DIRECTION DU CENTRE SPATIAL DE TOULOUSE

SGC

SOUS-DIRECTION ASSURANCE QUALITE
SERVICE GESTION PRODUIT
DCT/AQ/GP

AQGP-MU-3-2512-CNES
proj-typ---CN
Edition : 01 Date : 24/01/2014
Révision : 01 Date : 26/05/2015
Réf. : intentionnellement vide
Code diffusion : E

MANUEL UTILISATEUR DU LOGICIEL C'KOUASUM VERSION 2.8.9

Rédigé par : LEDOT Aurélien DCT/AQ /GP	le : 11/06/2015	
Validé par : ETIENNE Jean-Paul DCT/AQ /GP	le : 11/06/2015	**Validé le 11/06/2015**
Pour application :	le :	

BORDEREAU D'INDEXATION

Confidentialite : P	MOTS CLES : Clefs d'intégrité, checksums

TITRE DU DOCUMENT :

MANUEL UTILISATEUR DU LOGICIEL C'KOUASUM
VERSION 2.8.9

Auteur(s) :
LEDOT Aurélien DCT/AQ /GP

RESUME : Ce document donne les informations nécessaires à un utilisateur pour l'utilisation du logiciel de calcul et de comparaison de clefs d'intégrité C'KOUASUM.

DOCUMENTS RATTACHES : Ce document vit seul.	Localisation :

Volume : 1	NBRE TOTAL DE PAGES : 22 DONT PAGES LIMINAIRES : 5 NBRE DE PAGES SUPPL. : 0	DOCUMENT COMPOSITE : N	Langue : FR

GESTION DE CONF. : NG	RESP. GEST. CONF. :

CAUSE D'EVOLUTION : Prise en compte des FT suivant:
DM 3262: Identifier les clefs trouvées avec un nom de fichier erroné (§3.4.2)
DM 3292: Tracer dans l'analyse les fichiers ayant le même nom (§4.1.4)

CONTRAT : Néant

SYSTEME HOTE :
Microsoft Word 14.0 (14.0.7149)
D:\Utilisateurs\Public\Dot\normal.dotm
Version GDOC : v4.3.1.1
Base projet : \\to05res04\GdocBasesPartagees\Structures\CNES\CST\DCT\AQ\GP\SGC.mdb

DIFFUSION INTERNE

Nom	Sigle	Bpi	Observations
LEDOT Aurélien	DCT/AQ/GP	2513	
CONQUET Nathalie	DCT/AQ /GP	2513	
ETCHEVERRY Christophe	DCT/AQ /GP	2513	
ETIENNE Jean-Paul	DCT/AQ /GP	2513	
THERON Patrick	DCT /AQ /GP		
LAVAL Nadine	DCT/AQ /GP	2513	

DIFFUSION EXTERNE

Nom	Sigle	Observations

Sans Objet

MODIFICATION

Ed.	Rév.	Date	Référence, Auteur(s), Causes d'évolution
01	01	26/05/2015	intentionnellement vide LEDOT Aurélien DCT/AQ/GP Prise en compte des FT suivant: DM 3262: Identifier les clefs trouvées avec un nom de fichier erroné (§3.4.2) DM 3292: Tracer dans l'analyse les fichiers ayant le même nom (§4.1.4)
01	00	24/01/2014	intentionnellement vide LEDOT Aurélien DCT/AQ/GP Création du document pour la mise en ligne de la version 2.8.6 de l'outil.

SOMMAIRE

1. GLOSSAIRE ET LISTE DES PARAMETRES AC & AD 1

2. GENERALITES 2

2.1. OBJECTIF 2

2.2. FONCTION DE L'OUTIL 2

2.3. UTILISATION DES CLEFS D'INTEGRITE 2

3. UTILISATION 4

3.1. EXECUTER LE LOGICIEL 4

3.2. PRESENTATION DE L'IHM 4

3.3. CALCUL DES CLEFS D'INTEGRITE 5

3.3.1. Choix de l'algorithme 6

3.3.2. Imports des fichiers à calculer 6

3.3.3. Lancer le calcul 7

3.3.4. Résultats du calcul 7

3.4. COMPARER DES CLEFS D'INTEGRITE 7

3.4.1. Importer les clefs à comparer 7

3.4.1.1. Format des clefs à comparer 7

3.4.1.2. Import des clefs 8

3.4.2. Lancer la comparaison 9

3.5. RAPPORTS 9

4. PRINCIPES ET LIMITATIONS DE L'OUTIL 11

4.1.1. Import des fichiers à calculer 11

4.1.2. Calcul des checksums et algorithmes utilisés 11

4.1.3. Import des fichiers à comparer 11

4.1.4. Principe de la comparaison 12

4.1.5. Problèmes chemin Windows / linux 13

5. ENVIRONNEMENT NECESSAIRE POUR UTILISER L'OUTIL 15

5.1. CONFIGURATION REQUISE 15

5.2. INSTALLATION DE C'KOUASUM 15

5.3. VERIFICATION DES PROVIDERS DISPONIBLES PERMETTANT DE CALCULER LES CLEFS D'INTEGRITE 15

5.3.1. Provider utilisé lors du développement de C'KOUASUM 15

5.3.2. Providers par défaut 16

5.3.3. Sécurisation de la liste des providers par l'administrateur machine 16

1. GLOSSAIRE ET LISTE DES PARAMETRES AC & AD

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
IHM	Interface Homme Machine

Liste des paramètres AC :

Liste des paramètres AD :

2. GENERALITES

2.1. OBJECTIF

Ce document décrit les éléments à connaitre pour prendre en main l'outil C'KOUASUM.

2.2. FONCTION DE L'OUTIL

Le logiciel C'KOUASUM permet le calcul et la comparaison de clefs d'intégrité sur des fichiers ainsi que la réalisation des rapports contenant les clefs calculées et le résultat des comparaisons.

L'outil permet :

- le calcul de clefs d'intégrité à partir d'une liste de fichiers ou d'une arborescence (voir §3.3 - Calcul des clefs d'intégrité);
- la comparaison de clefs d'intégrité importées à partir d'un ou plusieurs fichiers (voir §3.4 - Comparer des clefs d'intégrité) ;
- la création du rapport contenant les clefs calculées et le résultat des comparaisons (voir §3.5 - Rapports).

Le procéssus d'utilisation des clefs d'intégrité sont définis dans le §2.3 - Utilisation des clefs d'intégrité

La procédure pour démarrer l'outil est précisée dans le §3 - Utilisation

Les principes et limitations de l'outil sont décrits dans le § 4 - Principes et limitations de l'outil.

En cas de dysfonctionnement ou de difficultés d'installation, l'environnement et la configuration requise pour utiliser l'outil sont décrits dans le §5 - Environnement nécessaire pour utiliser l'outil

> *Note : Cet outil n'a pas pour vocation d'optimiser les performances, ou le traitement quotidien à la chaine de clefs d'intégrité. Des outils en lignes de commandes sont plus adaptés pour des traitements réguliers. L'objectif de cet outil est de rester portable, flexible, compatible avec les principaux algorithmes et utilisable sans connaissances spécifiques en informatique.*

2.3. UTILISATION DES CLEFS D'INTEGRITE

Une clef d'intégrité permet de vérifier si des données ont évolué et donc de détecter lors d'un contrôle une modification ou corruption par une tierce personne ou une altération du fichier (suite à une transmission ou par altération involontaire de type disque endommagé). Une clef d'intégrité peut être calculée et vérifiée avec divers algorithmes, les plus communs sont MD5, SHA-1 et SHA-256.

> *A noter que l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) recommande de ne plus utiliser MD5 et SHA-1 pour calculer les clefs d'intégrité, jugés insuffisants d'un point de vue cryptographique, mais de préférer SHA-256 lorsque les systèmes le permettent.*

Le but de l'outil C'KOUASUM est de simplifier le calcul et la comparaison de clefs d'intégrité :

On souhaite envoyer un fichier (ou ensemble de fichiers) à une personne et garantir cet envoi :

On calcule pour ce fichier une clef d'intégrité avec l'algorithme SHA-256. Cette clef est unique, si le fichier est modifié et que l'on recalcule la clef, elle sera différente.
On transmet le fichier au correspondant. En parallèle, on lui transmet la clef si possible par un moyen différent et/ou un envoi distinct. Cet envoi séparé limite le risque qu'une personne mal intentionnée intercepte le fichier et la clef, modifie le fichier et recalcule la clef ce qui ne permettrait pas de détecter la corruption du fichier.

Vérification de l'intégrité du fichier (ou de l'ensemble des fichiers) reçu(s)

Calculer la clef d'intégrité du ou des fichier (s) avec le même algorithme que celui de la clef reçue

Comparer ces deux clefs : elles doivent être identiques. Dans le cas d'une différence sur les clefs calculées, le ou les fichier(s) a (ont) été(s) altéré(s)/modifié(s) entre l'émission et la réception.

3. UTILISATION

3.1. EXECUTER LE LOGICIEL

Deux solutions :

- en double cliquant sur le fichier jar ;
- via lignes de commandes.

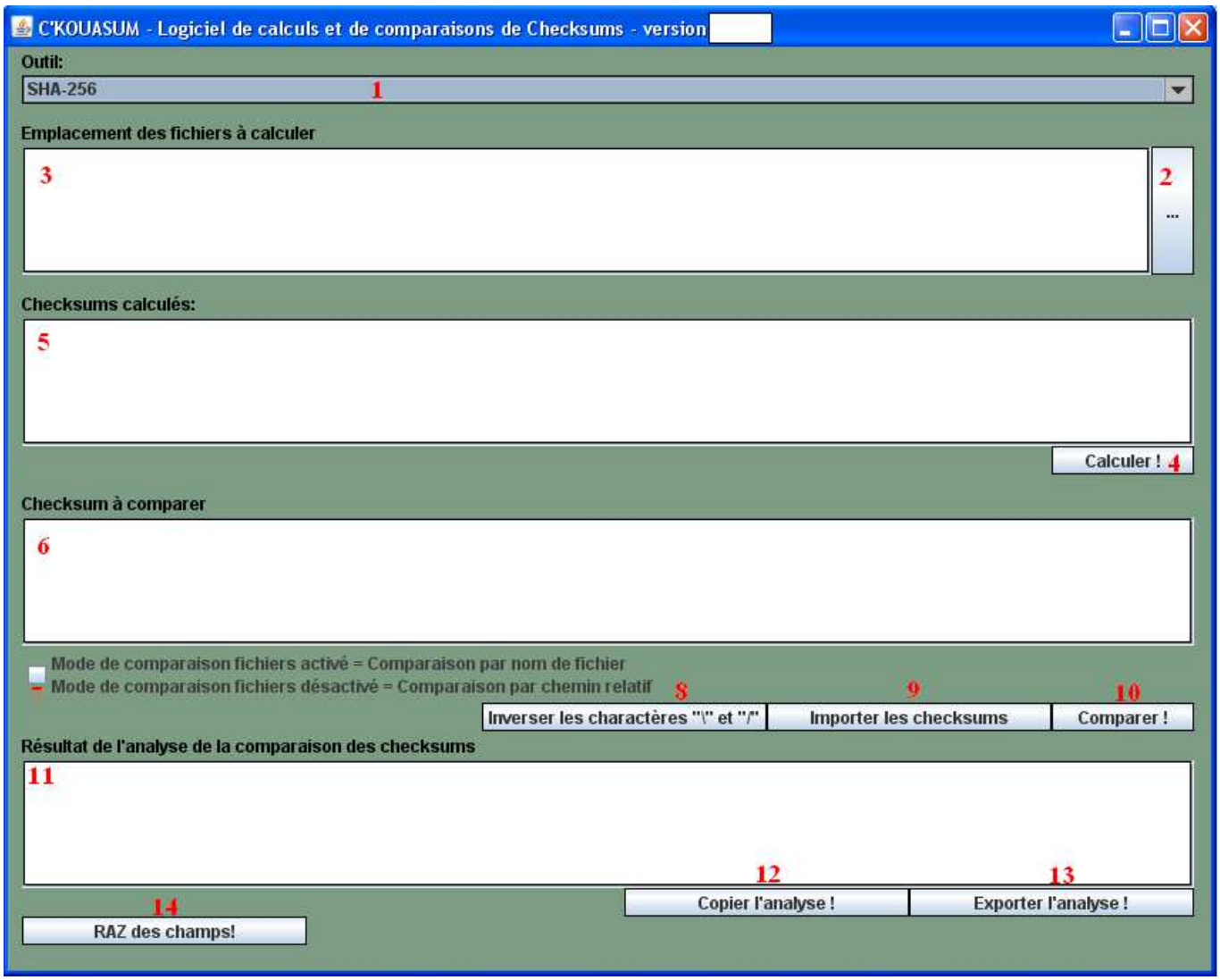
En ligne de commande

Sur Windows et linux:

Java -jar <Emplacement du fichier jar>

3.2. PRESENTATION DE L'IHM

L'interface graphique de l'outil est la suivante :



- IHM-1 :Liste des algorithmes gérés par l'outil
- IHM-2 :Bouton permettant d'importer les fichiers à calculer
- IHM-3 :Zone de texte qui affiche les fichiers dont l'outil va calculer les clefs d'intégrité
- IHM-4 :Bouton permettant de lancer les calculs des clefs d'intégrité
- IHM-5 :Zone de texte contenant les résultats des clefs calculées
- IHM-6 :Zone de texte affichant les clefs que l'on souhaite comparer aux clefs précédemment calculées
- IHM-7 :Choix du mode de comparaison des clefs
- IHM-8 :Bouton permettant de remplacer les caractères '/' par '\' et '\' par '/' dans la zone de texte IHM-6
- IHM-9 :Bouton permettant d'importer des clefs à comparer dans la zone de texte IHM-6
- IHM-10 :Bouton permettant de lancer la comparaison des clefs importées et calculées
- IHM-11 :Zone de texte contenant le résultat de la comparaison des clefs
- IHM-12 :Bouton permettant de copier le rapport dans le presse papier
- IHM-13 :Bouton permettant de sauvegarder le rapport dans un fichier texte
- IHM-14: Bouton permettant l'effacement de tout les champs

3.3. CALCUL DES CLEFS D'INTEGRITE

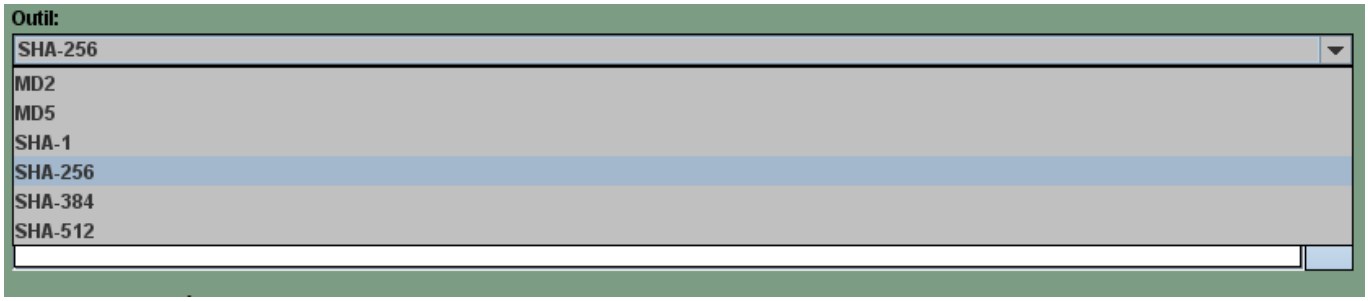
Ce chapitre donne la marche à suivre pour calculer une clef d'intégrité sur un fichier informatique.

3.3.1. Choix de l'algorithme

Avant d'effectuer un calcul, l'utilisateur peut sélectionner un des algorithmes suivants :

- MD2
- MD5
- SHA-1
- SHA-256 (à utiliser pour les envois de fichiers)
- SHA-384
- SHA-512

Pour sélectionner un de ces algorithmes, l'utilisateur doit cliquer sur la liste de choix déroulante présentée ci-dessous (« IHM-1 »):



Bonne pratique :

1 – Pour les échanges, l'algorithme SHA-256 est recommandé. **Dans tous les cas, il faut indiquer à votre correspondant l'algorithme utilisé.**

2 – Pour comparer des clefs d'intégrité, il faut **prendre le même algorithme que celui utilisé pour les clefs reçues**, l'expéditeur doit donc le préciser.

3.3.2. Imports des fichiers à calculer

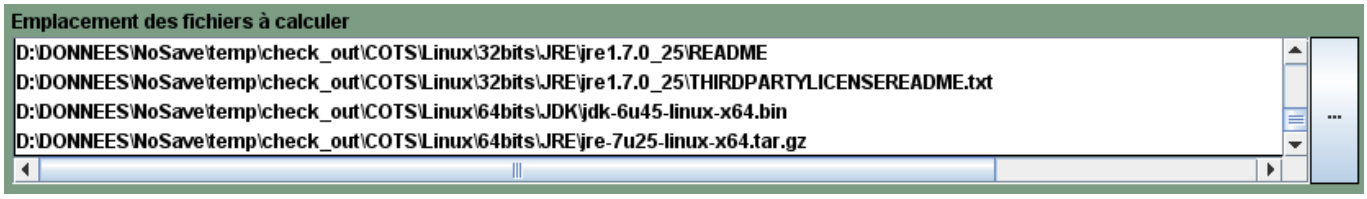
Ce chapitre précise comment sélectionner les fichiers dont on souhaite calculer le checksum.

Il y a deux manières d'importer les fichiers.

- en les sélectionnant à partir du bouton « IHM-2 - Bouton permettant d'importer les fichiers à calculer» une liste de fichiers et dossiers ;
- en réalisant un glissé/déposé des fichiers et dossiers dont on souhaite calculer les checksums dans la zone de texte « IHM-3 - Zone de texte qui affiche les fichiers dont l'outil va calculer les clefs d'intégrité» (dépend de la plateforme, non disponible sur toutes les versions Linux).

Note : si un dossier est sélectionné, tous les fichiers de ce dossier et de ses sous dossiers seront importés.

Une fois l'import réalisé, les fichiers seront présents dans la zone de texte « IHM-3 - Zone de texte qui affiche les fichiers dont l'outil va calculer les clefs d'intégrité» (exemple ci-dessous).



Astuce : Il est possible à tout moment d'interrompre l'import en cliquant sur la croix du message d'attente, l'interruption est prise en compte à la fin de l'import du fichier ou dossier en cours, cela peut donc prendre un peu de temps lors de la sélection d'un dossier contenant beaucoup d'éléments.

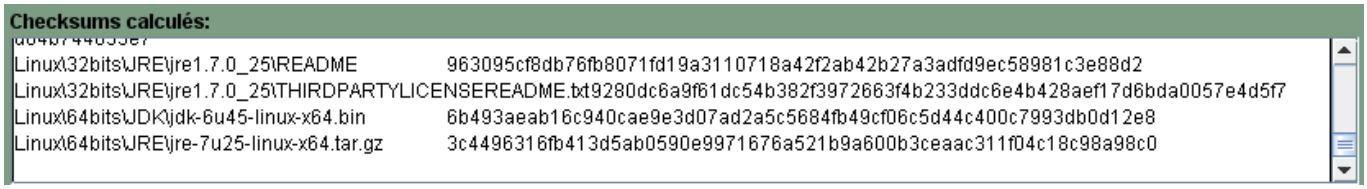
3.3.3. Lancer le calcul

Une fois que les fichiers sur lesquels on souhaite calculer un checksum sont sélectionnés, le calcul est lancé en cliquant sur le bouton « IHM-4 - Bouton permettant de lancer les calculs des clefs d'intégrité».

Astuce : Il est possible à tout moment d'interrompre le calcul en cliquant sur la croix du message d'attente, l'interruption est prise en compte à la fin du calcul du fichier en cours.

3.3.4. Résultats du calcul

Le compte rendu des calculs est disponible dans la boite de la zone de texte « IHM-5 - Zone de texte contenant les résultats des clefs calculées».



3.4. COMPARER DES CLEFS D'INTEGRITE

Ce chapitre donne la marche à suivre pour vérifier que les fichiers reçus n'ont pas été altéré/modifiés.

Le principe consiste à calculer la clef d'intégrité du paquet réceptionné et de comparer cette clef à celle fournie et correspondant à la livraison. Si les deux clefs sont identiques, alors la livraison est correcte, dans l'autre cas la livraison a été altérée ou modifiée.

3.4.1. Importer les clefs à comparer

3.4.1.1. Format des clefs à comparer

Les clefs peuvent avoir trois formats distincts pour être analysées par le logiciel C' KOUASUM

1 - <Nom fichier> <Clef d'intégrité>

2 - <Chemin complet du fichier>/<nom fichier> <Clef d'intégrité>

3 - <Chemin relatif du fichier>/<Nom fichier> <Clef d'intégrité>

Note : Il est obligatoire d'avoir sur la même ligne l'arborescence du fichier ou son nom ou son chemin relatif dans la livraison et la valeur du checksum associé. Les tabulations/espaces ou l'ordre n'ont pas d'importance.

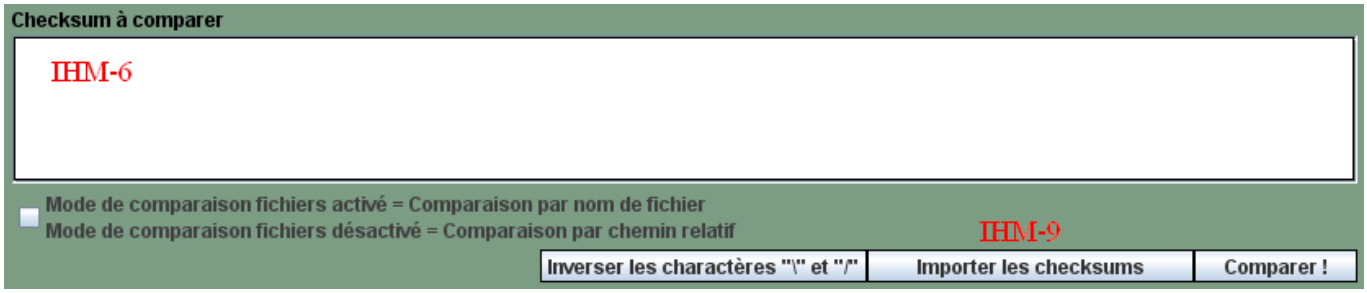
Pour le format « 1 », il faut que «IHM-7 - Choix du mode de comparaison des clefs » soit activé.

Pour le format « 2 » et « 3 », il faut que «IHM-7 - Choix du mode de comparaison des clefs » soit désactivé.

Pour plus d'informations, voir §4.1.4 - Principe de la comparaison.

3.4.1.2. Import des clefs

Ce chapitre précise comment importer les clefs à comparer dans (« IHM-6 - Zone de texte affichant les clefs que l'on souhaite comparer aux clefs précédemment calculées»).



Il y a trois manières d'importer les fichiers à comparer :

- en collant les données dans la zone de texte « IHM-6 - Zone de texte affichant les clefs que l'on souhaite comparer aux clefs précédemment calculées » ;
- en sélectionnant une liste de fichiers à partir du bouton « IHM-9 - Bouton permettant d'importer des clefs à comparer dans la zone de texte IHM-6» ;
- en réalisant un glissé/déposé des fichiers dont on souhaite importer le contenu (dépend de la plateforme, non disponible Linux) dans le zone de texte «IHM-6 - Zone de texte affichant les clefs que l'on souhaite comparer aux clefs précédemment calculées».

*Note pour les utilisateurs avancés dans la **méthode d'import des listes de clés** :*
1 - Pour les fichiers compilés type Word, Excel, etc… Il n'est pas possible d'importer directement ces fichiers avec les clés car ils ne sont pas lisibles par l'outil. Il faut alors ouvrir le fichier sélectionner la liste des clés et utiliser le copié/collé.
2 - Pour l'import à partir de fichiers de clés, seuls les fichiers ASCII (pas les programmes) seront importés.
3 - Dans le cas de la sélection de plusieurs fichiers lors d'un import, ces fichiers seront concaténés.

La liste des clefs à comparer est disponible dans la zone de texte «IHM-6» après l'import.

Astuce : Il est possible à tout moment d'interrompre l'import en cliquant sur la croix du message d'attente, l'interruption est prise en compte immédiatement.

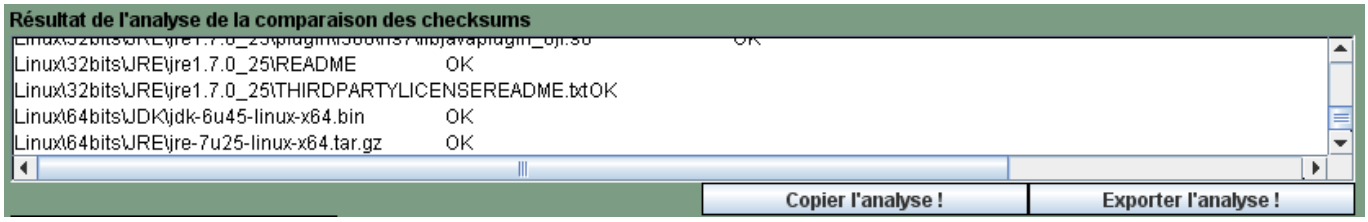
3.4.2. Lancer la comparaison

La comparaison peut être lancée si :

- des clefs ont précédemment été calculées (§3.3 - Calcul des clefs d'intégrité);
- des clefs à comparer ont été importées (§3.4.1 - Importer les clefs à comparer) ;
- le mode de comparaison est en accord avec le type de comparaison souhaité (4.1.4 - Principe de la comparaison), comparaison par arborescence, par nom de fichiers et avec le même algorithme.

La comparaison est exécutée par un clique sur le bouton adéquat : « IHM-10 - Bouton permettant de lancer la comparaison des clefs importées et calculées»

Les résultats de la comparaison sont stockés dans la zone de texte «IHM-11 - Zone de texte contenant le résultat de la comparaison des clefs»



Astuce : Il est possible à tout moment d'interrompre la comparaison en cliquant sur la croix du message d'attente, l'interruption est prise en compte immédiatement.

Typologie des résultats :
OK : Un nom de fichier avec un checksum identique a été trouvé
POK : Le checksum a été trouvé mais il y a une incertitude précisée dans le log sur le résultat
KO : Aucun checksum n'a été trouvé

3.5. RAPPORTS

Le rapport synthétisant les clefs d'intégrité calculées et le résultat de la comparaison, si effectué, est récupérable de deux manières :

- en cliquant sur le bouton « IHM-12 - Bouton permettant de copier le rapport dans le presse papier» : le rapport est copié dans le presse-papier et peut donc être collé dans un document/mail
  ; 

- en cliquant sur le bouton « IHM-13 - Bouton permettant de sauvegarder le rapport dans un fichier texte» : l'outil propose d'enregistrer le rapport dans un fichier texte dont l'utilisateur peut choisir le nom et l'emplacement.
  

Deux types de rapports sont disponibles :

1- Pas de comparaisons effectuées (si les zones de texte IHM-6 & IHM-11 sont vides)
   - le rapport contiendra les clefs calculées.
2- Comparaisons effectuées (si les zones de texte IHM-6 & IHM-11 sont non vides)

- le rapport contiendra les clefs calculées, à comparer et le résultat de la comparaison.

4. PRINCIPES ET LIMITATIONS DE L'OUTIL

Pour les utilisateurs qui veulent en savoir plus

4.1.1. Import des fichiers à calculer

Performance :

Le temps nécessaire pour l'import des fichiers dépend du nombre de fichiers et du nombre de sous dossiers.

Sécurité :

L'import des fichiers concerne uniquement l'emplacement sur le disque, les données ne sont pas chargées dans le logiciel pour des raisons de performance et de sécurité.

4.1.2. Calcul des checksums et algorithmes utilisés

Le calcul d'une clef d'intégrité s'appuie sur la class MessageDigest présente dans le JRE java du PC qui est une bibliothèque de calcul de clef d'intégrité reconnue.

Par sécurité deux calculs sont effectués puis leurs résultats comparés. S'ils sont différents, un troisième calcul est effectué afin de trancher sur la validité du résultat. Ceci ayant pour but de conforter les résultats et de prévenir une modification du fichier pendant le calcul. Ces calculs ont des impacts sur les performances, en effet le temps nécessaire par fichier est doublé.

Performance :

Le temps de calcul dépend de la quantité de fichiers, de la taille des fichiers et des performances de la machine. Les calculs ne sont pas effectués en parallèle et ne sont donc pas optimisés pour une machine à plusieurs cœurs.

Sécurité :

Le principe de l'algorithme est de parcourir le fichier concerné par paquet d'octets et de mettre à jour la clef d'intégrité en fonction du calcul correspondant à l'application du nouveau paquet. Cette méthode a pour avantage de ne pas garder en mémoire le document et donc d'augmenter les performances et la sécurité.

4.1.3. Import des fichiers à comparer

Erreur Heap Memory :

Dans le cas d'un message d'erreur « Heap Memory trop faible », ce message signifie que le fichier importé est trop volumineux pour la mémoire disponible pour l'application, il est donc nécessaire de lancer l'application avec une mémoire plus importante.

La commande adéquate permettant d'augmenter la mémoire disponible pour l'application au démarrage est la suivante :

Java -Xms512M -jar <Emplacement du fichier jar>

L'attribut XmsYYYM permet d'allouer au programme une mémoire de YYY méga. La valeur dépend des données chargées, pour une utilisation standard, cet attribut n'est pas nécessaire.

Performance :

Le temps nécessaire pour l'import des fichiers dépend du nombre de fichiers et de leurs tailles.

4.1.4. Principe de la comparaison

A chaque fichier précédemment calculé sont liés un nom de fichier, une arborescence relative (répertoire parent lors de la sélection des fichiers/dossiers), une clef d'intégrité.

Pour chaque clef calculée, l'outil va analyser chaque ligne de la zone de texte (IHM-6 - Zone de texte affichant les clefs que l'on souhaite comparer aux clefs précédemment calculées) contenant les clefs à comparer et vérifier s'il trouve une clef compatible, un nom de fichier compatible et éventuellement (en fonction du choix utilisateur, Boîte de validation « IHM-7 - Choix du mode de comparaison des clefs ») une arborescence compatible avec l'arborescence relative.

Deux modes de comparaison en fonction de l'état de la boîte de validation « IHM-7 - Choix du mode de comparaison des clefs » :

- Mode de comparaison fichiers activé (**recherche par nom de fichier**)
  - recherche un nom de fichier et une clef sur une même ligne compatible avec les fichiers précédemment calculés. Si l'outil trouve une ligne compatible le résultat est OK, dans le cas contraire KO
- Mode de comparaison fichiers désactivé (recherche par arborescence relative + nom de fichier)
  - recherche un nom de fichier, une clef et une arborescence relative, sur une même ligne, compatible avec les fichiers précédemment calculés. Si l'outil trouve une ligne compatible le résultat est OK, dans le cas contraire KO

Cas particuliers :

1. Dans le cas d'une **recherche par nom de fichiers**, l'outil va tout d'abord vérifier qu'il n'y a pas plusieurs fichiers du même nom dans la liste des fichiers dont l'outil a calculé la clef d'intégrité. Si c'est le cas il prévient l'utilisateur puis effectue le calcul. Le risque étant la présence de deux fichiers identiques avec le même nom dans l'arborescence. Les fichiers de même nom sont tracés à la fin de l'analyse.

Exemple :

Clefs calculées :

/test/**fichier.txt** 5d3dfea0e57ee9772bb142e418b87f7d06ffd2ee

fichier.txt 5d3dfea0e57ee9772bb142e418b87f7d06ffd2ee

Clefs à comparer :

/test/**fichier.txt** 5d3dfea0e57ee9772bb142e418b87f7d06ffd2ee

fichier.txt ed325514ebb5f683b203d1786c620d8af37f992a

Dans cet exemple le résultat sortirait OK alors qu'il devrait sortir KO. Le message pour prévenir l'utilisateur demande donc de revérifier pour les doublons. Même si ce cas est rare, l'outil permet de prévenir ce conflit. Dans

notre cas une vérification par arborescence permet de palier à ce problème (Mode de comparaison fichier désactivé).

2. Dans le cas d'une **recherche par arborescence** l'outil ne pourra pas efficacement distinguer deux fichiers ayant le même nom dans une arborescence de dossiers de même nom répétée.

Exemple :

Checksums calculés :

/test/**test/fichier.txt** 5d3dfea0e57ee9772bb142e418b87f7d06ffd2ee

/test/fichier.txt 5d3dfea0e57ee9772bb142e418b87f7d06ffd2ee

fichier.txt 5d3dfea0e57ee9772bb142e418b87f7d06ffd2ee

Checksums à comparer :

/test/**test/fichier.txt** 5d3dfea0e57ee9772bb142e418b87f7d06ffd2ee

/test/**fichier.txt** 5d3dfea0e57ee9772bb142e418b87f7d06ffd2ee

fichier.txt 5d3dfea0e57ee9772bb142e418b87f7d06ffd2ee

L'outil va détecter ce risque de conflit et l'indiquer dans le log de résultat avec une phrase. L'utilisateur devra donc faire la vérification fichier par fichier. Ce cas est également rare.

Pour notre exemple :

fichier.txt KO Risque de conflit sur le checksum "fichier.txt" avec le checksum "test\fichier.txt"

test\fichier.txt KO Risque de conflit sur le checksum "test\fichier.txt" avec le checksum "test\test\fichier.txt"

test\test\fichier.txt OK

Bonnes pratiques :
Il est conseillé de calculer et comparer les checksums sur des fichiers stables type archive. C'est même une exigence dans certaines normes comme par exemple les normes ECSS-M-ST-40C ou ISO 10303.

Performance :

Le temps nécessaire pour la comparaison dépend du nombre de fichiers dont on a calculé un checksum et du nombre de checksums à comparer.

4.1.5. Problèmes chemin Windows / linux

Dans le cas où les clefs d'intégrité sont calculées sur une plateforme Linux et la liste des clefs à comparer a été calculée sur une plateforme Windows (et vice versa), ces deux listes ne sont pas comparables en l'état avec le mode « **Mode de comparaison fichier désactivé** ». En effet les chemins d'accès ne sont pas écrits de la même manière sous Linux et sous Windows (« \ » sous Windows et « / » sous Linux). Le logiciel contient une macro permettant d'inverser les « / » et le « \ » dans la zone de texte contenant les checksums à comparer « IHM-6 - Zone de texte affichant les clefs que l'on souhaite comparer aux clefs précédemment calculées». La comparaison devient possible après exécution de cette macro.

Pour exécuter la macro, appuyer sur le bouton « IHM-8 - Bouton permettant de remplacer les caractères '/' par '\' et '\' par '/' dans la zone de texte IHM-6».

Exemple :

Checksum calculé

test\test\fichier.txt e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

Checksum utilisé pour la comparaison

test/test/fichier.txt e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

Mise à jour de la zone de texte contenant les checksums utilisés pour la comparaison après l'exécution de la macro

test\test\fichier.txt e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

5. ENVIRONNEMENT NECESSAIRE POUR UTILISER L'OUTIL

En cas de difficultés dans l'utilisation, ce chapitre devrait vous permettre d'y remédier.

5.1. CONFIGURATION REQUISE

Le logiciel CKOUASUM est prévu pour être multiplateforme Linux et Windows et fonctionner en 32 et 64 bits.

Pour fonctionner l'outil nécessite une version JRE 1.6.0 r27 ou supérieur et un environnement compatible avec ce JRE.

A noter que cet outil a été testé sur Windows XP SP2 et Redhat 5 en 32 bits.

5.2. INSTALLATION DE C'KOUASUM

Aucune installation n'est nécessaire pour utiliser CKOUASUM. Il suffit de copier l'outil en local.

5.3. VERIFICATION DES PROVIDERS DISPONIBLES PERMETTANT DE CALCULER LES CLEFS D'INTEGRITE

Ce chapitre s'adresse aux administrateurs de la machine et une modification des providers ne peut être effectuée sans l'accord des responsables sécurité du système d'information de la machine.

L'outil C'KOUASUM effectue les calculs de clefs d'intégrité via la bibliothèque MessageDigest du JRE de la machine. L'utilisation d'un service cryptographique JRE suppose en premier lieu l'instanciation d'une implémentation particulière, fournie par un provider. Ce chapitre a donc pour but de donner les consignes permettant de vérifier que la configuration est compatible avec l'application.

Cette configuration est réalisée pour le JRE Sun en éditant le fichier <JAVA_HOME>/lib/security/java.security. Les providers de confiance sont placés en premier et ceux non sûrs supprimés.

<JAVA_HOME> correspond au répertoire d'installation du JRE.

5.3.1. Provider utilisé lors du développement de C'KOUASUM

L'application a été testée avec la liste de providers suivante comme écrite dans le fichier « java.security » :

```
security.provider.1=sun.security.provider.Sun
security.provider.2=sun.security.rsa.SunRsaSign
security.provider.3=com.sun.net.ssl.internal.ssl.Provider
security.provider.4=com.sun.crypto.provider.SunJCE
security.provider.5=sun.security.jgss.SunProvider
security.provider.6=com.sun.security.sasl.Provider
```

5.3.2. Providers par défaut

La suppression du fichier **<JAVA_HOME>/**lib/security/java.security provoque l'attribution par défaut d'une liste de providers définie par la classe java.security.Security. Avec la bibliothèque standard de Sun ou d'OpenJDK, par ordre de priorité, les providers définis par défaut sont en pratique les suivants :

- sun.security.provider.Sun ;
- sun.security.rsa.SunRsaSign ;
- com.sun.net.ssl.internal.ssl.Provider ;
- com.sun.crypto.provider.SunJCE ;
- sun.security.jgss.SunProvider ;
- com.sun.security.sasl.Provider.

5.3.3. Sécurisation de la liste des providers par l'administrateur machine

La seule manière de modifier la priorité d'un provider depuis une application Java est de le retirer et de le réinsérer dans la liste des providers.

Par conséquent, dans le cas où l'administrateur du poste client souhaite maîtriser l'environnement d'exécution Java, il est recommandé de ne pas accorder aux applications Java les droits permettant de retirer ou de réinsérer des providers. Il doit donc configurer le gestionnaire de sécurité en tant que tel et ne pas accorder les permissions suivantes :

- java.security.SecurityPermission "insertProvider.<nom du provider>" ;
- java.security.SecurityPermission "removeProvider.<nom du provider>" ;
- java.security.SecurityPermission "removeProviderProperty.<nom du provider>";
- java.security.SecurityPermission "loadProviderProperties.<nom du provider>".

Référence :

[1] Rapport d'étude sur le langage Java, 6.4 Cryptographie
[2] http://www.ibm.com/developerworks/java/jdk/security/60/FIPShowto.html
[3] [Con09c], 6.4 Cryptographie
[4] http://www.ibm.com/developerworks/java/jdk/security/60/FIPShowto.html
[5] http://java.sun.com/javase/6/docs/api/java/security/Security.html#insertProviderAt(java.security.Provider,%20int)