COMMISSION de SURVEILLANCE
du SECTEUR FINANCIER

Luxembourg, le 4 janvier 2008

A toutes les personnes et entreprises
surveillées par la CSSF

CIRCULAIRE CSSF 08/334

Concerne : **Spécifications d'encryption pour les déclarants**

Mesdames, Messieurs,

Nous avons l'honneur de porter à votre connaissance un certain nombre de précisions concernant les modalités d'encryption applicables pour le reporting TAF/MIFID à partir du 1er mai 2008. Le détail de ces modalités est décrit dans le document « Spécifications d'encryption pour les déclarants » ainsi que dans le document « Standards techniques nouveaux reportings » (qui en fait partie intégrante).

Le certificat CSSF à utiliser sera publié en temps utile sur le site www.cssf.lu sous la rubrique « Reporting légal ».

Nous nous permettons d'ajouter en ce qui concerne les autres reportings légaux à transmettre à la CSSF que nous y reviendrons le moment venu.

Nous vous prions de recevoir, Mesdames, Messieurs, l'expression de nos sentiments distingués.

COMMISSION DE SURVEILLANCE DU SECTEUR FINANCIER

Simone DELCOURT
Directeur

Arthur PHILIPPE
Directeur

Annexes

COMMISSION de SURVEILLANCE
du SECTEUR FINANCIER

Spécifications d'encryption pour les déclarants

V 1.00

1 Versions

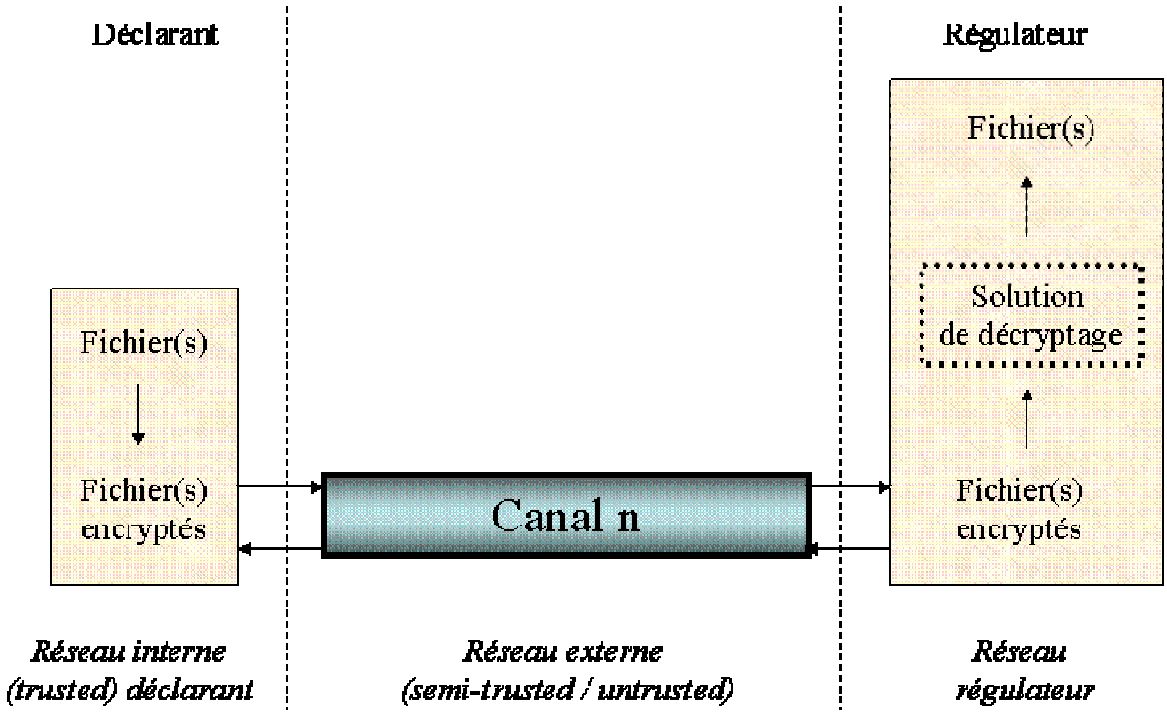
Date	Version	Description
31/12/2007	1.00	Version finale

2 Sommaire

3 Introduction

Le présent document entend mettre en place un concept de sécurité dans le cadre du reporting légal au Luxembourg respectant les normes de confidentialité habituelles en recourant à un encryptage de bout à bout entre le côté source d'une information et le côté destinataire. Ce document a pour objectif de spécifier les caractéristiques techniques et organisationelles à respecter par les déclarants pour instaurer l'encryptage de bout à bout entre le déclarant et la CSSF.

Voici une représentation du concept de bout en bout que le présent document introduit :



4 Spécifications pour les déclarants

Ce chapitre distingue entre :

Type d'intervenant	Caractéristiques
Déclarants	Les entités soumises au reporting
Régulateurs	Les régulateurs définissant le reporting à transmettre et ayant déclaré leur acceptation des spécifications du présent document
Opérateurs de canaux de transmission	Sociétés offrant un service de collecte sécurisé avec transfert aller-retour de fichiers de reporting vers les régulateurs
Editeurs d'un logiciel de reporting	Société offrant un outil de génération des fichiers de reporting
Editeurs d'un logiciel d'encryptage / décryptage	Société offrant un outil d'encryptage /décryptage de fichiers

Il décrit les consignes à respecter par les déclarants lorsqu'ils produisent des fichiers de reporting à destination de la CSSF.

Il faut noter qu'il incombe au déposant de vérifier auprès de son opérateur de canal de transmission si sa solution est bien acceptée par la CSSF.

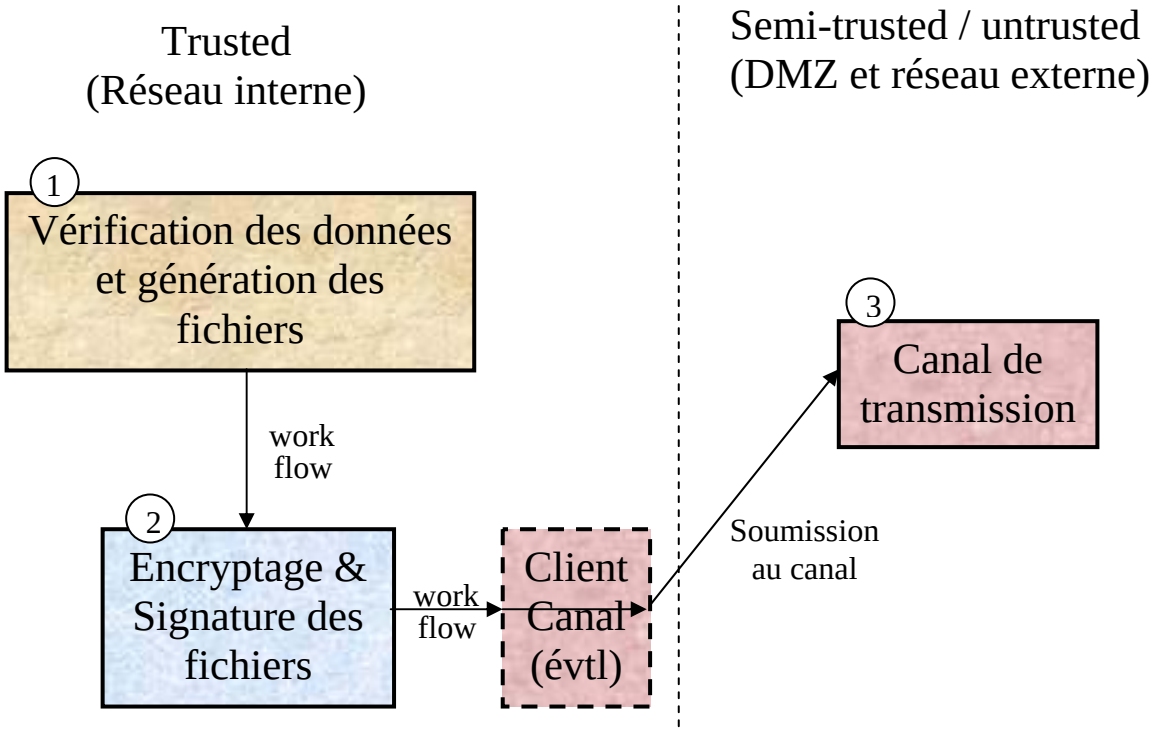
4.1 Dispositions organisationnelles chez le déclarant

Les déclarants sont amenés à réaliser une séparation stricte entre l'encryptage de fichiers à rapporter et leur injection dans le canal de transmission. On différenciera notamment les fonctions suivantes:

1. la génération des fichiers à rapporter
2. l'encryptage du fichier (ou décryptage du fichier de retour)
3. le transfert vers la CSSF à travers le canal de transmission

Il est à veiller à une séparation logique entre les fonctions 2 et 3 qui se montrera notamment à travers le fait que l'échange d'un de ces modules (notamment par un module équivalent d'un autre fournisseur) n'a pas d'impact fonctionnel direct sur les autres modules. Il est aussi à veiller à ce que l'encryptage ait lieu dans le réseau interne du déclarant.

Une illustration du concept à réaliser est montrée ci-dessous :



Il va sans dire que les 3 fonctions clairement séparées peuvent ensuite être reliées par des enchaînements (workflows) automatisés. Si la fonction de génération des fichiers se compose de plusieurs logiciels (évtl de plusieurs fournisseurs), l'encryptage se fera après la dernière instance ayant traité le fichier.

Une large intégration entre les fonctions 1 (génération des fichiers à rapporter) et 2 (encryptage/décryptage du fichier) est possible ; au cas où un déclarant souhaite utiliser un module d'encryption de son choix, l'éditeur de logiciel de reporting et l'opérateur du canal de transmission doivent accepter ce choix.

Il n'est pas exclu qu'un opérateur de canal ou un éditeur de logiciel de reporting agisse en même temps comme fournisseur de logiciel pour les autres fonctions mentionnées (y inclus la fonction d'encryptage / décryptage de fichiers) ; les principes du présent document doivent cependant être respectés.

4.2 Certificats

Les seuls certificats autorisés pour l'encryptage de fichiers par les soins du déclarant sont les certificats SSL de l'autorité de certification Luxtrust. Toutes les durées de validité (1 an, 3 ans, 5 ans) sont valables, les clés certifiées peuvent avoir soit 1024, soit 2048 bits. La CSSF se réserve le droit d'augmenter la longueur des clés minimale en fonction des besoins de sécurité futurs.

La CSSF n'accepte que des certificats valides (e. a. non expirés); à cet effet, il y aura une comparaison systématique de chaque certificat déclarant utilisé contre la liste de révocation (CRL) de Luxtrust lors de la réception d'un rapport encrypté. La CSSF se réserve la possibilité d'utiliser des CRL offline (avec donc un petit décalage de la mise à jour des CRL).

Les déclarants sont de leur côté également obligés de vérifier la validité du certificat de la CSSF avant l'encryptage des données et de n'utiliser qu'un certificat valide à cet effet.

Tous les rapports d'un déclarant se signent avec le même (et donc un seul) certificat. Le travail en interne chez le déclarant avec des copies du certificat (utilisées p.ex. par des sous-entités du déclarant) est autorisé ; il va sans dire que l'utilisation correcte de toutes les copies de son certificat est de l'entière responsabilité du déclarant.

4.3 Procédure d'enregistrement des certificats

Le déclarant enverra à la CSSF :

- un courrier électronique à l'adresse certrep@cssf.lu contenant les informations suivantes :
    - Le canal (ou les canaux) à travers le(s)quel(s) des fichiers signés avec ce certificat seront envoyés
    - Le code BIC pour le reporting TAF
    - Le numéro signalétique attribué par la CSSF (si applicable)
    - Le numéro du certificat (non nécessaire si le certificat est correctement attaché)
    - Le nom du déclarant
    - Nom d'une personne de contact
    - Prénom d'une personne de contact
    - Téléphone d'une personne de contact
    - Adresse-mail d'une personne de contact
    - **Fichier attaché** : le certificat Luxtrust utilisé pour la signature (formats autorisés spécifiés dans le document « Standards techniques nouveaux reportings »)
- un courrier officiel dûment signé indiquant le numéro du certificat avec lequel ses rapports seront signés

Le courrier électronique sera utilisé par la CSSF pour l'enregistrement des certificats déclarants, le courrier officiel impliquera la validation (activation) du certificat enregistré (après vérification du numéro).

En cas de changement de certificat (p.ex. à la fin de la période de validité du certificat précédent), le déclarant effectuera la même procédure au moins 5 jours ouvrables avant la fin de validité de l'ancien certificat pour le nouveau numéro de certificat. Après la confirmation de l'activation du certificat à la CSSF, le nouveau certificat pourra être utilisé.

Le déclarant a le droit de passer par une société de services tierce pour générer ses rapports et pour les envoyer à la CSSF. Le certificat à enregistrer dans ce cas est celui de la société de services tierce. Le courrier électronique ci-dessus peut alors se faire en bloc par la société de services tierce pour tous ses clients ; le courrier officiel se fera de toute façon par chaque déclarant.

4.4 Algorithmes d'encryptage / signature / compression des fichiers

Les algorithmes en question sont définis dans le document externe « Standards techniques nouveaux reportings »

5 Dispositions de transition

Le présent alinéa s'adresse aux déposants qui utilisent actuellement un canal de transmission qui ne répond pas encore aux spécifications d'encryption expliquées ci-dessus.

La CSSF mettra en place dans ses systèmes internes un nouveau certificat Luxtrust. Ce certificat sera publié sur le site www.cssf.lu et sera à utiliser pour l'encryptage de tous les rapports du déclarant.

Lorsqu'un déclarant a mis à jour son environnement software et intégré la fonction d'encryptage dans son réseau interne, il demande à son opérateur de canal la reconfiguration de son canal pour lui permettre de suivre les spécifications du présent document. Il active également le décryptage des fichiers de retour par son module de décryptage.

La réutilisation du certificat Luxtrust (qui est actuellement configuré au niveau du canal) est possible ; ce certificat peut donc être utilisé dans le module d'encryption interne end-to-end s'il n'est plus utilisé à l'intérieur du canal.

COMMISSION de SURVEILLANCE
du SECTEUR FINANCIER

Standards techniques
nouveaux reportings

V 1.00

1 Versions

Date	Version	Description
31/12/2007	1.00	Version finale

2 Sommaire

3 Standards à appliquer

Le présent document définit les standards techniques mandatoires pour les reportings applicables.

3.1 Algorithmes d'encryptage / signature des fichiers

Les standards choisis sont les suivants :

3.1.1 Cryptage / décryptage

Voici les spécifications à réaliser:

Algorithme de chiffrement symétrique	Algorithme AES 256 CBC (Rijndael) avec des clés d'une longueur de 256 bits (clé de session)
Algorithme de chiffrement asymétrique utilisé pour chiffrer la clé de session	Algorithme RSA avec au moins 1024 bits se basant sur les certificats Luxtrust
Padding utilisé avec l'algorithme de chiffrement symétrique	PKCS#5 (Standard Block Padding)
Padding d'encryption de la clé de session	Standard Block Padding (aka PKCS padding) défini dans section [8.1] "Encryption-block formatting" du document "PKCS #1: RSA Encryption Standard"

3.1.2 Structure des données

Voici les spécifications à réaliser:

Structure des données	PKCS#7 version 1.5
Ajoute certificat de signature	Oui, dans la structure PKCS#7

3.1.3 Signature électronique

Voici les spécifications à réaliser:

Algorithme de hashage	sha 1
Algorithme d'encryption	RSA
Attached content	Oui
Contre-signature	Non
Signatures multiples	Non

3.1.4 Ordre des opérations

Voici les spécifications à réaliser:

Ordre des opérations	Encryptage avant signature

3.1.5 Exemple

-----BEGIN PKCS7-----
MIK0jQYJKoZIhvcNAQcDoIK0fjCCtHoCAQAxggExMIIBLQIBADCBlTCBjzELMAkG
A1UEBhMCTFUxEzARBgNVBAgTCkx1eGVtYm91cmcxGTAXBgNVBAcTEEVzY2gtc3Vy
... stripped content ...
eALKKLsYzCk6zv3M4v24KmgdBRpKCcbwysXru1Vx1MnBRksuE2hdacuq72U3itaV
mg==
-----END PKCS7-----

3.2 Compression (génération de fichiers .zip)

Voici les spécifications à réaliser au cas où le reporting en question spécifie l'utilisation d'un archive .zip pour l'envoi des données:

Algorithme de compression	RFC 1951 (DEFLATE Compressed Data Format Specification version 1.3)
Archives multi-volumes (multi-part zipfile)	Non
Taille maximale d'un fichier dans l'archive	2 Giga-octets
Codepage	UTF-8

3.3 Formats de certificats acceptés pour l'enregistrement

Format	Description	Extension (Windows)
PEM	(fichier text -----BEGIN CERTIFICATE-----…-----END CERTIFICATE-----)	.cer
DER	(fichier binaire)	.cer ou .der
PKCS7	fichier binaire	.p7b