Comité National SEPA

Guide de bonnes pratiques pour la constitution de la Référence Unique de Mandat (RUM)

Le passage au prélèvement SEPA entraîne l'apparition d'un nouveau document, le mandat de prélèvement SEPA, qui vient remplacer la demande et l'autorisation de prélèvement national. A chaque mandat de prélèvement SEPA correspond une Référence unique de mandat (RUM) qui, couplée à l'Identifiant Créancier SEPA (ICS) propre à chaque créancier, permet d'identifier de manière précise le contrat sous-jacent à tout prélèvement SEPA.

La RUM étant diffusée au payeur avant tout prélèvement SEPA, elle est susceptible d'être détournée par un tiers à des fins frauduleuses, et doit donc faire l'objet d'une série de recommandations visant à en garantir la sécurité.

1/ Définition des données dites sensibles

Certaines données ou fractions de données permettant une reconstitution complète de la donnée initiale doivent être considérées comme sensibles lorsqu'elles sont susceptibles d'une réutilisation frauduleuse pour l'émission d'ordres de paiement non autorisés par le détenteur du compte débité. Ces données sensibles recouvrent ainsi principalement les identifiants de compte de type International Bank Account Number (IBAN) ou Relevé d'Identité Bancaire (RIB), ainsi que les numéros de carte de paiement. Pour cette raison, il convient que tous les acteurs économiques qui sont en possession de telles données, et notamment les créanciers, les manient avec précaution.

D'autres données (numéro de carte d'identité, de passeport, de sécurité sociale, etc.) ne devraient pas apparaître dans la RUM d'un mandat de prélèvement SEPA en ce qu'elles sont susceptibles de détournement frauduleux. Leur traitement n'entre toutefois pas dans le cadre de ce guide.

2/ Recommandations à l'attention des créanciers pour la constitution des RUM

a. Éviter l'utilisation des données sensibles pour la constitution de la RUM

Il est recommandé aux créanciers d'éviter d'utiliser les données identifiées comme sensibles lors de la constitution des RUM des mandats de prélèvement SEPA qu'ils produisent. En effet, la RUM faisant partie des éléments transmis aux débiteurs, des risques réels de détournement de cette information existent, pouvant mener à des mouvements de fonds non autorisés sur les comptes des débiteurs dont les identifiants ont été détournés.

b. Aménagements à apporter dans les cas où des créanciers utiliseraient déjà des données sensibles pour constituer des RUM

Dans le cas où un créancier utiliserait déjà les données sensibles évoquées ci-dessus pour la constitution des RUM de ses mandats de prélèvement, des solutions pourraient être mises en

œuvre afin d'empêcher l'utilisation frauduleuse de ces données, dans la mesure des possibilités techniques laissées à ce créancier et à condition que ces solutions ne remettent pas en cause sa migration vers le prélèvement SEPA.

Les solutions envisagées pourraient consister en un masquage total ou partiel des données utilisées ou dans l'élaboration d'algorithmes propres à chaque créancier permettant de modifier les données apparaissant dans la RUM tout en gênant le moins possible le traitement en interne des contrats.

La mise en place de solutions de masquage ou d'algorithmes ne peut remettre en question l'obligation qu'à chaque mandat de prélèvement SEPA ne corresponde qu'un seul couple RUM/ ICS. En aucun cas les solutions choisies ne doivent mener à l'existence de plusieurs RUM différentes pour un unique mandat de prélèvement SEPA.

Le masquage total ou partiel de données sensibles déjà utilisées dans des RUM ou la mise en place d'algorithmes modifiant complètement des RUM existantes entraînent nécessairement une modification de ces RUM et donc un amendement aux mandats de prélèvement SEPA concernés. L'amendement des mandats de prélèvement SEPA doit suivre les procédures déterminées par l'European Payments Council (EPC) dans ses recueils de règles, ainsi que par le Comité français d'organisation et de normalisation bancaires (CFONB) dans sa brochure « Le prélèvement SEPA – SEPA Core Direct Debit ».

- **Le masquage total ou partiel des données de la RUM**

Le masquage des données sensibles s'entend comme un remplacement dans la RUM de caractères déterminés par d'autres caractères choisis de manière aléatoire ou prédéfinie (à la convenance du créancier et selon son besoin).

Les méthodes de masquage que peuvent employer les créanciers sont laissées à leur libre convenance. Le masquage peut être réalisé à l'aide de tous les caractères autorisés dans la RUM par les recueils de règles de l'EPC, soit l'ensemble des lettres de l'alphabet latin en minuscules et majuscules, les chiffres de 0 à 9, tous les signes suivants : / - ? : ( ) . , ' + et l'espace.

Les solutions de masquage peuvent être totales ou partielles. Un masquage partiel doit, pour être efficace, empêcher la reconstitution complète de la donnée initiale. Dans les deux cas, le créancier s'assurera que la solution retenue lui permet bien de garantir l'unicité du couple RUM/ICS pour chaque mandat.

En vue de garantir leur efficacité la plus grande possible, les solutions de masquage doivent :

- pour les identifiants de compte de type IBAN/RIB, masquer les caractères significatifs, soit le numéro de compte ou l'une de ses parties (voir annexe).

- pour les numéros de carte de paiement, masquer les caractères significatifs, soit ceux qui ne font pas partie du code BIN (voir annexe). L'utilisation des numéros de carte de paiement est déjà soumise à un ensemble de règles de la profession qu'il convient également de respecter dans le cadre de la constitution de la RUM d'un mandat de prélèvement SEPA.

- **L’élaboration d’algorithmes permettant de modifier les données apparaissant dans la RUM**

Les créanciers qui utiliseraient déjà des données sensibles pour la constitution des RUM de leurs mandats de prélèvement SEPA pourraient mettre au point des algorithmes permettant de modifier les données apparaissant dans celles-ci. Il s’agirait alors pour les créanciers de déterminer une règle permettant de transformer les données sensibles actuellement utilisées en données aléatoires.

Cette solution pourrait permettre aux créanciers concernés de continuer à utiliser les solutions existantes pour le traitement interne de leurs fichiers tout en proposant en sortie pour les mandats de prélèvement SEPA des RUM ne contenant aucune donnée sensible.

Annexe : Structure détaillée des données sensibles mentionnées dans le guide

International Bank Account Number (IBAN)

Pour l'IBAN français composé de 27 caractères, la structure est la suivante :

FR	14	20041	01005	**05 0001 3M026**	06
Code pays	Clé	Code banque	Code guichet	**Numéro de compte**	Clé

Le numéro de compte correspond aux onze caractères compris entre la 15ème et la 25ème position de l'IBAN. Le masquage peut concerner la totalité des caractères du numéro de compte ou seulement certains d'entre eux si cette dernière solution empêche la reconstitution du numéro de compte dans son intégralité.

Relevé d'Identité Bancaire (RIB)

Pour le RIB français composé de 23 caractères, la structure est la suivante :

20041	01005	**0500013M026**	06
Code banque	Code guichet	**Numéro de compte**	Clé RIB

Le numéro de compte correspond aux onze caractères compris entre la 11ème et la 21ème position du RIB. Le masquage peut concerner la totalité des caractères du numéro de compte ou seulement certains d'entre eux si cette dernière solution empêche la reconstitution du numéro de compte dans son intégralité.

Numéro de carte de paiement

Pour les numéros de carte de paiement utilisés en France et composés de 16 caractères, la structure est la suivante :

1234 56	**78 9123 456**	7
Code BIN	**Numéro d'identification de la carte**	Chiffre de contrôle

Les caractères à masquer recouvrent les 10 derniers chiffres du numéro de la carte de paiement (numéro d'identification de la carte et chiffre de contrôle). Le masquage peut concerner la totalité de ces caractères ou seulement une partie d'entre eux si cela permet d'empêcher la reconstitution de l'intégralité de la donnée initiale ; il est impératif que lors de l'établissement de la RUM ce masquage suive les dernières règles professionnelles en vigueur dans le domaine.