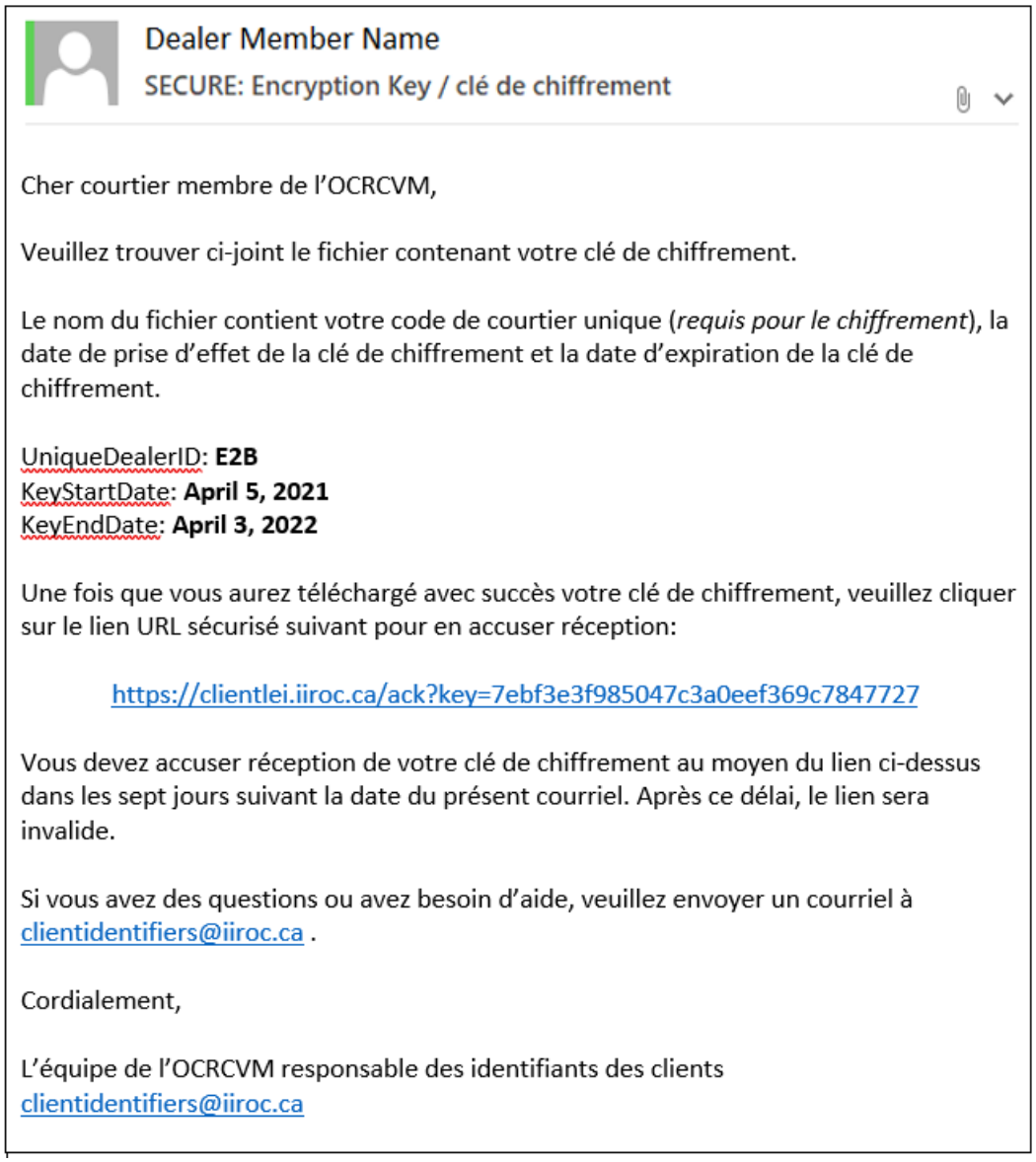
Téléphone :

_____

Description et distribution des clés de chiffrement

L'OCRCVM envoie la clé de chiffrement du courtier membre (sous forme de fichier texte) à l'adresse courriel correspondant à la liste de distribution prévue à cet effet, laquelle figure sur le formulaire d'inscription, par courriel sécurisé.

Modèle de courriel à utiliser pour l'envoi de la clé de chiffrement :



Dealer Member Name

SECURE: Encryption Key / clé de chiffrement

Cher courtier membre de l'OCRCVM,

Veuillez trouver ci-joint le fichier contenant votre clé de chiffrement.

Le nom du fichier contient votre code de courtier unique (*requis pour le chiffrement*), la date de prise d'effet de la clé de chiffrement et la date d'expiration de la clé de chiffrement.

UniqueDealerID: **E2B**
KeyStartDate: **April 5, 2021**
KeyEndDate: **April 3, 2022**

Une fois que vous aurez téléchargé avec succès votre clé de chiffrement, veuillez cliquer sur le lien URL sécurisé suivant pour en accuser réception:

https://clientlei.iiroc.ca/ack?key=7ebf3e3f985047c3a0eef369c7847727

Vous devez accuser réception de votre clé de chiffrement au moyen du lien ci-dessus dans les sept jours suivant la date du présent courriel. Après ce délai, le lien sera invalide.

Si vous avez des questions ou avez besoin d'aide, veuillez envoyer un courriel à clientidentifiers@iiroc.ca .

Cordialement,

L'équipe de l'OCRCVM responsable des identifiants des clients
clientidentifiers@iiroc.ca

Description du fichier de la clé de chiffrement joint au courriel :

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==

La clé de chiffrement est envoyée avec le code de courtier unique du courtier membre (ce code est requis pour chiffrer le LEI du client), la date de prise d'effet de la clé de chiffrement, la date d'expiration de la clé de chiffrement ainsi qu'un lien URL sécurisé permettant au courtier membre d'accuser réception de sa clé de chiffrement.

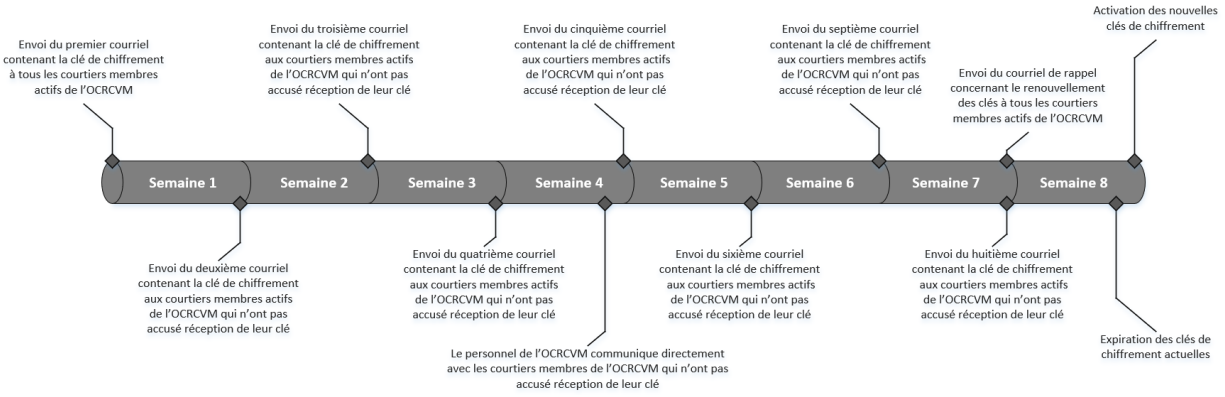
La clé de chiffrement est composée de données de 128 bits et chiffrée au moyen de l'encodage Base64 (en texte ASCII de 24 caractères). Elle est indispensable pour chiffrer le LEI du client avant sa transmission. La clé de chiffrement est renouvelée tous les ans.

Le code de courtier unique est un code alphanumérique de trois caractères que l'OCRCVM crée pour le courtier membre (ce code est permanent et ne change pas tous les ans comme la clé de chiffrement). Le corps du courriel et le nom du fichier de la clé de chiffrement joint au courriel contiennent le code de courtier unique. Le courtier membre doit indiquer son code de courtier unique sur les renseignements chiffrés concernant les clients, ce qui permet à l'OCRCVM de déterminer quel courtier membre a chiffré les renseignements. L'OCRCVM peut ensuite déchiffrer ces renseignements à l'aide de la clé de chiffrement correspondante du courtier membre (pour en savoir plus sur le processus de chiffrement, se reporter à la section « Stratégie de chiffrement des identifiants des clients » du site Internet de l'OCRCVM : https://www.ocrcvm.ca/industry/Client-Identifiers/Pages/Technical-Specifications.aspx).

Le corps du courriel et le nom du fichier contiennent également la date de prise d'effet et la date d'expiration de la clé de chiffrement. Le format des dates de prise d'effet et d'expiration est « AAAAMMJJ » dans le nom du fichier et « jour mois année » dans le corps du courriel. Lors de la distribution initiale (mise en production) et du renouvellement annuel des clés, la nouvelle clé de chiffrement est créée et envoyée huit semaines avant la date d'expiration de la clé de chiffrement actuelle (la date d'activation dans le cas de la mise en production). La nouvelle clé de chiffrement dure exactement 12 mois, sa date de prise d'effet étant fixée au premier lundi d'avril de l'année courante.

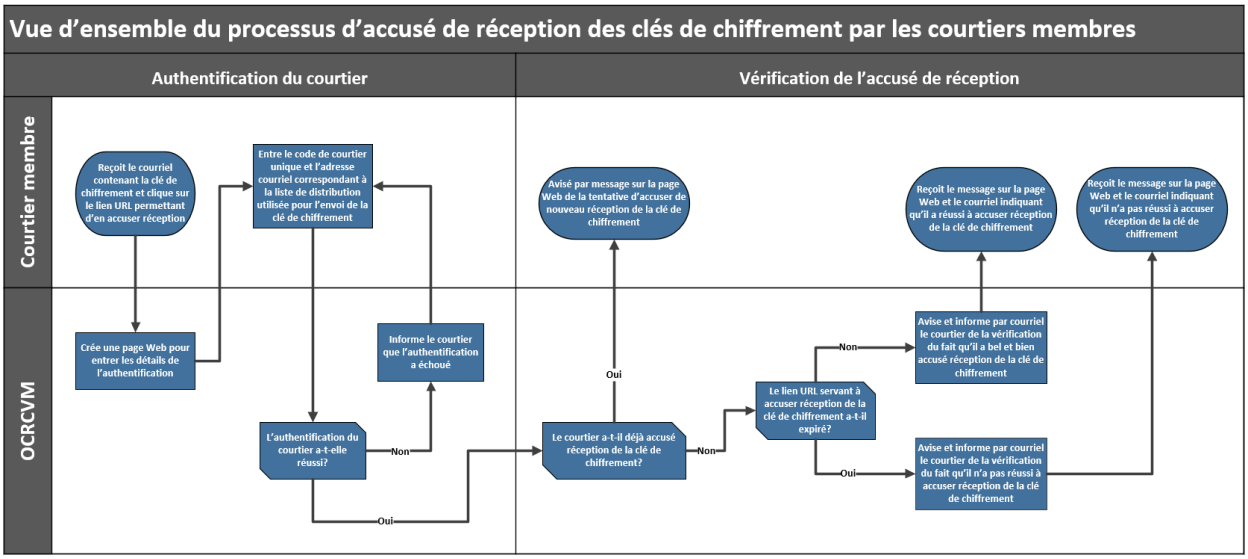
Le lien sécurisé servant à accuser réception de la clé de chiffrement est l'élément final du courriel sécurisé contenant la clé de chiffrement. Ce lien permet au courtier membre d'accuser réception de sa clé de chiffrement. Le lien URL sécurisé expire après sept jours civils; par conséquent, si le courtier membre n'accuse pas réception de sa clé de chiffrement dans les sept jours civils de la réception du courriel, l'OCRCVM lui enverra un nouveau courriel sécurisé (contenant un nouveau lien URL sécurisé lui permettant d'accuser réception de la clé). L'OCRCVM envoie ainsi jusqu'à huit courriels sécurisés. Si, au bout du huitième courriel, le courtier membre n'a toujours pas accusé réception de la clé, il ne recevra plus de courriels de l'OCRCVM lui demandant d'accuser réception de sa clé de chiffrement. Si, après l'envoi du quatrième courriel sécurisé au courtier membre, ce dernier n'a toujours pas accusé réception de la clé au moyen du lien URL sécurisé, l'OCRCVM communique directement avec lui. Une semaine avant l'activation des nouvelles clés de chiffrement, l'OCRCVM envoie également un courriel au courtier membre afin de lui rappeler de mettre en œuvre sa nouvelle clé de chiffrement.

Calendrier de renouvellement des clés



Date	Résultat
Huit semaines avant le premier lundi d'avril	Huit semaines avant la date d'expiration de la clé de chiffrement actuelle (la date d'activation dans le cas de la mise en production), l'OCRCVM crée les nouvelles clés de chiffrement pour les courtiers membres actifs et envoie le premier courriel sécurisé contenant la clé de chiffrement et un lien URL sécurisé permettant d'en accuser réception. Le lien URL sécurisé est valide sept jours civils.
Sept semaines avant le premier lundi d'avril	Si un courtier membre actif n'a pas accusé réception de sa clé de chiffrement et que le lien URL permettant d'en accuser réception a expiré, l'OCRCVM crée un nouveau lien URL et envoie un deuxième courriel sécurisé contenant la clé de chiffrement et le nouveau lien.
Six semaines avant le premier lundi d'avril	Si un courtier membre actif n'a pas accusé réception de sa clé de chiffrement et que le lien URL permettant d'en accuser réception a expiré, l'OCRCVM crée un nouveau lien URL et envoie un troisième courriel sécurisé contenant la clé de chiffrement et le nouveau lien.
Cinq semaines avant le premier lundi d'avril	Si un courtier membre actif n'a pas accusé réception de sa clé de chiffrement et que le lien URL permettant d'en accuser réception a expiré, l'OCRCVM crée un nouveau lien URL et envoie un quatrième courriel sécurisé contenant la clé de chiffrement et le nouveau lien.
Quatre semaines + un jour avant le premier lundi d'avril	Le personnel de l'OCRCVM communique directement avec les courtiers membres qui n'ont pas accusé réception de leur clé de chiffrement.
Quatre semaines avant le premier lundi d'avril	Si un courtier membre actif n'a pas accusé réception de sa clé de chiffrement et que le lien URL permettant d'en accuser réception a expiré, l'OCRCVM crée un nouveau lien URL et envoie un cinquième courriel sécurisé contenant la clé de chiffrement et le nouveau lien.
Trois semaines avant le premier lundi d'avril	Si un courtier membre actif n'a pas accusé réception de sa clé de chiffrement et que le lien URL permettant d'en accuser réception a expiré, l'OCRCVM crée un nouveau lien URL et envoie un sixième courriel sécurisé contenant la clé de chiffrement et le nouveau lien.
Deux semaines avant le premier lundi d'avril	Si un courtier membre actif n'a pas accusé réception de sa clé de chiffrement et que le lien URL permettant d'en accuser réception a expiré, l'OCRCVM crée un nouveau lien URL et envoie un septième courriel sécurisé contenant la clé de chiffrement et le nouveau lien.
Une semaine avant le premier lundi d'avril	Si un courtier membre actif n'a pas accusé réception de sa clé de chiffrement et que le lien URL permettant d'en accuser réception a expiré, l'OCRCVM crée un nouveau lien URL et envoie un huitième et dernier courriel sécurisé contenant la clé de chiffrement et le nouveau lien.
	L'OCRCVM envoie un courriel de rappel à tous les courtiers membres actifs dont la clé de chiffrement arrive à expiration.
Un jour avant le premier lundi d'avril	Expiration des clés de chiffrement / lancement du projet
Premier lundi d'avril	Activation des nouvelles clés de chiffrement.

Accusé de réception de la clé de chiffrement



Lorsque le courtier membre reçoit le courriel sécurisé contenant la clé de chiffrement de l'OCRCVM, il peut en accuser réception au moyen du lien URL sécurisé contenu dans le courriel. Le courtier membre doit utiliser le lien URL figurant dans le plus récent courriel envoyé par l'OCRCVM (datant de moins de sept jours civils, puisque le lien expire après ce délai). Le lien URL mène à une page Web qui invite le courtier membre à entrer son code de courtier unique et son adresse courriel (afin que l'OCRCVM puisse l'authentifier). Le code de courtier unique et l'adresse courriel du courtier se trouvent tous deux dans le courriel sécurisé contenant la clé de chiffrement.

Une fois le courtier membre authentifié, l'OCRCVM vérifie si l'accusé de réception de la clé de chiffrement a réussi (étant donné que le courriel contenant la clé de chiffrement est envoyé à une liste de distribution, plusieurs destinataires peuvent avoir tenté d'en accuser réception). Si oui, l'OCRCVM en avise le courtier membre (par message sur la page Web). Autrement, l'OCRCVM vérifie si le lien URL sécurisé est toujours valide. Si c'est le cas, il avise le courtier membre par message sur la page Web et par courriel sécurisé que l'accusé de réception de la clé de chiffrement a réussi. Si le lien n'est plus valide, l'OCRCVM avise le courtier membre par message sur la page Web et par courriel que l'accusé de réception de la clé de chiffrement a échoué (cela se produit seulement lorsque le courtier membre clique sur le lien URL à partir d'un courriel qui date de plus de sept jours civils).