Caisse.Enregistreuse

Dossier d'architecture technique

Version 0.9.6, dernière mise à jour le 14/10/2025 -
Net-assembly.com - Caisse.enregistreuse.fr

1. Architecture Générale

Le logiciel caisse.enregistreuse.fr repose sur une architecture SaaS multi-instance hébergée sur des serveurs Linux (Ubuntu 22.04) chez Digital Ocean, en data centers européens.

Application Web : Développée en PHP 8.2.

Base de données : MySQL 8, configurée en mode transactionnel réplication de base de données sur un serveur de réplication et procédure de sauvegarde automatisée réalisant une backup complète de la base de données dans un fichier zip au format SQL.

Serveurs : Accès sécurisé uniquement par les administrateurs Net-Assembly via SSH.

2. Sécurisation des flux et des données

- Tous les échanges entre client et serveur se font en HTTPS/TLS.
- Les bases de données sont protégées par firewall applicatif.
- Les signatures de transactions sont calculées et stockées immédiatement après enregistrement.

3. Enregistrements de commandes

3.1. Structure d'une commande

La base de données contient différents champs pour une commande.

La date de création de la commande, la date de validation de la commande, la date de valeur de la commande, l'identifiant de l'établissement d'utilisation du système d'encaissement, l'identifiant de la caisse, l'identifiant de l'utilisateur, l'identifiant du mode de paiement utilisé en tant que premier mode de paiement, le prix initial, le montant total des réductions, le montant total des TVA, le prix final total toute taxe comprise, un titre court pour la commande résumant les principaux articles de la commande, le nombre d'articles de la commande, le montant total payer pour cette commande, le numéro interne du compte client attaché à la commande, un champ indiquant si la commande est terminée ou non, une note privée sur la commande, note publique pour la commande, une pièce d'identité du client ayant effectuer cette commande, un champ indiquant s'il s'agit d'un remboursement ou d'un achat, un identifiant interne, le numéro de commande, la méthode de livraison, la

table sur lequel le client consomme, l'état de préparation de la commande, l'état de livraison de la commande, le nombre de couverts que constitue cette commande, le nombre de points de fidélité gagné avec cette commande, l'état de d'expédition de la commande l'état de facture envoyé de la commande, le sceau cryptographique de la commande, un numéro de bipper dans le cadre d'une gestion des bipeurs pour la préparation des commandes…

Chaque commande est constituée d'une liste d'articles chaque article disposant d'un prix initial, d'un prix final HT, d'un taux TVA, d'un montant de TVA, d'un taux de réduction si une réduction est appliquée ou d'un montant de réduction de réduction est appliquée en montant, d'un prix final, d'une quantité, d'un nom (libellé), d'une éventuelle image, d'un état de préparation d'un identifiant d'article.

A commande correspond une liste de règlement, la commande pouvant être payée en une seule ou plusieurs fois avec un seul mode de paiement ou plusieurs modes de paiement chaque paiement est enregistré en base de données avec à chaque fois la date du règlement le mode du règlement. Dès l'instant où le dernier règlement est enregistré pour la commande il devient impossible alors d'enregistrer d'autres règlements pour la commande ni d'en modifier.

3.2. Création et validation des commandes

Chaque commande doit passer par deux filtres afin d'être créée ou validée.

Les filtres pour ces deux opérations sont définis dans des fichiers dédiés :

Fichier "includes/article_add_check.php"

Contient les fonctions de vérification des conditions de création d'une nouvelle commande

```
if ($caisse[etat]=="N" || $caisse["id"]==0)
{
    ?>
    showErreurCaisse('<?=showTradJS("Veuillez ouvrir la caisse.")?>');
    showNotifInfoBox('<?=showTradJS("Veuillez ouvrir la caisse.")?>');
    getSystemPage('caisse_ouvre');
    <?
    die("");
}
if
(date("Y-m-d",strtotime($caisse[datedernierchangementetat])-60*60*$boutique[heureOuverture])<date("Y-m-d",
getBoutiqueTime()-60*60*$boutique[heureOuverture]) && $boutique["obligeFermeCaisseDaily"]==1 )
{
    ?>
    showErreurCaisse('<?=formatStr(showTradJS("La caisse n a pas ete fermee hier"),"Javascript")?>');
    showNotifInfoBox('<?=formatStr(showTradJS("La caisse n a pas ete fermee hier"),"Javascript")?>');
    getSystemPage('caisse_ferme');
    <?
    die("");
}
if
(date("Y-m",strtotime($caisse[datedernierchangementetat])-60*60*$boutique[heureOuverture])<date("Y-m",getB
outiqueTime()-60*60*$boutique[heureOuverture]) && $boutique["obligeFermeCaisseDaily"]==2 )
{
```


Version 0.9.6, dernière mise à jour le 14/10/2025 -
Net-assembly.com - Caisse.enregistreuse.fr

```
    ?>
    showErreurCaisse('<?=formatStr(showTradJS("La caisse n a pas ete fermee hier"),"Javascript")?>');
    showNotifInfoBox('<?=formatStr(showTradJS("La caisse n a pas ete fermee hier"),"Javascript")?>');
    getSystemPage('caisse_ferme');
    <?
    die("");
}
if (strtotime('+1 year', strtotime($caisse[datedernierchangementetat]))<getBoutiqueTime() &&
$boutique["obligeFermeCaisseDaily"]==3 )
{
    ?>
    showErreurCaisse('<?=formatStr(showTradJS("La caisse n a pas ete fermee hier"),"Javascript")?>');
    showNotifInfoBox('<?=formatStr(showTradJS("La caisse n a pas ete fermee hier"),"Javascript")?>');
    getSystemPage('caisse_ferme');
    <?
    die("");
}
```

Deux vérifications sont faites : vérification de la bonne ouverture d'une caisse, et vérification de l'obligation de fermeture de caisse quotidienne/mensuelle/annuelle

Fichier "includes/shouldStartNewOrder.php"

Contient les fonctions de vérification des conditions de modification d'une commande

```
<?php
if (intval($idcommande)==0 || mystrtotime ($commande[datevalidation])>0 )
{
    if ($boutique[choixlivraisonobligatoire] &&  $boutique[eatinspecialtva] )
    {
        ?>
        askDeliveryMethod();
        showNotifInfoBox('<?=showTradJS("Préciser le choix livraison/à emporter/sur place.")?>');
        <?
        die("");
    }
    if ($idplu==-1) die(" ");
    $idcaisse = $caisse["id"];
    $defDateValeur = 0;

    $query = "INSERT INTO commandes (datecreation, datevaleur, idboutique, idcaisse, idutilisateur,
idmodepaiement, prixinitial, totalreduction, totaltva, prixfinal, typetva, nbarticles,
montantpaye,choixlivraison) VALUES (FROM_UNIXTIME(?),0,?,?,?,null,?,?,?,?,?,?,? )";

mysql_q($query,array(getBoutiqueTime(),$idboutique,$idcaisse,$idutilisateur,$prixinitial,$totalreduction,$
totaltva, $prixfinal,$typetva, $nbarticles, 0, $defaultChoixlivraison) );

    $idcommande = getLastID();
    $query = "UPDATE utilisateurs SET idcommande=? WHERE id=? ";
    mysql_q($query,array($idcommande,$idutilisateur ) );
    $_SESSION['util']['idcommande'] = $idcommande;
    unset($commande);
    newOrderAction();
    echo "try {sIDc(".$idcommande."); } catch (e) {};";
}
else
{
    $shallUpdatePrixFinal = true;
}
```

Si la commande a déjà été validée, créer une nouvelle commande vierge pour y appliquer l'opération demandée.

Ceci rend donc impossible l'édition d'une commande validée.

Si des corrections modifications ou annulation sont apportées à des transactions, par quelque moyens que ce soit, ces corrections s'effectueront alors par un enregistrement de données d'encaissement corrective avec des opérations de plus ou de moins et non par modification directe des données d'encaissement enregistrées.

Fichier "includes/coreCert.php"

Contient toutes les fonctions liées aux signatures. Fonction de création du sceau cryptographique ; Fonction de validation d'une commande ; Fonction de génération de la clé cryptographique associée à la boutique

```
function validateOrderIntoInvoice($idcommande_i) {
    global $boutique,$idcommande;

    $idcommande = $idcommande_i;
    $validationOfOrderOK = true;
    updatePrixCommande ();

    $commande = mysql_one("SELECT * FROM commandes WHERE id=? ",array($idcommande));

    if (mystrtotime ($commande["datevalidation"])==0) {
        mysql_q("UPDATE commandes SET
datevalidation=FROM_UNIXTIME(".(getBoutiqueTime()).") WHERE id=? " , array($idcommande)
);
        $reload = true;
    }
    if ( mystrtotime ($commande[datevaleur])==0) {
        mysql_q("UPDATE commandes SET datevaleur=FROM_UNIXTIME(".(getBoutiqueTime()).")
WHERE id=? " , array($idcommande)  );
        $reload = true;
    }
    if ($reload) {
        $commande = mysql_one("SELECT * FROM commandes WHERE id=?
",array($idcommande));
    }

    $nextID = getCommandeNextID();

    //$query .= "UPDATE commandes SET
datevalidation=FROM_UNIXTIME(".(getBoutiqueTime()).")";
    $commande["idinterne"] = $nextID["maxID"];
    $query = "UPDATE commandes SET idinterne=".$commande["idinterne"];

    if ($nextID["thehash"] || $nextID["maxID"]==1) {
        $newHash =
makeHashOrder($boutique["id"],$commande,$nextID["thehash"],$nextID["maxID"]);

        $commande["thehash"] = $newHash;
        $query .= ",thehash='".$commande["thehash"]."'";
    }
    $query .= " WHERE idinterne=0 AND id=".$idcommande;
```

```
    /*echo $query;
     die();*/
    mysql_query_perso($query);

    mysql_q("UPDATE boutiques SET statNbSales=statNbSales+1 WHERE id=? ",
array($boutique[id] ) );

    return $commande;
}
function makeHashOrderAddB($idboutique,$hash) {
    return $hash."_".sha1($idboutique.$softwareSecretKey);
}
function makeHashOrder($idboutique,$c,$hash,$id) {
    $stringRes =
makeHashOrderAddB($idboutique,$c["datevalidation"]."_".$c["datevaleur"]."_".$c["idcaiss
e"]."_".$c["prixinitial"]."_".$c["totalreduction"]."_".$c["totaltva"]."_".$c["prixfinal
"]."_".$c["typetva"]."_".$c["nbarticles"]."_".$c["choixlivraison"]."_".$c["id"]."_".$c[
"idinterne"]."_".$hash."_".$id);
    return hash('sha256', $stringRes);
}
function getCommandeNextID() {
    global $boutique;
    my_sem_get("lockBoutique".$boutique["id"]);
    $i = mysql_q("SELECT max(idinterne) as maxid FROM commandes WHERE
idboutique=?",array($boutique["id"]));
    $maxid = $i[0][maxid];

    $c = mysql_one("SELECT thehash FROM commandes WHERE idboutique=? AND idinterne=?
LIMIT 1",array($boutique["id"],$maxid));
    return array("maxID"=>$maxid+1,"thehash"=>$c["thehash"]);
}

function updatePrixCommande () {
    global
$utilisateur,$boutique,$idcommande,$recalcTitre,$erreurReduction,$validationOfOrderOK;
    $comptabiliseCA = true;
    require "includes/export/calculePrixCommande.php";
    if ($validationOfOrderOK) {
        foreach ($pileArticlesRendus as $listedArt) {
            if ($listedArt["totalTTC"]) {
                mysql_q("UPDATE articles SET prixFinalHT=? WHERE
id=?",array($listedArt["totalTTC"]-$listedArt["totalTVA"],$listedArt["id"]));
            }
        }
    }
    //die();
    // un hack car sinon il faut recalculer les valeurs de prixfinal lors de la
suppression d'un article
    $montantTotalTVA = 0;
    foreach ($totauxTVA as $taux => $total)
        $montantTotalTVA += $total;
        $commande["prixfinal"] = priceImport($totalPrixFinal);
        $commande[totaltva] = $montantTotalTVA;

        if (!$erreurReduction) {
            $qP = "UPDATE commandes SET
nbarticles=".$nbTotalArticles.",prixfinal=".$totalPrixFinal.",totaltva=".$montantTotalT
VA." WHERE idinterne=0 AND id=".$idcommande."";
            mysql_query_perso($qP);
        }
        return $commande;
}
```

On trouve dans ce fichier les principales fonctions :

- validateOrderIntoInvoice : permet de transformer un devis en commande, donc lui affecter un numéro de commande, une date de valeur, un hash SHA 256
- makeHashOrder : fonction de création du hash SHA256
- getCommandeNextID : permet d'obtenir le prochain identifiant de commande
- makeHashOrderAddB : génére la clé privée d'un établissement à partir d'un sha1, et d'une clé privée du logiciel.
- updatePrixCommande : lors de la validation de la commande, calcule la valeur définitive des prix HT des articles de la commande, et les enregistre en base de donnée

3.3. Sécurisation des justificatifs

Le système d'encaissement permet de distinguer et d'identifier sans ambiguïté un justificatif émis avant paiement d'un justificatif émis après paiement. Tout justificatif réimprimé porte ainsi la mention duplicata. Le système assure la traçabilité des impressions et des réimpressions de justificatif de manière sécurisée. L'opération est enregistrée en base de données, côté serveur sans accès possible de la part du client. En cas de téléchargement, d'envoi par email ou d'envoi par SMS de la facture, le champ en base de données "factureEnvoyee" est **incrémenté**. Chacune des méthodes d'envoi des factures est soumise aux mêmes contraintes concernant l'émission et la rémission.

Les tickets doivent mentionner en fin de justificatif « Système de caisse certifié LNE ».

La procédure d'émission de justificatifs au format électronique est clairement documentée dans la page Aide du logiciel, incluant les protocoles d'envoi et les modalités de gestion des originaux et des duplicatas.

Ce mécanisme permet aussi que toute absence d'impression ou d'envoi de justificatif au format numérique soit enregistrée de manière sécurisée (le champ duplicata reste alors positionné à zéro).
Les tickets doivent mentionner en fin de justificatif « Système de caisse certifié LNE ».

Cf : https://caisse.enregistreuse.fr/logiciel-de-caisse-enregistreuse/facturation/

3.4. Signatures

Chaque table de donnée est signée par une chaîne cryptographique indépendante :

- commande
- articles
- paiements
- tracabilite (archives)
- fermeturesAutomatiques

Pour chaque table, la fonction de signature est la même : HMAC-SHA256

La fonction de signature n'a besoin que des paramètres :

- sourceHash (résulte de la concaténation des champs fiscaux de la table)
- idboutique (identifiant interne du compte de boutique/établissement)
- hash (signature du précédent enregistrement)

A partir du paramètre idboutique, génére une clé publique, qui sera concaténée à sourceHash et hash (avec underscore comme séparateur) puis ensuite la fonction hmac_sha256 est appliquée.

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 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);
}
```

3.4.1 Transactions

Chaque transaction est signée selon l'algorithme HMAC-SHA256, en chaînant chaque signature à celle de la transaction précédente, assurant l'intégrité de l'historique.

La signature d'une transaction se base sur les informations suivantes :

- prix final de la commande
- prix initial de la commande
- Date de valeur
- date de validation
- identifiant interne de la caisse ayant procédé à l'enregistrement
- montant total des réductions appliquées à la commande
- montant total de la TVA collectée

- nombre d'articles dans la commande
- choix de la méthode de livraison
- identifiant interne de la commande
- identifiant public de la commande
- hash cryptographique de la commande précédente portant le numéro interne inférieur
- identifiant interne de la boutique

```
function validateOrderIntoInvoice($idcommande_i) {
    global $boutique,$idcommande;

    $idcommande = $idcommande_i;
    updatePrixCommande ();

    $commande = mysql_one("SELECT * FROM commandes WHERE id=? ",array($idcommande));

    if (mystrtotime ($commande["datevalidation"])==0) {
        mysql_q("UPDATE commandes SET datevalidation=FROM_UNIXTIME(".(getBoutiqueTime()).") WHERE id=? " ,
array($idcommande)  );
        $reload = true;
    }
    if ( mystrtotime ($commande[datevaleur])==0) {
        mysql_q("UPDATE commandes SET datevaleur=FROM_UNIXTIME(".(getBoutiqueTime()).") WHERE id=? " ,
array($idcommande)  );
        $reload = true;
    }
    if ($reload) {
        $commande = mysql_one("SELECT * FROM commandes WHERE id=? ",array($idcommande));
    }

    $nextID = getCommandeNextID();

    $commande["idinterne"] = $nextID["maxID"];
    $query = "UPDATE commandes SET idinterne=".$commande["idinterne"];

    $newHash = makeHashOrder($boutique["id"],$commande,$nextID["thehash"],$nextID["maxID"]);

    $commande["thehash"] = $newHash;
    $query .= ",thehash='".$commande["thehash"]."'";

    $query .= " WHERE idinterne=0 AND id=".$idcommande;

    mysql_query_perso($query);

    mysql_q("UPDATE boutiques SET statNbSales=statNbSales+1 WHERE id=? ", array($boutique[id] ) );

    return $commande;
}
function makeHashOrderAddB($idboutique,$hash) {
    return $hash."_".sha1($idboutique."myCustumSoftwareKey5d9RuGgµgéd_tçdjkdr");
}
function makeHashOrder($idboutique,$c,$hash,$id) {
    $srcHash =
    $stringRes =
makeHashOrderAddB($idboutique,$c["datevalidation"]."_".$c["datevaleur"]."_".$c["idcaisse"]."_".$c["prixinitial"]."_".$c
["totalreduction"]."_".$c["totaltva"]."_".$c["prixfinal"]."_".$c["typetva"]."_".$c["nbarticles"]."_".$c["choixlivraison
"]."_".$c["id"]."_".$c["idinterne"]."_".$hash."_".$id);
    return hash('sha256', $stringRes);
}
function getCommandeNextID() {
          global $boutique;
          my_sem_get("lockBoutique".$boutique["id"]);
          $i = mysql_q("SELECT max(idinterne) as maxid FROM commandes WHERE idboutique=?",array($boutique["id"]));
          $maxid = $i[0][maxid];

          $c = mysql_one("SELECT thehash FROM commandes WHERE idboutique=? AND idinterne=? LIMIT
1",array($boutique["id"],$maxid));
          return array("maxID"=>$maxid+1,"thehash"=>$c["thehash"]);
}
```


Version 0.9.6, dernière mise à jour le 14/10/2025 -
Net-assembly.com - Caisse.enregistreuse.fr

3.4.2 Fermetures

La table qui enregistre les fermetures de caisse automatiques (quotidiennes, mensuelles, annuelles).
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

3.4.3 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"])

3.4.4 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

Version 0.9.6, dernière mise à jour le 14/10/2025 -
Net-assembly.com - Caisse.enregistreuse.fr

3.4.5 Évènements/Rapports

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

4. Gestion des sauvegardes et des archives

4.1. Sauvegarde par l'utilisateur du logiciel d'encaissement

Le logiciel permet de télécharger les données dans différents formats, ceux-ci peuvent être Format HTML, PDF, FEC, SAF-T, CSV, Excel, ou Archive fiscale.

L'administration fiscale pourra se baser sur le type de rapport "Archive fiscale" afin d'obtenir les données qui lui sont destinées.

Les autres formats d'archives/rapports permettront d'obtenir des informations complémentaires, orientés "comptabilité", lui permettant de mieux analyser le détail de ces archives, de croiser les informations, et d'obtenir une lecture plus rapide de ces informations.

Dans ce logiciel les archives sont désignées par le terme "Rapports" et ils peuvent être téléchargés en se rendant dans la page "rapport" du logiciel.

Indépendamment du format d'export choisi, le rapport présentera à minima les informations suivantes, adossées aux commandes : l'identifiant interne de la commande, sa date de création, sa date de validation, sa date de valeur, le nom de la caisse ayant effectué la vente, le dernier mode de paiement utilisé, la table du client, le client en question (son identifiant son nom et son prénom), les différents montants de TVA ventilés par taux de TVA, le nombre d'articles, le montant payé, le prix final, le prix d'achat, le détail de la commande, et sceau cryptographique de la commande, et le vendeur qui a procédé à l'enregistrement de la commande.

Le rapport de type "Archive fiscale" sera au format archive (fichier zip), et le fichier contiendra plusieurs fichiers :

- Le fichier de documentation destiné à l'administration fiscale
- Les fichiers d'export de données pour les tables : commandes, articles, paiements, fermeturesAuto, tracabilite
- Un fichier "Rapport.txt" qui contient le rapport de vérification des signatures, et affiche éventuellement la liste des signatures dont la vérification a échouée, afin que toute erreur de signature détectée soit bien mise en évidence.

Pour chaque fichier de donnée, sera indiqué la signature HMAC 256 recalculée, ainsi que la signature stockée en base, ainsi qu'une colonne affichant une alerte si les deux signatures ne sont pas égales, ce qui permet de disposer d'une vérification de la signature de chaque ligne de chaque table de donnée.

Concernant les rapports standards, il sera possible de télécharger uniquement les données qui sont associées à une caisse en particulier ou à toutes les caisses, un utilisateur en particulier ou à tous les utilisateurs.

Différentes plages de dates pour l'export de données seront disponibles : l'export quotidien, hebdomadaire, mensuel, annuel mais il sera également possible de télécharger des rapports portant sur une plage de date personnalisée.

Deux formats de rapport se distinguent des autres rapports parce qu'ils présentent un panel plus élargi de donner pour le rapport. Ces rapports sont les rapports au format PDF et HTML qui permettent d'afficher différentes tables de données au sein d'un même fichier. On retrouvera dans ses rapports : un tableau récapitulatif qui présente la date de création du rapport, le chiffre d'affaires global, le montant total des ventes et des remboursements, le montant total de la TVA collectée, le nombre d'opérations enregistrées, la valeur moyenne d'une opération. Sous forme de tableau distincts on retrouvera ensuite : la liste complète des commandes, le rapport par taux de TVA, le rapport par table de consommation, le rapport quotidien, le rapport des sorties de caisse, le rapport des fermetures de caisse, le graphique des ventes au cours du temps, le graphique du nombre de ventes au cours du temps, le rapport des fermetures de caisse, le rapport par caisse, par client, par utilisateur, par rayon, par groupe de rayon, par article, par méthode de paiement, par méthode de livraison, le rapport des réductions, le rapport sur les heures d'affluence, le rapport par chapitre comptable, le rapport des livraisons externes, le rapport sur les DLC.

Les rapports peuvent être également configurés pour être automatiquement envoyés quotidiennement ou mensuellement.

La fonctionnalité de rapport ou d'archivage permet d'exporter les données portant sur n'importe quelle plage de date.

Si la période couverte par une archive est supérieure à un an ou un exercice fiscal, il est clairement indiqué dans le nom du fichier (et dans le fichier en lui-même lorsque c'est possible) que celui-ci n'a pas de valeur légale.

Les archives téléchargées par l'utilisateur sont également enregistrées dans notre base de données et sont conservées pendant une durée qui dépend de la période sur laquelle porte l'archive. Si la période est une année la durée de conservation du rapport sera de 7 ans, si la période est d'un mois, la durée de conservation sera d'un an , pour une période d'une semaine, 30 jours de conservation, pour un rapport quotidien 10 secondes de conservation, pour un rapport sur une plage de date personnalisée 7 ans de conservation.

Du fait de l'utilisation d'un sceau cryptographique sur chaque commande, en temps réel, au moment de la validation de la commande, et que ce sceau (hash 256) prenne en compte le hash de la commande portant le numéro de facture précédent, et que ce même hash soit disponible à la consultation, et présent dans les exports utilisateurs, et également sauvegardé dans les dumps de la base de donnée effectués en interne, ce logiciel garantit de manière fiable et sécurisée que vos données respectent bien les exigence de fiabilité, traçabilité, vérifiabilité, sécurisation, intangibilité inhérente aux devoirs liés à la publication de ce logiciel.

4.1.1 Données enregistrées

Parmi les données qu'il est possible d'exporter figurent :

Table des commandes

- Le numéro de justificatif ("Numéro de commande") :
- L'identifiant du TPV : ("Numéro de caisse")
- Un identifiant unique de l'établissement d'utilisation du système d'encaissement : ("idBoutique")
- La date et l'heure de la transaction (année, mois, jour, heure, minute)
- Le montant total TTC du ticket
- Date validation, datevaleur, totalreduction, totaltva, nbarticles, choixlivraison, ID interne
- Toute donnée permettant la production de justificatifs (définitifs ou provisoires)
- Réimpressions des tickets
- Le mode de règlement (et les détails des montants réglés par mode de paiement si le règlement a lieu via plusieurs modes de paiement)

Table des articles

libellé, quantité, prix unitaire, total HT de la ligne (prix unitaire HT*quantite), taux de TVA associé, donnée élémentaire nécessaire au calcul HT de la ligne

Table des paiements

Champs : date, modePaiement (0 = espèces, 1 = chèques, 2 = CB), idModePaiement (correspond à un identifiant interne de mode de paiement permettant d'avoir plus d'informations sur celui-ci), montantPaye, caisseEncaissement, idBoutique, hash, isHashValid

Table des fermetures de caisse

Champs : dateCloture, totalPeriode, totalPerpetuel, niveauCloture, hash, isHashValid

Table des rapports téléchargés

Champs : date de création, HMAC SHA256 du fichier, titre de l'archive, type de l'archive, ID du TPV, ID utilisateur

• les données correctives sont enregistrées comme des commande normales à ceci près qu'elle disposent d'un champ "referenceCommande" qui indique que la commande fait référence à une autre commande

• il n'y a pas de données du mode école/test (car aucune donnée ne peut être enregistrée en mode test)

• les données cumulatives et récapitulatives via l'historique des fermetures de caisse et les rapports

• Les données de traçabilité d'impression/ré-impression via le champ "JustificatifImprimé"

• Les données de traçabilité des opérations de purge, archivage et restauration des données : Non applicable, aucune purge

4.1.2. Traçabilité des opérations

Chaque téléchargement de Rapport (Export de données) est enregistré dans une table d'historique des téléchargements de Rapports.

Cette table est également exportée parmi les données de caisse.

Les données enregistrées sont :

- date de création
- HMAC SHA256 du fichier
- titre de l'archive
- type de l'archive
- ID du TPV
- ID utilisateur

Ces données constituent l'intégralité des opérations d'archivage, de purge, et de restauration de données, puisque ce logiciel ne permet ni les restaurations de données, ni la purge de données.

4.2. Sauvegardes réalisées en interne par l'éditeur du logiciel

- Serveur de réplication de base de donnée en temps réel
- Sauvegardes automatiques des bases de données.
- Sauvegarde sur support externe tous les 3 mois

5. Conservation des données

5.1 Données utilisateur

Les données d'encaissement, de traçabilité, ainsi que les preuves de l' inaltérabilité, sont conservées de manière illimitée dans le temps en base de données. Les données cumulatives ainsi que les données de traçabilité sont également conservées dans le système sans limite de durée. Les données d'encaissement peuvent être conservées soit dans le système lui-même, soit dans le système lui-même ainsi que dans les archives téléchargées par l'utilisateur du système de caisse.

L'utilisateur reçoit par défaut des rapports par email, contenant une copie des rapports de fermeture de caisse. Il peut également programmer l'envoi automatisé par email des rapports.

Les rapports restent consultables à vie, 24h/24, 7j/7 et peuvent être interrogés sur n'importe quelle période ne dépassant pas la durée d'un an, à n'importe quelle date dans le passé en se rendant dans la page Rapport du logiciel.

Ces données sont accessibles à la fois pour le client, mais également à la demande de l'administration fiscale, lui permettant de télécharger les rapports portant sur n'importe quelle période, et de consulter l'historique des rapports émis.

Le client peut lui-même créer un accès pour l'administration fiscale, ou l'administration fiscale peut s'adresser à nous pour avoir un accès (contact@net-assembly.com).

Il est clairement indiqué dans l'aide qu'il est la responsabilité du client de télécharger et conserver ses rapports pendant une durée minimale de 6 ans

5.2. Modalités de génération des clés de chiffrement

Les clés cryptographiques utilisées pour le stockage sécurisé et la signature des données sont générées et gérées selon les principes suivants :

1. **Génération des clés**
    - Les clés sont générées de manière aléatoire à l'aide du générateur conforme aux standards cryptographiques reconnus OpenSSL (openssl rand -hex 32)
    - Les clés ne sont jamais dérivées d'informations prévisibles (nom d'utilisateur, date, etc.).
2. **Protection et stockage**
    - Les clés sont stockées dans un espace sécurisé du système (fichier de configuration protégé).
    - L'accès à ces clés est restreint au processus applicatif autorisé et protégé par des droits d'accès système.
    - Les clés ne sont jamais exposées en clair dans le code source ni dans les journaux d'exécution.
3. **Renouvellement et rotation**
    - En cas de compromission suspectée, de mise à jour de sécurité ou de changement de version majeure, de nouvelles clés sont générées.
    - Les anciennes clés restent conservées uniquement pour la vérification des signatures des données historiques, conformément aux obligations de traçabilité.
4. **Confidentialité et intégrité**
    - La génération et le stockage des clés respectent les bonnes pratiques de sécurité afin de garantir l'intégrité des données enregistrées et d'empêcher toute falsification ou suppression de transactions.

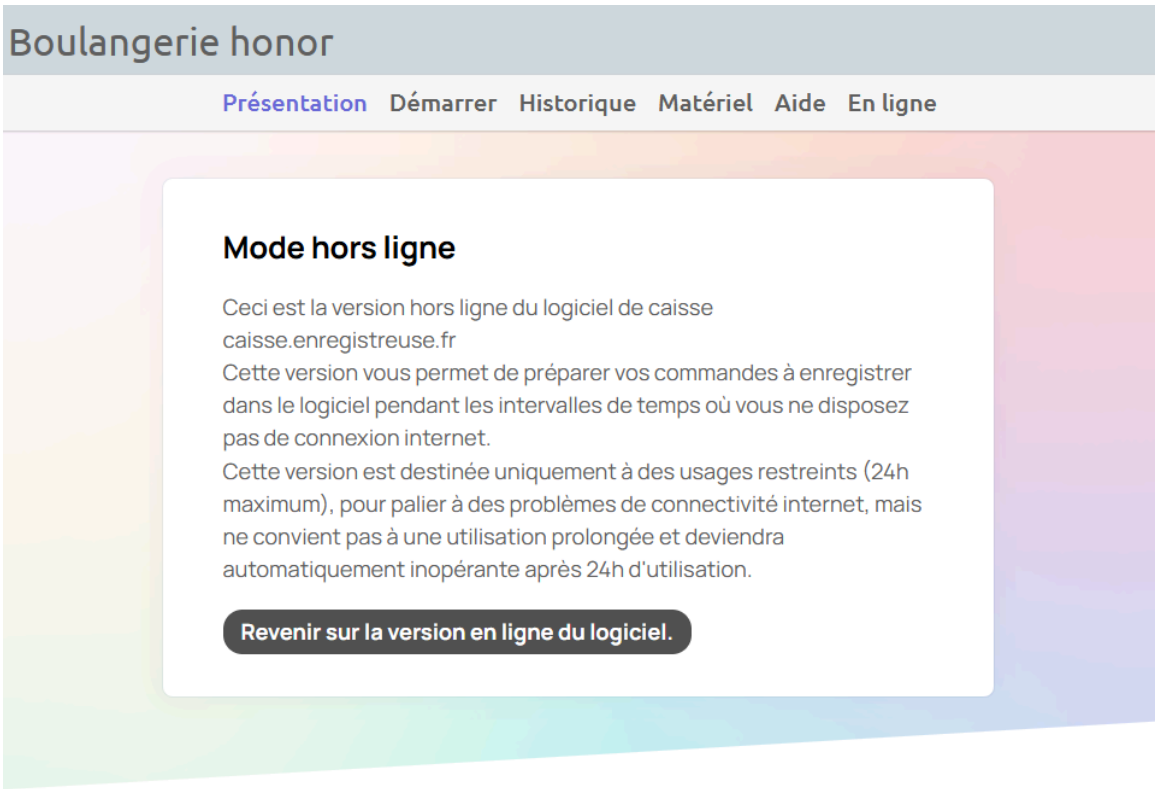
6. Mode hors ligne

Le mode hors ligne existe dans le logiciel mais celui-ci ne permet pas d'enregistrer des opérations de caisse mais seulement de préparer des brouillons de commandes qui ne pourront pas être validés (cf chapitre sur la validation des commandes) tant que l'accès à Internet ne sera pas rétabli.

Cela signifie qu'il n'est pas possible d'imprimer un reçu de caisse, de télécharger une facture, d'enregistrer une facture, d'obtenir un numéro de commande, etc.

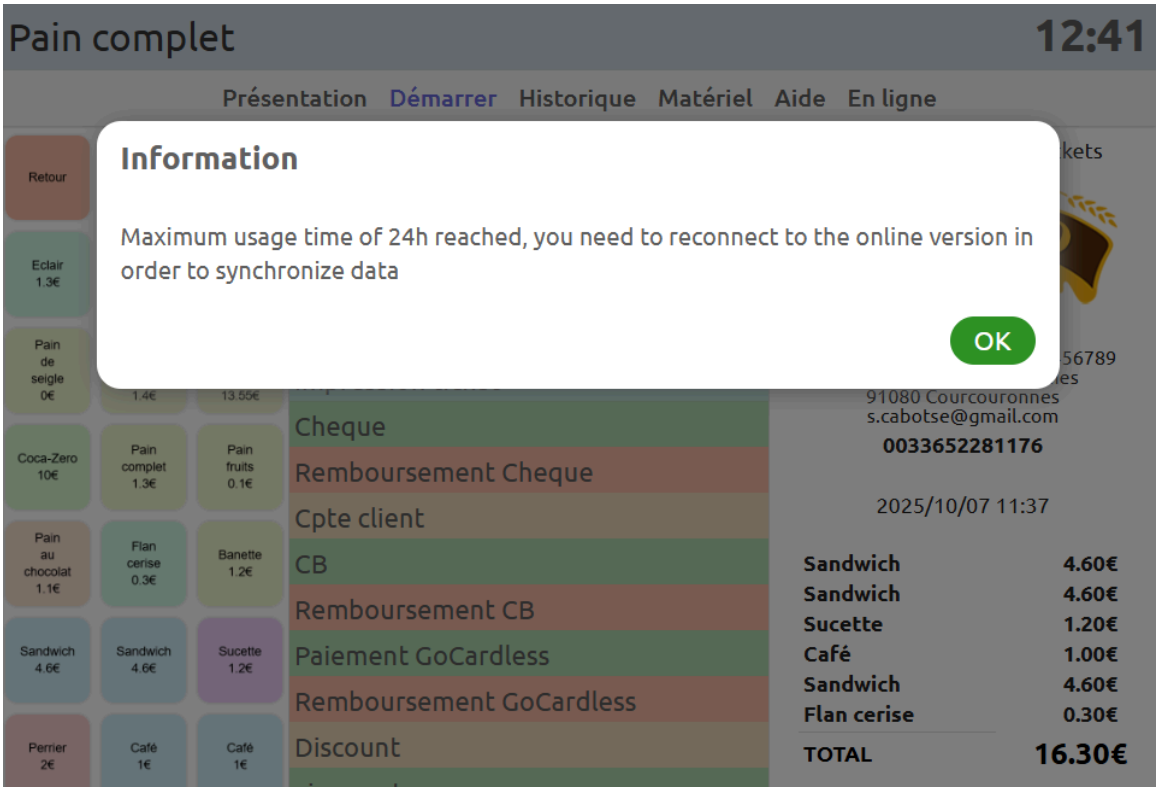
La durée maximale pour utiliser le système en mode hors ligne est de 24h, passé ce délai le mode hors ligne ne sera plus utilisable, et l'utilisateur sera invité à se connecter à internet pour enregistrer ses données préparées.

L'utilisateur du système de caisse est notifié que le système fonctionne en mode hors-ligne, via le biais d'un message sur la page d'accueil du mode hors ligne qu'il doit obligatoirement visualiser en accédant au mode Hors ligne.



Si l'utilisateur utilise la version Hors ligne pendant plus de 24h, l'ajout d'articles a une commande, ou la saisie d'un paiement pour une commande (donc toutes les fonctionnalités

d'enregistrement de données de ventes), sont désactivées, et retournent un message d'erreur.



7. Système centralisateur

La conservation des données étant assurée par un unique système, le système d'encaissement a prévu un mécanisme fiable de transfert des données pour assurer que l'exhaustivité du flux de données soit transférée y compris en cas de déconnexion en cours.

Lorsque l'utilisateur du système de caisse ajoute un article à une commande, celui-ci s'affiche temporairement sur la commande et une requête est envoyée au serveur afin d'enregistrer la modification. Lorsque la requête aboutit, le ticket de caisse est mis à jour afin de présenter la commande telle qu'elle est enregistrée dans le système centralisateur. L'opération de validation permettant de transformer le devis en facture ne pourra être réalisée que lorsque toutes les opérations de modification de la commande ont abouti et que l'utilisateur dispose à l'écran de la version enregistrée dans le système de centralisation de la commande.

Toutes les fonctions du logiciel utilisent les données enregistrées dans la base de donnée MySql. La génération d'une facture PDF, la génération d'un ticket de caisse, l'envoi d'une facture, la validation d'une commande.

Le client final exécute sur son poste un applicatif qui n'enregistre aucune donnée de vente en local.

Autrement dit, il n'y a pas de centralisation au sens prévu par le référentiel de certification, puisqu'une seule version des données existe.

Ni le mode hors ligne, ni le mode école ne permettent d'enregistrer des données de vente.

Le système est un système WYSIWYG (what you see is what you get) : si un ajout d'article à la commande n'abouti pas (le requête vers le serveur échoue), alors l'article n'est pas ajouté à la commande, et l'utilisateur ne le voit pas s'afficher sur la commande. Si la requête d'enregistrement d'un paiement n'arrive pas jusqu'au serveur, la commande n'est pas validée, ni enregistrée comme payée, et le ticket de caisse n'est pas mis à jour.

8. Accès de l'administration fiscale aux données

Le système d'encaissement prévoit un accès pour l'administration fiscale à l'ensemble des données d'encaissement enregistrées. Nous fournissons un moyen automatisé pour que l'administration fiscale puisse vérifier l'intégrité des données d'encaissement. Un manuel de l'utilisateur à destination de l'administration fiscale, en français, détaille la procédure permettant d'accéder aux données, ainsi qu'un descriptif clair du fonctionnement des outils utilisés pour accéder aux données et en vérifier l'intégrité.

L'administration fiscale à la possibilité de soit s'adresser à l'utilisateur du système de caisse ou de soit s'adresser directement à l'éditeur du logiciel de caisse, chacun de ces interlocuteurs sera en mesure de communiquer à l'administration fiscale un accès qui lui sera destiné. La procédure à réaliser pour accorder un tel accès à l'administration fiscale est très simple. Il suffit de se rendre en page Configuration, Utilisateurs, puis d'ajouter un nouveau compte utilisateur en saisissant son email, un mot de passe qui lui sera attribué et le rôle "Comptable". Le rôle comptable est un rôle commun à l'administration fiscale et au comptable de l'utilisateur du système d'encaissement.

Une fois connecté avec un tel compte l'administration fiscale aura accès au logiciel avec les onglets suivants :

Historique : cette page permet d'accéder à la liste complète des commandes du compte, il est possible d'effectuer une recherche par numéro de commande par date par identifiant client par nom de clients par caisse d'encaissement

Rapport : cette page permet d'accéder au rapport comptable et aux données consolidées intitulées dans ce document archives. Il sera possible dans cette page de procéder aux exports de données au format CSV, XLS, FEC, SAFT,, HTML, PDF

Vérification des sceaux cryptographiques

Cette page permet d'accéder à deux outils : le premier effectue une vérification de la chaîne de sceaux cryptographiques de l'intégralité des commandes de l'utilisateur du système d'encaissement et affiche le résultat, le deuxième outil permet de manuellement vérifier l'exactitude de la valeur du code de hachage enregistré dans la base de données courant l'authenticité l'intangibilité des données enregistrées.

Aide : cette page permet d'accéder à l'aide utilisateur du logiciel. Il est possible dans cette page de consulter la procédure permettant d'accéder aux données de caisse ainsi qu'un descriptif clair du fonctionnement des outils utilisés pour accéder aux données et en vérifier l'intégrité.

L'accès destiné à l'administration fiscale ne permettrait pas de modifier d'ajouter des données d'encaissement, cet accès sera limité à une consultation.

9. Gestion des incidents

- Surveillance 24/7 des serveurs via monitoring interne (munin, outils internes digital ocean, outils de notification en cas de crash)

10. Purges

Ce logiciel ne réalise pas de purge de données, les données sont conservées de manière illimitée dans le temps en base de données. Les données sont simplement déplacées d'une table à une autre pour alléger le système, mais restent disponibles à la consultation de la même manière.

11. Versions de l'application

Le système d'encaissement identifie clairement ces versions par un numéro de version majeur, un numéro de version mineur, et un numéro de révision. Ces numéros de version sont inextricablement liés au système d'encaissement. Ils sont aisément accessibles depuis l'interface utilisateur standard du système d'encaissement en vous rendant en page aide rubrique mention légale du logiciel. Toute modification de code dans le périmètre fiscal ou dans le paramétrage impactant le respect des exigences du référentiel entraîne une incrémentation du numéro de version majeure. une empreinte unique pour chaque version majeure et générer en fonction de la concaténation de la liste des fichiers qui constituent le périmètre fiscal. Cette empreinte est réalisée en effectuant un SHA 256 sur le résultat de la concaténation du contenu des fichiers qui constituent le périmètre fiscal et du numéro de version majeure. Cette empreinte peut être consultée en page aide du logiciel.

12. Périmètre fiscal

L'intégralité des fonction ayant un impact sur les fonctionnalités et exigences énoncées dans le référentiel de certification sont réunies dans un unique fichier :

Fichier "includes/coreCert.php"

Ce fichier contient entre autres: le numéro de version majeur et mineur, toutes les fonctions liées aux signatures : Fonction de création du sceau cryptographique ; Fonction de validation d'une commande ; Fonction de génération de la clé cryptographique associée à la boutique; Fonction de protection de la modification des commandes validées ; Les fonctions de signatures

Le périmètre fiscal contient ainsi les fichiers de documentation règlementaires, ainsi que le fichier coreCert.php

```
$certifiedFiles[] = "includes/coreCert.php";
$certifiedFiles[] = "documentation/coreCert.php";
$certifiedFiles[] = "documentation/dossier_d'architecture_technique.pdf";
$certifiedFiles[] = "documentation/dossier_de_conception_générale.pdf";
$certifiedFiles[] = "documentation/dossier_de_maintenance.pdf";
$certifiedFiles[] = "documentation/dossier_de_spécifications_fonctionnelles.pdf";
$certifiedFiles[] = "documentation/dossier_d'exploitation.pdf";
$certifiedFiles[] = "documentation/dossier_organisationnel.pdf";
$certifiedFiles[] = "documentation/Documentation complémentaire.pdf";
```

Conformité au Référentiel de Certification v1.7

Documentation technique (Exigence IV.1)
La structure du système et les processus sont documentés. L'organisation et les technologies sont précisément décrites.

Inaltérabilité et sécurisation des données (Exigence IV.4 - Exigences 8 et 9)
Le chaînage SHA256 assure l'inaltérabilité. Les transmissions et les données sont sécurisées via HTTPS/TLS et accès SSH restreint.

Archivage (Exigence IV.5 - Exigence 10)
Les données sont archivées périodiquement et sécurisées par compression et signature.

Conservation des archives (Exigence IV.8 - Exigences 16 et 17)
Les archives sont conservées sur des serveurs protégés pour une durée minimale de 6 ans.

Système centralisateur et mode hors-ligne (Exigence IV.8 - Exigence 18)
Le logiciel ne permet pas la réalisation de facture en mode déconnecté. Le mode déconnecté permet uniquement la préparation de devis / brouillons et ne permet pas l'enregistrement de commandes, ni l'émission de documents justificatifs. Il sera ensuite nécessaire de se reconnecter à Internet puis d'importer les brouillons dans le logiciel, afin de les transformer en commande, afin de pouvoir obtenir une facture, un ticket de caisse, ou un justificatif. Le mode déconnecté n'est prévu que pour subvenir à des courtes interruptions de service de l'ordre de quelques minutes.

Accès administration fiscale (Exigence IV.9 - Exigence 19)
Un module d'export CSV est disponible pour répondre aux demandes de l'administration fiscale.