COMMISSION de SURVEILLANCE du SECTEUR FINANCIER

In case of discrepancies between the French and the English text, the French text shall prevail

Luxembourg, 4 January 2008

To all persons and undertakings under the supervision of the CSSF

CIRCULAR CSSF 08/334

Re: **Encryption specifications for reporting firms**

Ladies and Gentlemen,

We are pleased to inform you that certain details relating to the encryption methods for TAF/MiFID reporting will be applicable as of 1 May 2008. Details of these methods are described in the documents "Encryption specifications for the reporting firms" as well as "Technical standards for new reportings" (which are part of this circular).

The CSSF certificate to be used will be published in due time on the website www.cssf.lu, section Legal reporting.

Please note that we will refer to the other legal reportings to be transmitted to the CSSF in due time.

Yours sincerely,

COMMISSION DE SURVEILLANCE DU SECTEUR FINANCIER

Simone DELCOURT
Director

Arthur PHILIPPE
Director

Appendices

COMMISSION de SURVEILLANCE
du SECTEUR FINANCIER

In case of discrepancies between the French and the English text, the French text shall prevail

Encryption specifications for reporting entities

V 1.00

1 Versions

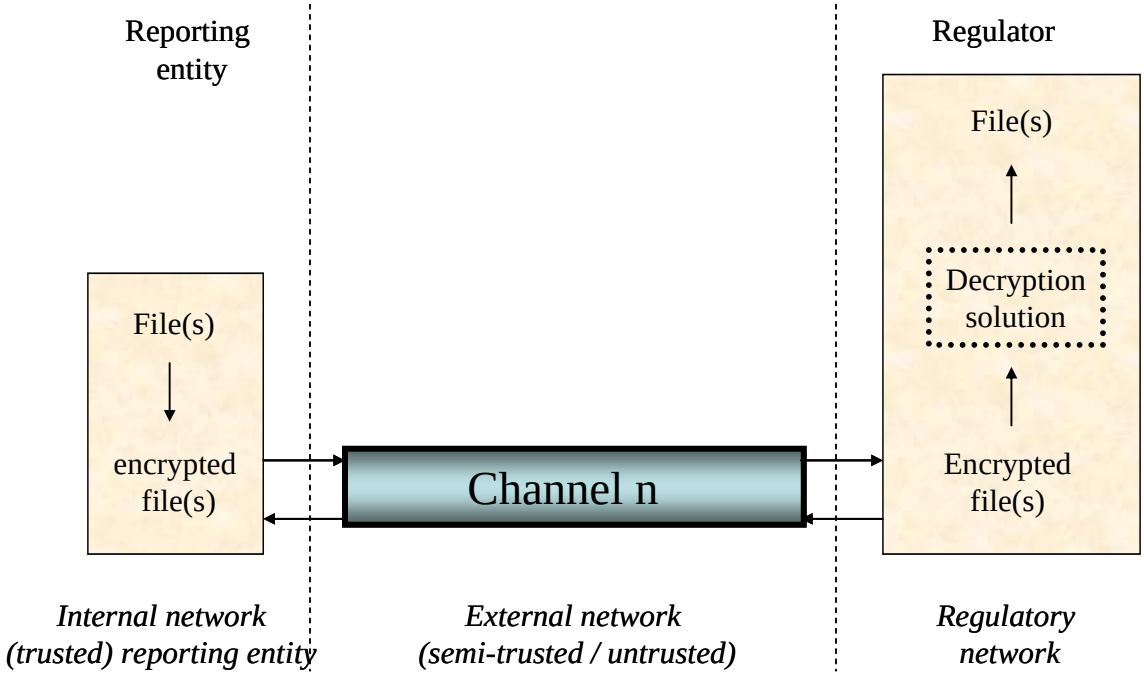
Date	Version	Description
31/12/2007	1.00	Final version

2 Summary

3 Introduction

This document is setting up a security concept for legal reporting in Luxembourg while observing at the same time the usual confidentiality standards by using the End-to-end encryption between the source of information and the recipient. The purpose of this document is to specify the technical and organisational characteristics to be observed by the reporting entities in order to implement the End-to-end encryption between the reporting entity and the CSSF.

The following illustration represents the End-to-end concept as introduced by this document:



4 Specifications for reporting entities

This chapter distinguishes between:

Type of intervening party	Characteristics
Reporting entities	Entities subject to reporting
Regulators	Regulators defining the reporting to be transmitted and having accepted the specifications of this document
Transmission channel operators	Companies offering a secured collection service with a return transfer of reporting files to the regulators
Reporting software publishers	Company offering a generation tool for reporting files
Encryption / decryption software publishers	Company offering an encryption / decryption tool for files

It provides guidelines the reporting entities have to adhere to when they generate reporting files to be sent to the CSSF.

Please note that the reporting entitiy is responsible for verifying with its transmission channel operator if its reporting system has indeed been approved by the CSSF.

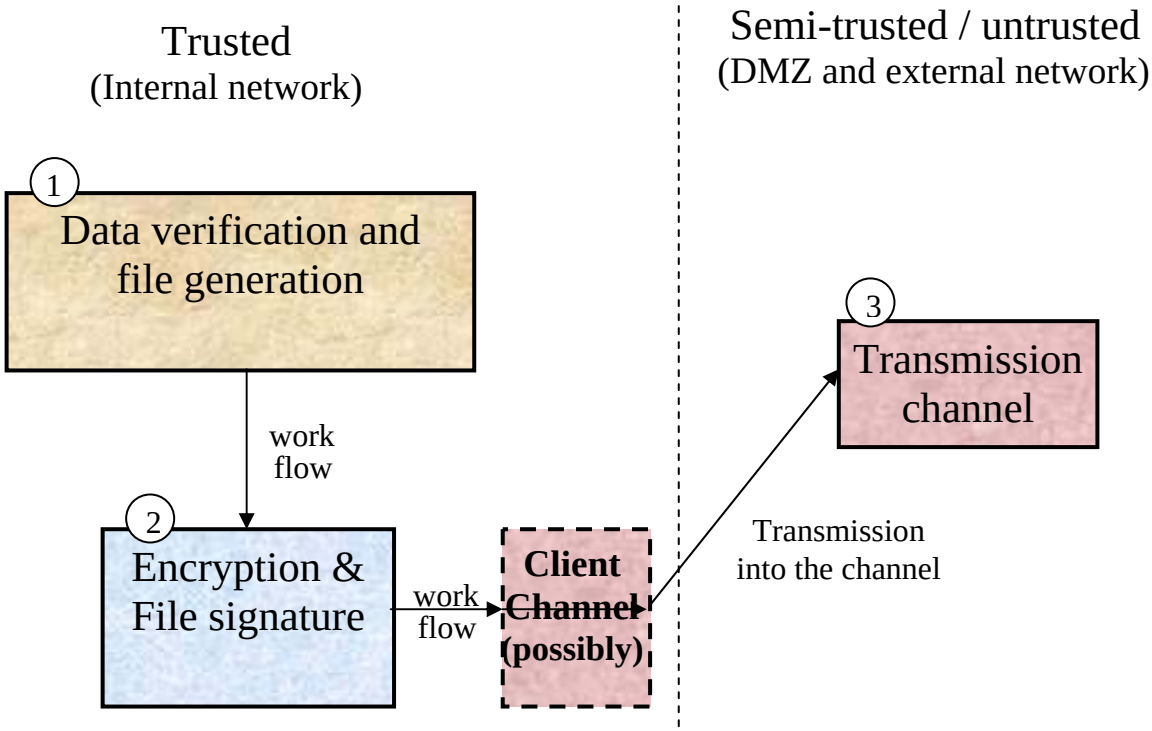
4.1 Organisational provisions for the reporting entity

The reporting entities must set up a strict separation between the encryption of the files to transmit and their injection into the transmission channel. The following functions will notably be distinguished:

1. the generation of files to be reported
2. file encryption (or feedback file decryption)
3. transfer to the CSSF through the transmission channel

There must be a logical separation between the functions 2 and 3 which notably appears when the change of one of these modules (notably by a similar module of another provider) has no direct functional impact on the other modules. It must also be ensured that the encryption takes place within the internal network of the reporting entity.

The following illustration shows the concept to be realised:



The 3 clearly separated functions may of course be linked afterwards by automatic workflows. If the function of file generation consists of several software (possibly of several providers), the encryption will be performed after the last software (provider) has processed the file.

A large integration of functions 1 (generation of files to be reported) and 2 (file encryption / decryption) is possible; if the reporting entity wishes to use an encryption module of its choice, the reporting software publisher and the transmission channel operator must accept this choice.

It is not excluded that a channel operator or a reporting software publisher acts at the same time as a software provider for the other mentioned functions (including the file encryption / decryption function); the principles of this document must nevertheless be observed.

4.2 Certificates

The only certificates authorised for the file encryption by the reporting entity are SSL certificates from the certification authority Luxtrust. All the validity periods (1 year, 3 years, 5 years) are accepted and the certified keys may be either 1024 or 2048 bits. The CSSF reserves the right to increase the minimal key length based on the future needs of security.

The CSSF only accepts valid certificates (i.e. not expired) and for this purpose there will be a systematic comparison of each certificate used by the reporting entity and the Luxtrust revocation list (CRL) during the receipt of the encrypted report. The CSSF reserves the right to use CRL offline (thus with a slight time-lag in the CRL update).

The reporting entities must for their part also verify the validity of the CSSF certificate before the data encryption and must only use a valid certificate for this purpose.

All the reports of a reporting entity are signed with the same (and thus only one) certificate. Internal work at the reporting entity with copies of the certificate (used, for example, by sub-entities of the reporting entity) is authorised. Nevertheless the appropriate use of all the copies of its certificate is under the full responsibility of the reporting entity.

4.3 Registration procedure for the certificates

The reporting entity must send to the CSSF:

- an e-mail on the address certrep@cssf.lu which contains the following information:
    - The channel (or channels) through which the files signed with this certificate will be sent
    - The BIC code for TAF reporting
    - The identification number allocated by the CSSF (where applicable)
    - The certificate number (not necessary if the certificate is correctly attached)
    - The name of the reporting entity
    - Surname of a contact person
    - Forename of a contact person
    - Phone number of a contact person
    - E-mail address of a contact person
    - **Attached file**: Luxtrust certificate used for the signature (authorised formats specified in the document "Technical standards for new reportings")
- an official letter duly signed indicating the certificate number with which the reports will be signed

The e-mail will be used by the CSSF for the registration of reporting certificates and the official letter will imply the validation (activation) of the registered certificate (after the verification of the certificate number).

In the event of change of certificate (i.e. at the end of the validity period of the preceding certificate), the reporting entity will execute the same procedure at least 5 working days prior to the expiry date of the old certificate for the new certificate number. After the confirmation of the certificate activation by the CSSF, the new certificate may be used.

The reporting entity has the right to go through a third party service company to generate its reports and send them to the CSSF. The certificate to be registered in that case is the one from the third party service company. The above e-mail may then be sent as a whole by the third service company for all its clients. The official letter will be sent anyway by each reporting entity.

4.4 Algorithms for encryption / signature / compression of files

The algorithms in question are defined in the external document "Technical standards for new reportings"

5 Transition provisions

This paragraph is intended for the reporting entities currently using a transmission channel which does not yet meet the encryption specifications stated above.

The CSSF will set up a new Luxtrust certificate in its internal systems. This certificate will be published on the website www.cssf.lu and will be used for the encryption of all the reporting entity's reports.

When a reporting entity has updated its environment software and included the encryption function in its internal network, it requests of its channel operator the reconfiguration of the channel in order to enable the reporting entity to follow the specifications of this document. It also activates the feedback file decryption *via* its decryption module.

The reuse of the Luxtrust certificate (which is currently configured at the channel level) is possible. This certificate may thus be used in the internal End-to-end encryption module if it is not used within the channel anymore.

COMMISSION de SURVEILLANCE
du SECTEUR FINANCIER

In case of discrepancies between the French and the English text, the French text shall prevail

Technical standards for new reportings

V 1.00

1 Versions

Date	Version	Description
31/12/2007	1.00	Final version

2 Summary

3 Standards to apply

This document defines the mandatory technical standards for applicable reportings.

3.1 Algorithms for encryption / signature of files

The chosen standards are the following:

3.1.1 Encryption / decryption

The following specifications shall be realised:

Symmetrical algorithm ciphering	Algorithm AES 256 CBC (Rijndael) with 256 bits keys (session key)
Asymmetrical algorithm ciphering used to encode the session key	Algorithm RSA with at least 1024 bits based on Luxtrust certificates
Padding used with the symmetrical algorithm ciphering	PKCS#5 (Standard Block Padding)
Encryption padding of the session key	Standard Block Padding (aka PKCS padding) defined in section [8.1] “Encryption-block formatting” of the document “PKCS #1: RSA Encryption Standard”

3.1.2 Data structure

The following specifications shall be realised:

Data structure	PKCS#7 version 1.5
Addition signature certificate	Yes, in the structure PKCS#7

3.1.3 Electronic signature

The following specifications shall be realised:

Hash algorithm	sha 1
Encryption algorithm	RSA
Attached content	Yes
Counter signature	No
Multiple signatures	No

3.1.4 Order of operations

The following specifications shall be realised:

Order of operations	Encryption before signature

3.1.5 Example

-----BEGIN PKCS7-----

MIK0jQYJKoZIhvcNAQcDoIK0fjCCtHoCAQAxggExMIIBLQIBADCBlTCBjzELMAkG

A1UEBhMCTFUxEzARBgNVBAgTCkx1eGVtYm91cmcxGTAXBgNVBAcTEEVzY2gtc3Vy

... stripped content ...

eALKKLsYzCk6zv3M4v24KmgdBRpKCcbwysXru1Vx1MnBRksuE2hdacuq72U3itaV

mg==

-----END PKCS7-----

3.2 Compression (generation of .zip files)

The following specifications shall be realised in case the reporting in question specifies the use of a .zip archive for the dispatch of data:

Compression algorithm	RFC 1951 (DEFLATE Compressed Data Format Specification version 1.3)
Multi-volumes archives (multi-part zipfile)	No
Maximum file size in the archive	2 Gigabytes
Codepage	UTF-8

3.3 Certificate formats accepted for registration

Format	Description	Extension (Windows)
PEM	(file text -----BEGIN CERTIFICATE-----…----- END CERTIFICATE-----)	.cer
DER	(binary file)	.cer or .der
PKCS7	binary file	.p7b