E-TRANSACTIONS

Guide des bonnes pratiques sur la sécurisation et le stockage de la clé HMAC

VERSION DU

01/03/2015

AVERTISSEMENT

Les informations contenues dans ce document n'ont aucune valeur contractuelle. Elles peuvent faire l'objet de modification à tout moment. Elles sont à jour en date de rédaction au 01/03/2015.

E-transactions est une solution d'encaissement et de gestion des paiements à distance par carte bancaire, dans un environnement sécurisé, distribuée par les Caisses régionales de Crédit Agricole.
Renseignez-vous auprès de votre conseiller sur les conditions générales et tarifaires de cette solution.

Cette documentation peut être enrichie par vos commentaires. Vous pouvez nous envoyer un email à support@e-transactions.fr, en indiquant votre remarque aussi précisément que possible. Merci de préciser la référence du document ainsi que le numéro de la page.

ASSISTANCE

Pour tout renseignement ou assistance à l'installation et à l'utilisation de nos produits, nos Equipes restent à disposition des commerçants et Intégrateurs, du lundi au vendredi de 9H à 18H30 :

Support Technique & Fonctionnel :

E-mail : support@e-transactions.fr

Téléphone : 0 810 812 810 810 *(1)*

(1) prix d'un appel local non surtaxé depuis un poste fixe

Pour tout contact auprès de nos services, il faut IMPERATIVEMENT communiquer les identifiants :

- numéro de SITE (7 chiffres)
- numéro de RANG (2 chiffres)
- numéro d'identifiant (1 à 9 chiffres)

TABLE DES MATIERES

1. GLOSSAIRE

Abréviations	Signification
HMAC	keyed-hash message authentication code (RFC 2104) (EN) code d'authentification d'une empreinte cryptographique de message avec clé (FR)
API	Application Programming Interface (EN) Interface de programmation (FR)
ZIP	Format de fichier permettant l'archivage et la compression des données

2. PRESENTATION DE LA CLE HMAC

HMAC (pour Hash-based Message Authentication Code) est un protocole standard (RFC 2104) permettant de vérifier l'intégrité d'une chaîne de données et utilisé sur la solution E-transactions pour vérifier l'authenticité du site Marchand qui se connecte.

3. CREATION ET UTILISATION DE LA CLE HMAC

3.1 Création de la clé HMAC dans Vision Commerçant

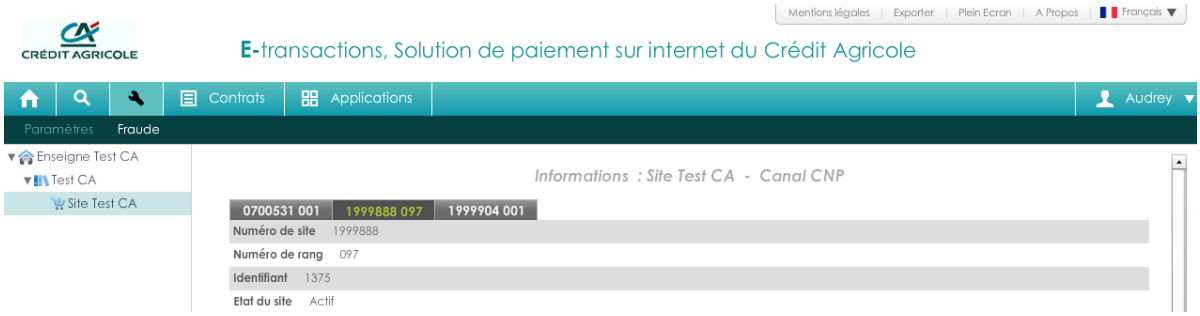
Cette clé est indispensable, elle permet d'authentifier tous les messages échangés entre le site marchand et les serveurs E-transactions. Le commerçant doit générer sa propre clé confidentielle.

Cette clé valide l'identité du commerçant et sécurise les échanges avec E-transactions. Elle ne doit en aucun cas être diffusée.

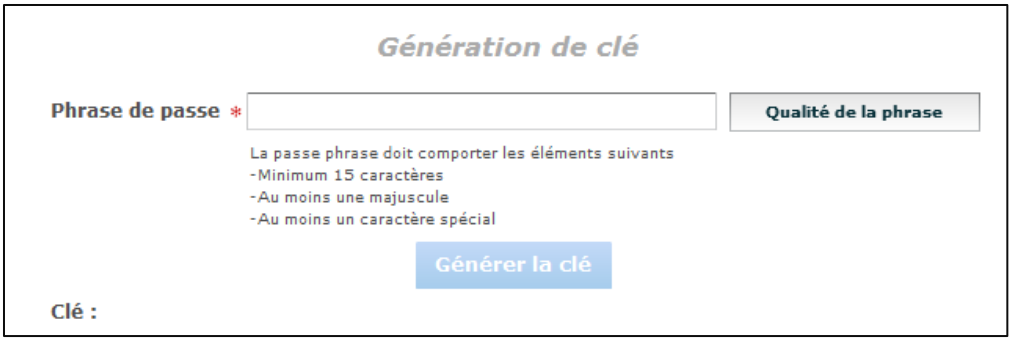
3.1.1 Génération

La clé HMAC est différente suivant l'environnement choisit pour le module. Pour générer une clé HMAC, il faut se rendre dans le Back Office E-transactions :

- De « test » si le module est en mode « test » : https://preprod-guest.e-transactions.fr/Vision/.
- De « production » si le module est en mode « production » : https://guest.e-transactions.fr/Vision/.



L'interface de génération de la clé HMAC se trouve dans l'onglet « Informations », en bas de la page.



Le champ « Phrase de passe » peut être renseigné avec une phrase, un mot de passe ou tout autre texte.

Le champ « Qualité de la phrase» est mis à jour automatiquement lorsque la « phrase de passe » est saisie. Ce champ permet de vérifier que les règles de sécurité d'acceptation minimales de la « phrase de passe » sont respectées (minimum 15 caractères, au moins une majuscule et au moins un caractère spécial et une force de 90 %). Le bouton « Générer la clé » restera grisé tant que ces limitations ne sont pas respectées.

La force de la « phrase de passe » est calculée selon plusieurs critères spécifiques : le nombre de majuscules, minuscules, caractères spéciaux, etc. Il conviendra donc de varier les caractères saisis, de les alterner et d'éviter les répétitions qui tendent à diminuer le score final.

Le bouton « Générer la clé » permet de calculer la clé HMAC à partir de la « phrase de passe » saisie. Ce calcul est une méthode standard assurant le caractère aléatoire de la clé et renforçant sa robustesse. Cette méthode de calcul étant fixe, il est possible à tout moment de retrouver sa clé en retapant la même phrase de passe et en relançant le calcul.

Il est possible que le calcul de la clé prenne quelques secondes, selon le navigateur Internet utilisé et la puissance de l'ordinateur. Au cours du calcul, il se peut que le navigateur Internet Explorer demande s'il faut "arrêter l'exécution de ce script". Il faut répondre "Non" à cette alerte et patienter jusqu'à la fin du calcul.

Une fois le calcul terminé, la clé sera affichée dans le champ « Clé ». Il faut alors copier/coller la clé HMAC dans le champ « HMAC » de la configuration du module sur le site marchand.

Le bouton « Générer la clé » est grisé par défaut. Il faut saisir une « phrase de passe » de plus de 15 caractères et dont la force est de plus de 90% pour rendre le bouton actif.

Après validation du formulaire, le marchand va recevoir un email de demande de confirmation de création de clé HMAC (avec lien de confirmation).

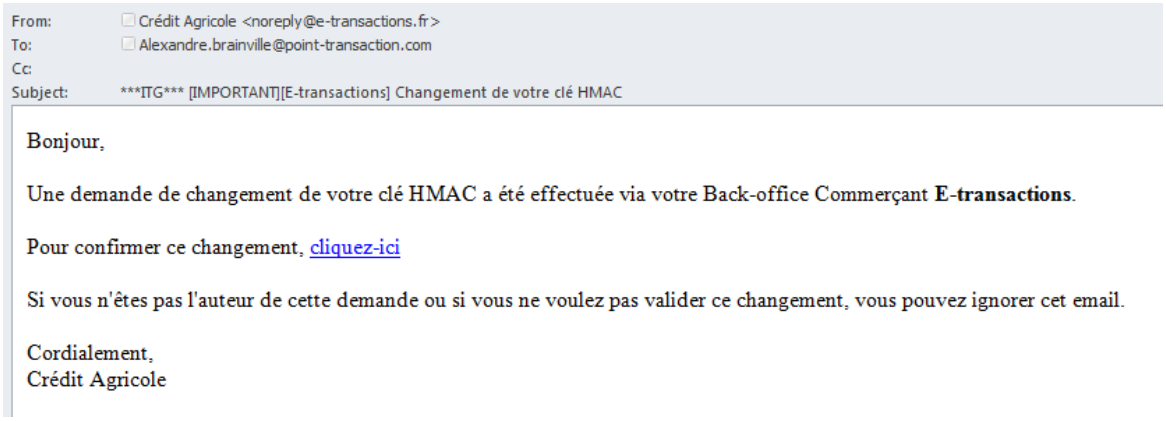
La clé qui vient d'être générée n'est active qu'une fois la procédure décrite dans l'email respectée.

La clé est affichée sous le bouton « Générer la clé ». Pour des raisons de sécurité, cette clé ne sera jamais transmise ni demandée par nos services. Par conséquent, si cette clé est égarée, il sera nécessaire d'en générer une nouvelle. **Il est important de veiller conserver de manière sécurisée la clé d'authentification affichée, avant de quitter la page.**

La clé est dépendante de l'environnement dans lequel elle est générée. Cela signifie qu'il faut générer une clé pour l'environnement de test **et** une pour l'environnement de production.

3.1.2 Validation

Une fois l'enregistrement de la nouvelle clé effectué, un email de demande de confirmation est envoyé au commerçant. Dans cet email se trouvera un lien pointant sur le programme "CBDValid.cgi". Voici un exemple de mail :



From: Crédit Agricole <noreply@e-transactions.fr>
To: Alexandre.brainville@point-transaction.com
Cc:
Subject: ***ITG*** [IMPORTANT][E-transactions] Changement de votre clé HMAC

Bonjour,

Une demande de changement de votre clé HMAC a été effectuée via votre Back-office Commerçant **E-transactions**.

Pour confirmer ce changement, cliquez-ici

Si vous n'êtes pas l'auteur de cette demande ou si vous ne voulez pas valider ce changement, vous pouvez ignorer cet email.

Cordialement,
Crédit Agricole

Après avoir cliqué sur ce lien, si un message annonce « Clé Hmac confirmée », alors la clé est immédiatement en fonction. Ce qui signifie que la clé qui vient d'être validée doit impérativement être aussi en fonction sur le site Marchand.

3.1.3 Expiration

Lorsque la clé est validée, celle-ci est valable 1 an.

Passé ce délai, pour permettre au site marchand de continuer à fonctionner, la clé n'est pas désactivée. Cependant le commerçant est averti par email, et sur la page d'accueil du Back Office E-transactions,de la nécessité de générer une nouvelle clé HMAC afin de garantir une sécurité optimale.

3.1.4 Transmission

La clé HMAC ne doit en aucun cas être transmise par e-mail SANS SECURISATION (fichier chiffré). E-transactions ne la demandera jamais au commerçant. Les commerçants doivent donc être particulièrement vigilants quant aux demandes suspectes de transmission de la clé d'authentification, il s'agit probablement d'une tentative de phishing ou de social engineering.

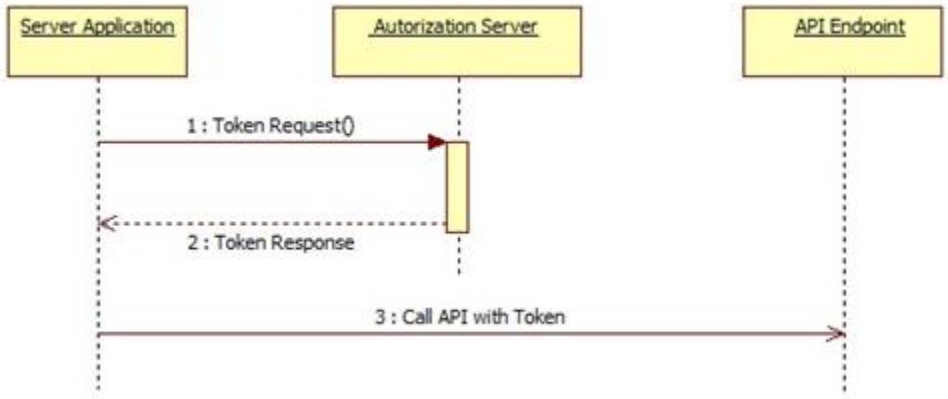
En cas de perte de la clé secrète, E-transaction ne sera pas en mesure de la redonner. Il faudra en générer une nouvelle via le Back Office Vision.

3.2 Creation de la clé HMAC via l'API HMAC

Procédure à l'usage des intégrateurs, agences web, prestataires techniques.
L'utilisation de cette procédure requière la création préalable d'un compte intégrateur auprès de E-transactions. Cela vous donnera accès à des web services spécifiques de génération de clé.

3.2.1 Autorisation d'une requête

Votre application doit envoyer une demande d'authentification en communiquant le login et mot de passe intégrateur. En retour, si l'authentification est valide, E-transactions renvoie un token. Ce Token sera ensuite utilisé pour les envois, dans le champ « Authorization » du header http pour l'ensemble des appels Web Services. La durée de validité du token est de 20 min. Au-delà, il faut en demander un nouveau.



3.2.1.1 DEMANDE DE TOKEN

La demande de token est un appel POST HTTPs dont le corps URL est encodé. L'appel est à diriger vers l'URL ci-dessous :

```
https://guest.e-transactions.fr/Vision/API/v1/token
```

Les deux paramètres ci-dessous sont obligatoires dans le POST HTTPs.

Name	Description
login	Login du compte intégrateur
password	Mot de passe du compte intégrateur

Veuillez trouver ci-dessous un exemple du POST HTTPs utilisé dans la demande de token :

```
POST Vision/API/v1/token HTTP/1.1
Host : guest.e-transactions.fr
Content-Type: application/json

{
        "login": "integ",
        "password": "P12345!89"
}
```

3.2.1.2 REPONSE

Le Serveur d'autorisation renvoie une réponse au format JSON. L'exemple ci-dessous nous montre une réponse type.

```
{
"access_token" : "srct69hmq1hrc23r3q5me2jhb7",
"expires" : 1357042332
}
```

Le token d'accès est délivré par le Serveur d'autorisation E-transactions qui expire au bout de 20 minutes.

3.2.2 Automatisation de la clé HMAC

L'API est un touil facilitant le travail d'intégration concernant la génération de la clé HMAC et concerne principalement des profils techniques. Cet objet gère la génération automatique de clé d'authentification HMAC. Veuillez trouver en bas de cette page les méthodes pour cette ressource.

3.2.2.1 REPRESENTATION DES RESSOURCES

```
{
        "site": {string},
        "rang": {string},
        "pass_phrase": {string},
        "hmac": {
                        "id": {string},
                        "key": {string},
                        "active_key": {boolean},
                        "used_key": {boolean},
                        "key_creation_date": {date},
                        "key_expiration_date": {date},
                        "key_stop_date": {date},
                        "key_used_onRMPI": {boolean},
                        "key_used_onPPPS": {boolean},
                        "key_used_onRESABON": {boolean},
        },
}
```

Property name	Value	Description	Restriction
site	string	site identifier (provided by the bank)	7 digits
rang	string	Rank identifier (provided by the bank)	3 digits
pass_phrase	string	Sentence for generate the HMAC key	15 digits
hmac	object		
id	string	HMAC Identifier	13 digits
key	string	HMAC key	256 digits
active_key	boolean	Active HMAC key flag (from Vision Commerçant : related to the email sent to the merchant with the activation link from the HMAC API : Automatically active. Just need to send an information email to the integrator)	O / N - by default "N" (from Vision commerçant) -by default "O" (from the HMAC API)
used_key	boolean	Used HMAC key flag (at least one time) - the status change when first payment call	O / N - by default "N"
key_creation_date	date	HMAC key creation date	YYYY-MM-DD
key_expiration_date	date	HMAC key expiration date	YYYY-MM-DD
key_stop_date	date	HMAC key deactivation date	YYYY-MM-DD - By default NULL
key_used_onRMPI	boolean	Used HMAC key on Remote MPI	O / N - by default "N"
key_used_onPPPS	boolean	Used HMAC key on PPPS	O / N - by default "N"
key_used_onRESABON	boolean	Used HMAC key on RESABON (terminate subscription)	O / N - by default "N"

3.2.2.2 METHODES

insert

Génère / Renouvèle la clé d'authentification HMAC

3.2.3 HMAC insert

| Require authorization

Retourne la clé d'authentification HMAC générée.

3.2.3.1 REQUETE

3.2.3.1.1 Requete HTTP

```
POST https://guest.e-transactions.fr/Vision/API/v1/hmac/insert/
```

3.2.3.1.2 Autorisation

Cette requête requiert "authorization".

3.2.3.1.3 Corps de la requête

Parameter name	Value	Description
Required parameters		
site	string	Site (provided by the bank)
rang	string	Rang (provided by the bank)
pass_phrase	string	Sentence for generate the HMAC key

3.2.3.2 RESPONSE

En cas de succès, cette méthode retourne la clé HMAC générée dans le corps de la requête.

3.2.3.3 EXAMPLES

3.2.3.3.1 Requête

```
POST https://guest.e-transactions.fr/Vision/API/v1/hmac/insert/
Authorization: Paybox srct69hmq1hrc23r3q5me2jhb7r
{
        "site": "1999888",
        "rang": "02",
        "pass_phrase": "atw%py8BJR2k&lz",
}
```

3.2.3.3.2 Réponse

```
200 OK
{
        "site": "1999888",
        "rang": "02",
        "pass_phrase": "atw%py8BJR2k&lz",
        "hmac": {
                        "id":"9800000000008",
                        "key":
"KTPBRXBA5C4FC8EE49C91D82A61A7633CCC4BDC12111F78B838162249PP9BF62288E1385DA1C
E37271E691338FF42212E5C18C123CFFAA048ECFB773DB8D1E075D8EB081E487A62FDFE6AB58F
13EFB19",
                        "active_key":"O",
                        "used_key":"N",
                        "key_creation_date":"2014-01-27",
                        "key_expiration_date":"2015-01-27",
                        "key_stop_date":"",
                        "key_used_onRMPI":"N",
                        "key_used_onPPPS":"N",
                        "key_used_onRESABON":"N",
                },
}
```

3.2.4 Messages d'erreurs

3.2.4.1 REPRESENTATION DES MESSAGES

Property name	Value	Description
code	integer	error code
message	string	description of the error

3.2.4.2 CODES D'ERREURS

Code	Value	Scope
2000	Arguments manquants.	All
2001	Login ou mot de passe non renseigné.	All
2002	Erreur inconnue.	All
2003	Token d'accés manquant.	All
2004	Méthode HTTP invalide (GET, POST).	All
2005	Arguments invalides.	All
2006	Token non valide.	All
2007	Entité incorrecte.	All
2008	Fonction incorrecte.	All
2009	Fonction non implémentée.	All
2010	Tous les champs requis ne sont pas remplis.	All
2019	Le content-type doit être application/json.	All

3000	Code d'application inconnu.	Contrats
3001	Insertion impossible: contrat existant.	Contrats
3002	Type de contrat inexistant.	Contrats
3020	Numéro logique invalide.	Contrats
3021	Code d'application invalide.	Contrats
3022	Format d'email invalide.	Contrats
3023	Le contrat existe déjà.	Contrats
3024	Code banque invalide.	Contrats
3025	Contrat inexistant.	Contrats
3026	Mise à jour échouée: données invalides.	Contrats
3027	Mise à jour échouée: champ renseigné non modifiable.	Contrats
3028	Mise à jour échouée: x25address est manquant dans bank.	Contrats
3100	Entreprise parente introuvable.	Company
3101	Type du parent invalide.	Company
3102	Suppression impossible: le magasin a un contrat.	Company
3103	Suppression impossible: le magasin a un sous-site.	Company
3104	Suppression impossible: la sous-enseigne a un magasin.	Company
3105	Suppression impossible: l'enseigne a une sous-enseigne.	Company
3106	Entreprise introuvable.	Company
3107	Erreur interne.	Company
3108	Suppression impossible: le magasin a un contrat léger.	Company
3200	Site ou Rang incorrect.	HMAC
3201	Phrase de passe incorrecte.	HMAC
3202	Données incorrectes.	HMAC

3.2.4.3 EXEMPLES

```
200 OK
{
        "code": 3106,
        "message": "Entreprise introuvable."
}
```

Paragraphe ci-dessous à mettre mettre au niveau des erreurs

Si une erreur se produit lorsque le client est redirigé vers la plateforme de paiement E-transactions, vérifiez que la clé HMAC renseignée correspond bien à celle de l'environnement actif.

4. RISQUE ASSOCIE A L'UTILISATION DE LA CLE HMAC

La compromission de la clé HMAC, utilisée pour le calcul de l'empreinte HMAC a pour conséquence de ne plus garantir l'intégrité des données et l'identification du commerçant lors des échanges.

Il est impératif de protéger cette clé aussi bien lors de son stockage que de son utilisation. Il convient aussi de conserver une copie sécurisée de la clé (archivage) afin de permettre une réactivation rapide du service en cas de dégradation ou de perte du support principal **:**

- L'archivage de la clé doit être réalisé sur un support durable, sécurisé (encrypté) et isolé du système opérationnel,
- La mise en œuvre opérationnelle de la clé doit aussi faire l'objet d'une sécurisation, support crypté, et contrôle d'accès au système l'hébergeant,
- Le stockage « en clair » dans un fichier ou sur tout autres supports quelle qu'en soit la nature est à proscrire.

5. DIFFUSION DE LA CLE HMAC

La communication de données sensibles doit être sécurisée, c'est-à-dire que la confidentialité, l'intégrité et l'authenticité des informations doivent être assurées.

Concernant la confidentialité de la communication :

- Chiffrer les données avant leur enregistrement sur le support lorsque la transmission de données s'effectue par l'envoi d'un support physique.

- Lors d'un envoi via un réseau :
  - Si cette transmission utilise la messagerie électronique, chiffrer les pièces à transmettre.
  - S'il s'agit d'un transfert de fichiers, utiliser un protocole garantissant la confidentialité, tel que SFTP ;
  - Si cette transmission utilise le protocole HTTP, utiliser le protocole SSL (HTTPS) pour assurer l'authentification des serveurs la confidentialité des communications.

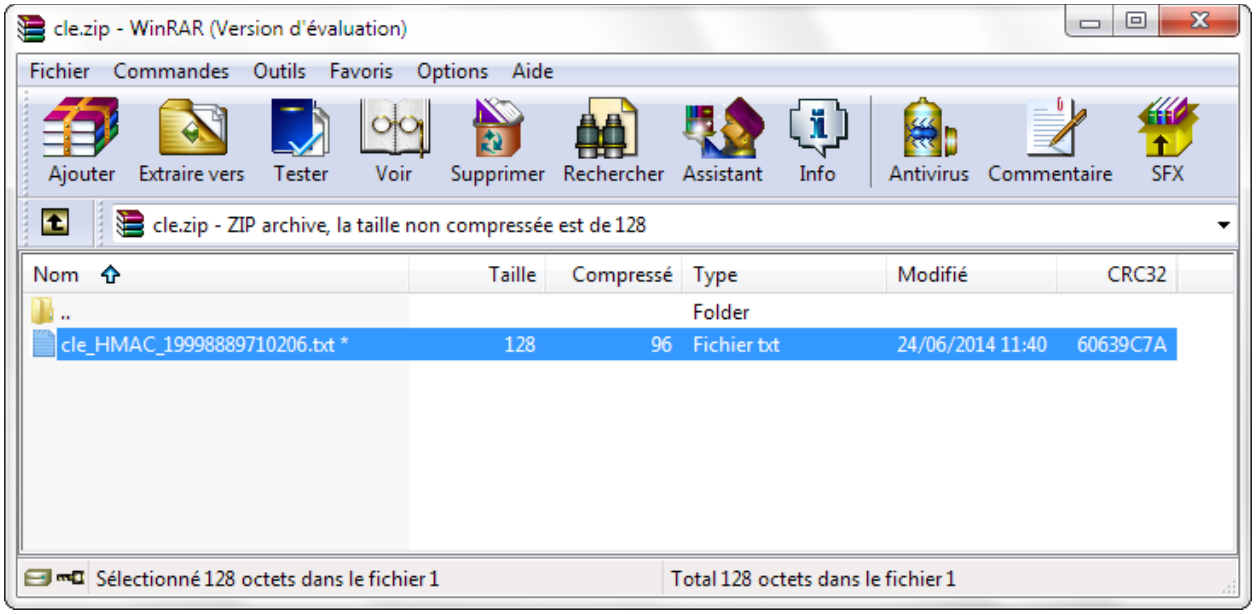
- Dans tous les cas, la transmission du secret (clé de déchiffrement, mot de passe, etc.) garantissant la confidentialité du transfert doit s'effectuer dans une transmission distincte, si possible via un canal de nature différente de celui qui servira à la transmission des données (par exemple, envoi du fichier chiffré par mail et communication du mot de passe par téléphone ou SMS).

La gestion de la clé HMAC ne doit jamais se faire en communiquant à un tiers,ses identifiants (login / mot de passe) de connexion au back office Vision.

Si ce tiers doit récupérer la clé HMAC, vous devez générer la clé sur le Back Office Vision et lui transmettre via email (Voir procédure ci-dessous).

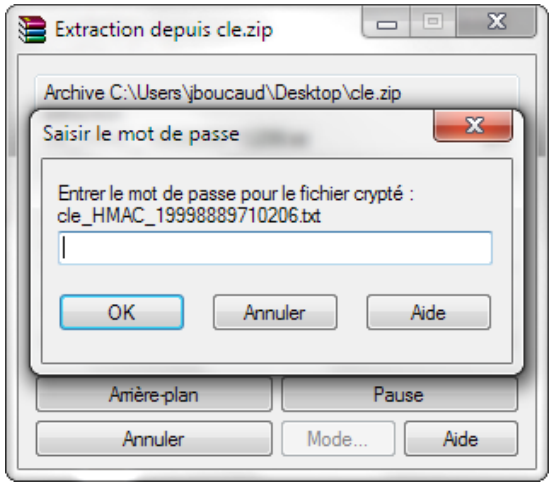
5.1 Par email

- Récupérer la clé HMAC (depuis le back office Vision ou l'API HMAC).
- Copier la clé HMAC dans un fichier texte.
- Mettre le fichier texte dans une archive avec mot de passe.



- Envoyer ensuite l'archive avec mot de passe dans un 1er email.
- Envoyer le mot de passe associé à l'archive par un autre moyen (SMS …) afin que le destinataire puisse récupérer la clé HMAC.

Voici le rendu final, c'est-à-dire lors de l'ouverture de l'archive .zip



Une fois le mot de passe renseigné, l'accès aux fichier de l'archive est possible.