

AMALFI



CU 2410

Vérification du scellement en batch

AMALFI V2

Historique du Document

Révision N°	Date de cette révision	Résumé des Modifications	Modifications indiquées	Version AMALFI
1.0		Version initiale	N	
2.0	10/06/2010	[TMAC-883] Réactiver dans PACS/PAVE la vérification du scellement greffe	N	57.0
3.0	11/03/2011	[TMAC-1393] Limiter la vérification du scellement greffe aux seules requêtes à l'état « A ordonnancer » [TMAC-334] Lors de la vérification, utilisation de liste blanche pour les erreurs déjà connues Corrections diverses : messages manquants Correction mineure : le code d'erreur E0323 existait déjà mais n'était pas documenté. On utilise donc E0325 pour le nouveau code	N	59.0
3.1	14/03/2011	Mise à niveau du CU par rapport à l'existant Ajout d'un complément d'information sur la protection de la liste blanche	N	59.0
4.0	09/02/2011	[TMAC-2142] Ajout du type de XMLDSig « WLSIGNER » pour les signatures de type JUGE [TMAC-2143] Nouveau batch de vérification sur la plateforme DVS (Dictao Validation Server)	N	61.1
5.0	26/10/2012	[TMAC-2365] Duplication des lanceurs du batch de vérification pour les modes de scellement S4 et AMALFI	N	62.0
6.0	12/05/2014	[TMAC-3415] SD-DSS : Intégration de DSS comme nouvelle signature pour AMALFI	N	65.5
6.1	23/05/2014	Prise en compte PVAT P-1060	N	65.5
7.0	07/07/2014	Prise en compte PVAT P-1061 [TMAC-3446] Intégration Signature SD-DSS Phase 2 Corrections complémentaires : - §1.3.1 : la vérification des signatures BlueZign n'est pas réalisée par l'API SD-DSS, mais par une implémentation intégrée à Amalfi - §1.3.2.1 : correction dans le nom d'un fichier de sortie en mode BLUEZIGN/S4	N	65.6
7.1	30/07/2014	Relivraison du CU pour levée de la réserve suivie (aucune nouvelle remarque n'a été émise)	N	65.6
8.0	16/07/2015	[TMAC-3557] Nettoyage du code S4 et bluezign et WLSigner [TMAC-3559] Nettoyage et rationalisation de tous les batchs AMALFI	<u>ON</u>	68.0
8.1	20/07/2015	Prise en compte PVAT-1464	<u>ON</u>	68.0
<u>9.0</u>	<u>20/05/2016</u>	[TMAC-2419] Mise en cohérence de la vérification d'intégrité d'AMALFI avec ce qui est fait dans le batch PavePacs	<u>O</u>	<u>71.0</u>
<u>9.1</u>	<u>03/06/2016</u>	Prise en compte PVAT-1838	<u>O</u>	<u>71.0</u>

Mis en forme : Surlignage

Mis en forme : Police :Non Gras, Surlignage

Mis en forme : Surlignage

Code de champ modifié

Code de champ modifié

Code de champ modifié

Table des matières

1.	Présentation	4
1.1	Objectif du document	4
1.2	Lexique.....	4
1.3	La synthèse des solutions retenues.....	4
1.3.1	Processus PavePacs.....	4
2.	Fonctionnement de la vérification PavePacs.....	6
2.1	Déroulement du traitement	6
2.2	Paramètres.....	6
2.3	Liste blanche.....	8
2.3.1	Format du fichier.....	89
2.3.2	Mise à jour de la liste blanche	9
2.4	Code de retour	949
2.5	Messages d'erreur	949
2.6	Messages d'avertissement	949
2.7	Traces	10

1. Présentation

1.1 Objectif du document

Ce document a pour objet de décrire la solution retenue pour contrôler la signature des objets sur l'ensemble de la base de données par des traitements de masse.

1.2 Lexique

Le terme « **signature** » utilisé dans ce document englobe les notions suivantes :

1. La génération par un processus à sens unique d'une empreinte numérique d'une partie des données (dans AMALFI V2 il s'agit toujours de l'empreinte des données relatives à une requête, cf. « CU 2905 Ordonnancer l'inscription » et TC31a.3.13) ;
2. La génération d'un document XMLDSig contenant cette empreinte, le chiffage de cette empreinte et les données nécessaires à leur validation (certificats, CRL, horodatage sécurisé de l'ensemble), ainsi que le document XMLDSig généré
3. Un document XMLDSig contenant cette empreinte, le chiffage de cette empreinte et une partie des données nécessaires à leur validation (certificat), généré par le composant de création de signature.

Le terme « **objet** » utilisé dans ce document englobe les notions suivantes :

- Requête ;
- Acte de gestion ;
- Objets du livre foncier.

Le terme « **scellement** » utilisé dans ce document correspond à la définition de l'EPELFI (i.e. une signature effectuée par un processus automatique et qui ne peut donc pas être attribuée à une personne physique).

1.3 La synthèse des solutions retenues

La solution retenue pour les contrôles du scellement en batch met en œuvre les traitements de vérification décrits dans le CU SECU_DET_APP.

1.3.1 Processus PavePacs

Le processus peut se décomposer en parties fonctionnelles :

1. **La vérification de la cohérence** des données consiste à vérifier que les données en base sont cohérentes. Cette vérification consiste essentiellement à vérifier que chaque objet du livre foncier est associé à une requête de manière à garantir que la vérification de toutes les requêtes à l'étape 2 vérifie effectivement tous les objets.
2. **La vérification du contenu des objets** consiste à vérifier que les empreintes des objets stockés en base correspondent bien aux empreintes contenues dans les signatures. Les requêtes sont vérifiées successivement. Une empreinte des données associées à la requête est prise pour chaque requête. Ce processus de prise d'empreinte est identique à celui appliqué lors de la signature d'une requête. Il est décrit dans les documents CU SECU_DET_APP et CU 2905. Pour les erreurs connues dues à des données non corrigibles, un mécanisme de liste blanche est mis en place : l'empreinte recalculée est comparée à celle stockée dans la liste blanche.

-
3. **La vérification des signatures** consiste à vérifier que les signatures stockées en base de données sont valides. Le fonctionnement de cette vérification est décrit dans le document SECU_DET_APP. Le système utilise deux implémentations de la vérification des signatures :
- Une implémentation pour la vérification des signatures JUGE SD-DSS,
 - une implémentation pour la vérification des signatures BLUEZIGN et des scellements HORO, GREF et SCEL.

Le traitement est interruptible (soit manuellement par envoi d'un signal au processus soit automatiquement au bout d'un temps configurable), c'est-à-dire capable de reprendre à partir d'une clé de reprise enregistrée par l'exécution précédente du traitement.

2. Fonctionnement de la vérification PavePacs

2.1 Déroulement du traitement

Le traitement se déroule de la manière suivante :

1. Lancement du traitement,
2. Détermination automatique du mode d'exécution :
 - Lancement sans clé de reprise
 - Lancement depuis une clé de reprise
3. Vérification de la cohérence des données,
4. Pour chaque requête, en fonction des paramètres d'exécution (Voir 2.2 Paramètres) :
 - a. Obtention des signatures de la requête et vérification de leur cohérence. Les cas possibles sont :
 - i. Requête migrée issue de la migration terminée lors de la migration et avec un scellement technique scellée.
 - ii. Requête issue de la migration migrée non terminée lors de la migration et non terminée au moment de la vérification dont l'horodatage est scellé.
 - iii. Requête issue de la migration migrée non terminée lors de la migration et terminée au moment de la vérification dont l'horodatage est scellé ; signée par un juge.
 - iv. Requête technique scellée.
 - v. Requête en cours et dont l'état n'est pas « SAISIE » dont l'horodatage est scellé.
 - vi. Requête en cours dont l'état est « SAISIE » dont l'horodatage est scellé ; scellée avec un scellement greffier.
 - vii. Requête terminée dont l'horodatage est scellé ; signée par le juge.
 - viii. Requête terminée non inscrite signée dont l'horodatage est scellé ; avec scellement greffier (requête terminée par jonction).
 - b. Pour chaque signature :
 - i. Vérification des données ;
 1. si le hash recalculé est différent du hash stocké, si l'exécution utilise la liste blanche :
 - a. si le hash recalculé est identique au hash présent dans la liste blanche, l'erreur est loguée dans le fichier warn-verif.txt
 - b. si le hash recalculé est différent du hash présent dans la liste blanche, l'erreur est loguée dans le fichier erreurs-verif.txt
 - ii. Vérification de la signature ;
 5. En fin de traitement (arrêt manuel ou programmé) horodatage du journal :
 - a. Une empreinte SHA-256 du fichier journal est calculée (journal-verif.txt)
 - b. Un scellement d'horodatage de cette empreinte est demandé à la TSA.
 - c. Le scellement d'horodatage est stocké au format ASN.1 dans un fichier nommé journal-verif.tst

Mis en forme : Surlignage

Mis en forme : Surlignage

Mis en forme : Surlignage

Mis en forme : Surlignage

Mis en forme : Surlignage

Mis en forme : Surlignage

2.2 Paramètres

Les paramètres suivants permettent de modifier le comportement du traitement.

Fichier verif.properties

Paramètre	Description
verifContenu	booléen qui indique si la vérification du contenu est effectuée
verifSignature	booléen qui indique si la vérification des signatures est effectuée
verifScellementGreffé	booléen qui indique si la vérification des scellements greffier est à effectuer
utilisationlisteBlanche	valant O ou N, indiquant si la liste blanche doit être utilisée
repertoireXml	Nom du répertoire contenant les fichiers XML générés
maxExecutionTime	Temps maxi d'exécution en minutes
nbThreads	le nombre de vérifications exécutées en parallèle (permet d'optimiser l'utilisation des ressources d'entrée/sortie et des processeurs).
nbRequetesThreads	nombre de requêtes traitées en une fois. Le processus lit ce nombre de requêtes en base avant de passer le lot à un thread de traitement (permet d'optimiser l'utilisation des ressources mémoire et des entrées/sorties d'accès à la base de données).
base-Url	Url de la base de données Exemple : jdbc:db2://db295:50003/DBQUAL11
base-User	Utilisateur de connexion à la base de données Exemple : amalfi
base-Password	Mot de passe associé
base-Schema	Schéma de la base de données Exemple : DBAMALFI
tsaUri	Uri de la tsa Exemple : https://srvs2:4436/tsa/AMALFI
uriRefdata	URL du refdata Exemple : https://10.1.2.6:643/refdata.xml
urlKeystoreServeurSecurite	URL absolue du fichier PKCS#12 contenant le certificat et la clé privée pour l'authentification au serveur web de sécurité Exemple : trousseaux/i09_10.1.1.41.p12
mdpKeystoreServeurSecurite	mot de passe correspondant
urlTruststoreServeurSecurite	URL absolue du truststore pour l'authentification au serveur web de sécurité
mdpTruststoreServeurSecurite	mot de passe correspondant
typeTruststoreServeurSecurite	type de truststore : JKS
tsaUrlKeystore	URL absolue du fichier PKCS#12 contenant le certificat et la clé privée pour l'authentification à la tsa Exemple : trousseaux/i09_10.1.1.41.p12
tsaMdpKeystore	mot de passe correspondant
tsaUrlTruststore	URL absolue du truststore pour l'authentification au à la tsa
tsaMdpTruststore	mot de passe correspondant
tsaTypeTruststore	type de truststore : JKS

2.3 Liste blanche

L'utilisation de la liste blanche est facultative, suivant la valeur du paramètre « utilisationlisteBlanche ».
La liste blanche est un fichier XML situé dans le répertoire config, et nommé config-verif-whitelist.xml.
Si l'utilisation de la liste blanche est demandée, et si ce fichier n'existe pas, est illisible ou n'est pas valide une erreur apparaît et le traitement est interrompu.
Si le fichier est un fichier XML valide mais vide, le traitement continue.

Protection de la liste blanche contre les altérations : le fichier config-verif-whitelist.xml sera protégé par application du mécanisme de signature applicative sur ce batch.

2.3.1 Format du fichier

Le fichier est au format XML en caractères ISO-8859-1 (LATIN-1)

2.3.1.1 Exemple

Le fichier aura le format suivant (pour des raisons de mise en forme automatique de Word, les doubles quotes sont remplacées par des simples):

```
<? xml version='1.0' encoding='iso-8859-1' ?>
<pavePacs>
  <listeBlanche>
    <contenu>
      <requete oid='RQ100123456'>
        <documentRequete type='JUGE' hash='hashRecalculéEncodéEnBase64' />
      </requete>
      <requete oid='RQ100654321'>
        <documentRequete type='HORO' hash='hashRecalculéEncodéEnBase64' />
      </requete>
    </contenu>
  </listeBlanche>
</pavePacs>
```

2.3.1.2 Description du format

Élément pavepacs

L'élément racine pavepacs est obligatoire

Éléments listeBlanche et contenu

Les éléments listeBlanche et contenu sont obligatoires si au moins 1 élément requête est présent

Élément requete

L'attribut oid est obligatoire

Cet élément peut contenir 1 ou 2 élément(s) documentRequete parmi les combinaisons suivante :

- Type HORO
- Type SCEL
- Types HORO + GREF
- Types HORO + JUGE

Élément documentRequete

L'attribut type est obligatoire et peut prendre 1 des 4 valeurs SCEL , HORO, GREF, JUGE

L'attribut hash est obligatoire. Il correspond au hash du document XMLRequete recalculé

2.3.2 Mise à jour de la liste blanche

Si une nouvelle erreur de vérification apparaît, après analyse et vérification que les données ne peuvent être modifiées, la liste blanche pourra être complétée avec les informations relevées dans le fichier journal (journal-verif.txt) ou dans le fichier des erreurs (erreurs-verif.txt)

```
<requete oid='RQ1001036545'>
  <documentRequete type='JUGE' hash='s9LLkignS9iqhTgM8JUSjaPF3hMu+ewQDjX1M3rdTCs=' />
</requete>
```

2.4 Code de retour

Lorsque le traitement s'arrête, il retourne les valeurs et messages suivants :

Valeur	Libellé
0	Le traitement s'est déroulé sans erreur et s'est arrêté faute de données à vérifier.
1	Le traitement s'est déroulé sans erreur.
-1	Le traitement s'est déroulé avec des erreurs.
-2	Le traitement s'est interrompu suite à une erreur.

2.5 Messages d'erreur

Le tableau, ci-dessous, liste les messages d'erreur et leurs codes. La colonne « Interr. » indique si cette erreur interrompt le traitement.

Code	Libellé	Interr.
E0301	Erreur d'accès à la base de données.	Oui
E0302	L'objet de n° Amalfi <numéro> ne fait pas partie d'une requête.	Non
E0310	La requête technique <oid> n'est pas scellée.	Non
E0311	L'horodatage de la requête <oid> n'est pas scellé.	Non
E0312	La requête saisie <oid> n'est pas scellée par le greffier.	Non
E0313	La requête inscrite <oid> n'est pas signée par le juge.	Non
E0320	Le hash calculé <hash> de la requête <oid> diffère de celui stocké dans la signature de type <type de signature>.	Non
E0321	La vérification de la signature de type <type de signature>/<type de XMLDSIG> de la requête <oid> a échoué.	Non
E0322	La signature de la requête <oid> n'a pas pu être lue.	Non
E0323	Le contenu XMLDSIG de la signature de type <type de signature>/<type de XMLDSIG> de la requête <oid> est nul.	Non
E0324	Le fichier config-verif-whitelist.xml n'existe pas, est illisible ou n'est pas valide. (seulement si le paramètre utilisationlisteBlanche vaut « O »)	Oui
E0325	Le hash calculé <hash> de la requête <oid> pour la signature diffère de celui stocké dans la signature de type <type de signature>/<type de XMLDSIG> et de celui stocké dans la liste blanche	Non

2.6 Messages d'avertissement

Le tableau, ci-dessous, liste des messages d'avertissement et de leurs codes.

Code	Libellé
A0320	Le hash calculé <hash> de la requête <oid> diffère de celui stocké dans la signature de type <type de signature>/<type de XMLDSIG>, mais est identique à celui stocké dans la liste blanche

2.7 Traces

Le tableau, ci-dessous, liste les messages de traces envoyés par le traitement.

Code	Libellé	Occurrence
I0301	Début de la vérification de <nb> signatures.	Au lancement
I0302	<nb> signatures vérifiées en <temps d'exécution> ms. Total signatures traitées : <nb traitées>/<nb total>. Dernière requête : <oid de la requête>.	A l'arrêt
I0303	Fin de la vérification.	A l'arrêt
I0306	Toutes les tâches n'ont pas été traitées pendant le temps d'exécution de <nb de minutes> minutes alloué. Environ <nb de tâches> sur <nb total de tâches> ont été accomplies.	A l'arrêt
I0307	Pas de requête vérifiée.	Au lancement
I0308	Données de référence : <fichier XML des données de référence>	Au lancement
I0309	La vérification que chaque objet appartient à une requête n'a pas été faite. Elle n'a lieu que si la vérification du contenu est demandée et qu'aucun oid de requête n'a été fourni au batch (roid dans config-verif.properties).	Au lancement
I0310	Paramètres de fonctionnement de la vérification	Au lancement
I0311	Bureau foncier: <codeBureauFoncier>	Au lancement
I0312	Vérification du contenu : <verifContenu>	Au lancement
I0313	Vérification de la signature : <verifSignature>	Au lancement
I0314	Maximum de tâches: <nbThread>, traitant <nbRequetesThreads> requête(s) à la fois	Au lancement
I0315	Durée maximale de la vérification: <maxExecutionTime> minutes	Au lancement
I0316	Vérification du Bureau foncier : <codeBF>	Au commencement de la vérification pour chaque bureau foncier
I0317	Vérification du scellement greffe : <verifScellementGreffe>	Au lancement
I0318	Utilisation de liste blanche : <utilisationlisteBlanche>	Au lancement

Le message I0003 signifie la fin globale du traitement. Le message I0002 signifie l'arrêt du traitement alors qu'il reste encore des vérifications à faire.

-- FIN DE DOCUMENT --