Introduction

Ce manuel, destiné à l'administration fiscale, fournit une documentation permettant de réaliser des archives et vérifier les signatures cryptographiques des documents exportés. Ces documentation vous expliquera à la fois comment obtenir un accès aux données pour un compte en particulier, comment obtenir une copie des archives et comment vérifier l'intégrité des données présentes dans ses rapports par le biais d'une fonction cryptographique HMAC SHA256

Connexion à votre espace

Il est possible d'obtenir des identifiants de connexion au logiciel qui vous donneront accès à des fonctionnalités spécifiquement étudiées pour l'administration fiscale.
Ces identifiants de connexion peuvent être obtenues par deux manières : soit directement auprès de l'établissement pour lequel le contrôle est effectué soit en s'adressant directement à l'éditeur de ce logiciel en contactant contact@net-assembly.com
L'établissement contrôlé à la possibilité de créer un compte pour l'administration fiscale en se rendant dans la page “Configuration”, “Utilisateurs” du logiciel. Dans cette page, il pourra utiliser le bouton Ajouter pour ajouter un nouvel utilisateur puis sélectionner comme droit utilisateur le droit intitulé : “Comptable”.
Une fois connecté avec vos identifiants utilisateur disposant des droits “Comptable”, vous aurez alors accès à une interface simplifiée du logiciel.
Le menu principal permettra d'accéder à différentes pages :

- “Historique” (historique des commandes) : permet d'accéder à la liste des commandes avec une interface graphique des outils de recherche une visualisation du ticket ainsi que des factures associées
- “Inalterabilite” : Permet d'accéder aux outils de vérification des signatures cryptographiques HMAC SHA256
- “Rapports” : Permet de générer des archives sur des plages temporelles
- “Aide” : Permet d'accéder à la documentation générale du logiciel

Génération d'archives

En page rapport il est possible de générer des archives portant sur une plage de date personnalisée.
Le format de fichier qui convient pour la génération d'archives fiscales et le fichier intitulé "Archive fiscale".
Ceci vous permettra d'obtenir un fichier au format ZIP contenant différents fichiers au format CSV.
Les fichiers CSV exportés sont : paiements, commandes, articles, fermetures, tracabilite
Les données de chaque fichier CSV sont signées à l'aide d'une chaine de signature HMAC-SHA256.
Chaque ligne étant signée à l'aide de deux fonctions, makeHashOrderAddB qui ajoute une clé publique propre à chaque établissement à la chaîne qui est signée, et signeMessage qui utilise le résultat de cette fonction pour appliquer la signature HMAC-SHA256
La méthode pour construire la chaîne qui est signée est indiquée pour chaque table dans ce même document.

```
$softwarePublicKey="myCustumSoftwareKey5d9RuGgµgéd_tçdjkdr";
function importFloat($floatNumber) {
    return round($floatNumber*1000000)/1000000;
}
function makeHashOrderAddB($idboutique,$hash) {
    global $softwarePublicKey;
    return $hash."_".sha1($idboutique.$softwarePublicKey);
}
function signeMessage($value) {
    global $theHiddenSecretKey;
    return hash_hmac('sha256', $value, $theHiddenSecretKey);
}
```

Données archivées

Commandes

- id : identifiant interne à l'application
- datecreation : **date de création** de la commande
- datevalidation : **date de validation** (affectation du numéro de facture)
- datevaleur : **date de valeur comptable**
- idboutique : identifiant interne de l'établissement
- idcaisse : identifiant interne de l'établissement
- idutilisateur : identifiant interne de l'établissement
- idmodepaiement : identifiant interne de l'établissement
- prixinitial : **avant TVA, avant reductions**
- totalreduction : total des réductions appliquées
- totaltva : **montant total de TVA**
- prixfinal : **prix final TTC**
- titre : **intitulé de la commande**
- typetva : champ interne (champ non fiscal)
- nbarticles : nombre d'articles
- montantpaye : champ interne (champ non fiscal)
- idcompteclient : identifiant interne de l'établissement
- modepaiement : champ interne (champ non fiscal)
- terminee : champ interne (champ non fiscal)
- note : champ interne (champ non fiscal)
- notePublique : champ interne (champ non fiscal)
- pieceID : champ interne (champ non fiscal)
- remboursement : champ interne (champ non fiscal)
- idinterne : le **numéro de facture** attribué à la commande lors de sa validation
- choixlivraison : identifiant interne de l'établissement
- idtable : identifiant interne de l'établissement
- preparation : champ interne (champ non fiscal)
- alivrer : champ interne (champ non fiscal)
- livraisonTerminee : champ interne (champ non fiscal)
- numcouverts : champ interne (champ non fiscal)
- pointsfidelite : champ interne (champ non fiscal)
- readyprepa : champ interne (champ non fiscal)
- dureePrepa : champ interne (champ non fiscal)
- dureePrepaOK : champ interne (champ non fiscal)
- numbippeur : champ interne (champ non fiscal)
- expediee : champ interne (champ non fiscal)

- factureEnvoyee : **compteur d'impression/envoi de facture**
- thehash : signature HMAC-SHA256 des champs fiscaux
- verifName : la signature recalculée lors de l'archive
- hashSource : la source du calcul de la signature
- validity : = "Valid HMAC SHA256" si la signature de la ligne correspond bien à la signature recalculée, sinon affiche "**** ERROR *****"

Format de la chaîne de caractères signée :
$c["datevalidation"]."_".$c["datevaleur"]."_".$c["idcaisse"]."_".importFloat($c["prixinitial"])."_".importFloat($c["totalreduction"])."_".importFloat($c["totaltva"])."_".importFloat($c["prixfinal"])."_".$c["typetva"]."_".importFloat($c["nbarticles"])."_".$c["choixlivraison"]."_".$c["id"]."_".$c["idinterne"]."_".$hash

Articles

- id : identifiant interne
- datecreation : date de l'ajout de l'article à la commande
- idboutique : identifiant interne de l'établissement
- idcommande : identifiant interne de commande
- idutilisateur : identifiant interne d'utilisateur
- idrayon : identifiant interne du rayon
- idplu : identifiant interne de l'article
- prixinitial : prix initial unitaire
- tauxtva : valeur du taux de TVA
- montantTvaDeductible : montant de TVA deductible
- tauxtva2 : montant de TVA en consommation sur place (champ non fiscal)
- tauxreduction : taux de réduction
- montantreduction : montant de réduction
- prixfinal : prix final TTC
- prixAchatPlu : prix achat (champ non fiscal)
- quantite
- nom : titre donnée à l'article
- image
- ventePartielle : champ interne (champ non fiscal)
- idpaiement : champ interne (champ non fiscal)
- preparation : champ interne (champ non fiscal)
- position : champ interne (champ non fiscal)
- idDeclinaison0-4 : champ interne (champ non fiscal)
- prixFinalHT : prix final HT
- thehash : signature de cette ligne
- verifName : la signature recalculée lors de l'archive
- hashSource : la source du calcul de la signature
- validity : = "Valid HMAC SHA256" si la signature de la ligne correspond bien à la signature recalculée, sinon affiche "**** ERROR *****"

Format de la chaîne de caractères signée :
$lasthash."_".$a["id"]."_".$a["datecreation"]."_".$a["idcommande"]."_".$a["idutilisateur"]."_".importFloat($a["prixinitial"])."_".importFloat($a["tauxtva"])."_".importFloat($a["montantTvaDeductible"])."_".importFloat($a["tauxtva2"])."_".importFloat($a["tauxreduction"])."_".importFloat($a["montantreduction"])."_".importFloat($a["prixfinal"])."_".importFloat($a["quantite"])."_".$a["nom"]."_".importFloat($a["prixFinalHT"])

Paiements

- id : identifiant interne
- idboutique : identifiant interne de l'établissement
- idCommande : identifiant interne de la commande payée
- idVendeur : identifiant interne de l'utilisateur
- idCaisse : identifiant interne de la caisse
- idTypePaiement : identifiant interne de
- idModePaiement : identifiant interne de
- idUtilisateurCreditPaiement : donnée interne
- datePaiement : la date du paiement = date d'enregistrement du paiement
- montantPaye : le montant payé
- montantVerse : le montant utilisé pour payer le commande (si rendu de monnaie, différent)
- gocardlessID : donnée interne
- thehash : signature de cette ligne
- verifName : la signature recalculée lors de l'archive
- hashSource : la source du calcul de la signature
- validity : = "Valid HMAC SHA256" si la signature de la ligne correspond bien à la signature recalculée, sinon affiche "**** ERROR *****"

Format de la chaîne de caractères signée :
$idcommande."_".$idUtil."_".$idCaisse."_".$datePaiement."_".$typeDeModesPaiement."_".$idModePaiement."_".importFloat($montantPaye)."_".importFloat($montantVerse)."_".$hash

Fermetures

La table qui enregistre les fermetures de caisses automatiques (quotidiennes, mensuelles, annuelles) s'intitule "fermeturesAuto".
Le logiciel procède automatiquement à des clôtures de caisse automatique. Ces clôtures de caisse enregistrent pour chaque clôture : le niveau de la clôture, le total sur la période, le total historique, la date de début et la date de fin de la période.
L'événement qui déclenche la clôture de caisse automatique est la tentative par l'utilisateur d'enregistrer ou de modifier une opération de caisse comme par exemple la validation d'une commande, l'enregistrement d'un paiement pour une commande, etc.
Cette clôture est effectuée de manière transparente sans que l'utilisateur soit averti de celle-ci et ne perturbe pas le processus de vente car elle est instantanée.
Cette clôture est réalisée à trois niveaux différents : quotidien, mensuel et annuel.
La clôture annuelle tient compte de la date de fin d'exercice de l'établissement tel que configuré dans la page configuration du logiciel.

- id : identifiant interne
- idboutique : identifiant interne de l'établissement
- dateStart : Date de début de période clôturée
- dateEnd : Date de fin de période clôturée
- idStart : Identifiant de la première commande de la période clôturée
- idEnd : Identifiant de la dernière commande de la période clôturée
- niveau : Niveau de clôture
- totalPeriode : Total du chiffre d'affaires sur la période clôturée
- totalHistorique : Total du chiffre d'affaires historique
- thehash : Y a-t-il un numérique de l'enregistrement
- thehash : signature de cette ligne
- verifName : la signature recalculée lors de l'archive
- hashSource : la source du calcul de la signature
- validity : = "Valid HMAC SHA256" si la signature de la ligne correspond bien à la signature recalculée, sinon affiche "**** ERROR *****"

Format de la chaîne de caractères signée:
$totaltsstart."_".$totaltsend."_".$totalidstart."_".$totalidend."_".importFloat($total)."_".importFloat($totalhistorique)."_".$lastHash

Traces

Cette table contient les données relatives à la traçabilité des opérations d'archivage. La purge n'étant pas effectuée dans le logiciel.
Les champs de l'archive sont :

- id : identifiant interne
- idboutique : identifiant interne de l'établissement
- idutilisateur : identifiant de l'utilisateur de l'établissement
- typeoperation : le type de l'opération (toujours 'archive')
- idcaisse : identifiant de la caisse
- dateoperation : la date de l'opération
- params : nom du fichier archivé
- idServer : l'adresse IP du serveur ayant réalisé l'opération traçée
- fileHash : signature HMAC-SHA256 du fichier archivé
- thehash : signature de cette ligne
- verifName : la signature recalculée lors de l'archive
- hashSource : la source du calcul de la signature
- validity : = "Valid HMAC SHA256" si la signature de la ligne correspond bien à la signature recalculée, sinon affiche "**** ERROR *****"

Format de la chaîne de caractères signée:
$c["idutilisateur"]."_".$c["typeoperation"]."_".$c["dateoperation"]."_".$c["params"]."_".$c["fileHash"]."_".$hash

Vérification des sceaux HMAC-SHA256

Il est mis à disposition de l'administration fiscale un outil permettant de vérifier les signatures HMAC SHA 256. Il est possible d'accéder à cet outil en vous rendant en page "Inaltérabilité" du logiciel.
Il suffit alors de saisir une chaîne de caractères puis de saisir la signature que vous avez obtenue de cette chaîne de caractère pour vérifier si celle-ci est bien exacte.
Le logiciel vous affichera si le résultat est un succès ou un échec.