FRENCH ENCRYPTION REGULATION

YVES LE ROUX-DIGITAL EQUIPMENT

VERSION: 05 MAY 1998

SUMMARY

In the French system, the cryptographic products (hardware or software) are classified according to the service(s) to be delivered by the product: Authentication and/or Confidentiality. According to "The Regulation and Decision of the Council of the European Union of 19 December 1994 concerning the control of the exports of dual-use goods", import of Cryptographic products from E.U. Members Countries is authorized. I will try to summarize in one table the French regulation:

Functionality	Supply	Import from outside E.U	Usage	Export
Authentication Only	Declaration	Declaration	Free	Declaration
Confidentiality with Key length < 40 bits	Authorization Or Declaration *	Authorization or Free *	Authorization or Free *	Authorization
Confidentiality using Key Escrow Agency	Authorization	Authorization	Free	Authorization
Other Confidentiality	Authorization	Authorization	Authorization	Authorization

* In order to be eligible for the dispensation, the supplier MUST include, in every cyphertext, a fixed field, the cleartext of which MUST be given to the French Authorities. This will allow the French Authorities to do a attack on the cypher text with a known plaintext and to be sure to succeed in 2^{40} operations by comparing the cyphertext and the known plaintext encrypted…(Decret 98-207 and 98-206 du 23 mars 1998 Annexe clause 1)

Cryptography that does not provide confidentiality or provide confidentiality with a key length inferior to 40 bits can be used without restriction, but supply of this cryptography still has to be declared.

A supplier is exempted from the formalities for use exclusively for developing, validating or demonstrating cryptography, if he informs the French Authorities at least two weeks in advance.

Declaration and Authorization have to be accepted by Authorities prior to any action.

The files to be completed for Declaration and Authorization are almost identical. They have two parts one administrative and one technical giving all design and implementation details of the products.
The main difference between Declaration and Authorization is the delay for the Administration to reply: For Declaration it is 1 month, for an Authorization 4 months. In both cases, the Administration has a 1-month delay for consider if the files are complete or not. If not, the Administration will request complementary information and the delay will restart from the date of completion.

Currently, the only authorized Key Escrow Agency is " Le Service Central de la Sécurité de Systèmes d'Information"(SCSSI) a Prime Minister Office…. (Arrêté du 13 mars 1998 fixant la liste des organismes agréés pouvant recevoir dépôt des conventions secrètes)

TEXTS OF REFERENCE

(AVAILABLE IN FRENCH ONLY THROUGH HTTP://WWW.IN2P3.FR/SECUR/LEGAL/LEGI-CRYPTO.HTML)

The regulation is contained in a very lengthy collection of texts:

- Loi no 90-1170 du 29 décembre 1990 modifiée sur la réglementation des télécommunications, notamment son article 28

- Décret no 98-101 du 24 février 1998 définissant les conditions dans lesquelles sont souscrites les déclarations et accordées les autorisations concernant les moyens et prestations de cryptologie

- Décret no 98-102 du 24 février 1998 définissant les conditions dans lesquelles sont agréés les organismes gérant pour le compte d'autrui des conventions secrètes de cryptologie en application de l'article 28 de la loi no 90-1170 du 29 décembre 1990 sur la réglementation des télécommunications

- Arrêté du 13 mars 1998 définissant la forme et le contenu du dossier concernant les déclarations ou demandes d'autorisation relatives aux moyens et prestations de cryptologie

- Arrêté du 13 mars 1998 définissant les dispositions particulières qui peuvent être prévues dans les autorisations de fourniture d'un moyen ou d'une prestation de cryptologie

- Arrêté du 13 mars 1998 fixant la forme et le contenu du dossier de demande d'agrément des organismes gérant pour le compte d'autrui des conventions secrètes

- Arrêté du 13 mars 1998 définissant le modèle de notification préalable par le fournisseur de l'identité des intermédiaires utilisés pour la fourniture de moyens ou prestations de cryptologie soumis à autorisation

- Arrêté du 13 mars 1998 fixant la liste des organismes agréés pouvant recevoir dépôt des conventions secrètes

- Arrêté du 13 mars 1998 fixant le tarif forfaitaire pour la mise en oeuvre des conventions secrètes au profit des autorités mentionnées au quatrième alinéa du II de l'article 28 de la loi no 90-1170 du 29 décembre 1990 sur la réglementation des télécommunications

- Décret no 98-206 du 23 mars 1998 définissant les catégories de moyens et de prestations de cryptologie dispensées de toute formalité préalable

- Décret no 98-207 du 23 mars 1998 définissant les catégories de moyens et de prestations de cryptologie pour lesquelles la procédure de déclaration préalable est substituée à celle d'autorisation

DETAILED UNDERSTANDING

France has the most comprehensive cryptologic control and use regime in Europe, and possibly worldwide.
In the French Regulation, cryptographic equipment is separated into three categories. The first category includes encryption devices and services, the technical characteristics and usage conditions of which should not effect the interests of national defence and internal and external State security. The second category includes equipment which "does not provide confidentiality, particularly when its only purpose is to authenticate a communication or to ensure the integrity of the information transmitted". The third category includes cryptographic methods or devices, which provide for the confidentiality of data or transmissions.
But, a supplier is exempted from the formalities for use exclusively for developing, validating or demonstrating cryptography, if he informs the French Authorities at least two weeks in advance.

A- FIRST CATEGORY

The exhaustive list of encryption devices and services, the technical characteristics and usage conditions of which should not effect the interests of national defence and internal and external State security is in the "Annexe of the Décret no 98-206 du 23 mars 1998 définissant les catégories de moyens et de prestations de cryptologie dispensées de toute formalité préalable"

It includes Pay-TV decoder, DVD readers, Automatic Teller Machines, electricity meters.

In the table contained in the annex, a column indicates which operations are in derogation of formalities.

Four kind of operations are considered: F = Supply, U = Use, I = Import, E = Export

Only the devices with F,U,E,I are free of all formalities

As an example, a software which encrypts password and only passwords with any kind of cryptology needs a license subject to a declaration before any supply…..but Usage, Export and Import are unrestricted…

B- SECOND CATEGORY: AUTHENTICATION-ONLY DEVICE AND SERVICES

The use of this category of device is unrestricted, but Supply, Import and Export are subject to declaration.

DECLARATION AND AUTHORIZATION REQUEST

Content of the Declaration and Authorization Request is defined in the " Arrêté du 13 mars 1998 définissant la forme et le contenu du dossier concernant les déclarations ou demandes d'autorisation relatives aux moyens et prestations de cryptologie".

Contents for Declaration and Authorization Request are almost identical. They have two parts:one administrative and one technical which must provide a "description of the security functions or mechanisms, including a detailed description of the cryptologic algorithm(s) (mathematical formulae) used and the system for the creation, development, and protection of the secret conventions; the software must be provided . . . in the source language."

.
The main difference between Declaration and Authorization is the delay for the Administration to reply: For Declaration, it is 1 month, for an Authorization, it is 4 months. At the end of this delay, a non-reply by the Administration is equivalent to an acceptation.

In both cases, the Administration has a 1-month delay for consider if the files are complete or not. If not, the Administration will request complementary information and the delay will restart from the date of the files completion.

Another difference is the fact that a product with a license following a declaration may be resale by any company; for a product subject to authorization, the Prime Minister Office has the right to reject the right to supply to one or more proposed reseller.

A supply, import or export license is given for up to 5 years and the usage one up to 10 years.

C- THIRD CATEGORY: CONFIDENTIALITY DEVICES AND SERVICES

In this category, we must consider three sub-categories:

- Cryptography with key length limited to 40 bits and a known plaintext inserted
- Cryptography without limit on the key length but using a Key Escrow Agent
- Others types of Cryptography

C-1 Cryptography with key length limited to 40 bits and a known plaintext inserted

The Import and Use of this type of confidentiality devices and services are unrestricted and free of formalities, but the supply is subject to a Declaration and the Export to an Authorization.

In order to be accepted in this type of confidentiality devices and services, the supplier MUST:

- Use a symmetrical algorithm with a key length limited to 40 bits using the Electronic CodeBook (ECB) mode of operation (CBC, CFB and OFB modes of operation are not allowed) AND
- Include in every cyphertext cyphertext a fixed field, the cleartext of which MUST be given to the French Authorities. This will allow the French Authorities to do a attack on the cypher text with a known plaintext and to be sure to succeed in 2^{40} operations by comparing the cyphertext and the known plaintext encrypted…(Decret 98-207 du 23 mars 1998 Annexe clause 1)

If the confidentiality devices or services do not fulfill those two conditions, they are considered as relevant of the "Others types of Cryptography" and consequently, the Import, Export, Use and Supply of them are subject to an Authorization.

C-2 Cryptography without limit on the key length but using a Key Escrow Agent (KEA)

French Authorities are ahead of others Countries in specifying the need for a "Tiers de Confiance" which may be translated as a Key Escrow Agent (KEA).

In order to be considered in this category, "the encryption device must provide confidentiality functions based solely on secret conventions managed under approved procedures and by an organisation

approved" by the French Authorities. If a KEA and its key-escrow scheme have been approved, users who escrow their keys with the KEA will be able to freely use the cryptography scheme with these keys. The KEAs will be required to hand over keys to law enforcement under certain conditions.

The use and import of this type of confidentiality devices and services are unrestricted and free of formalities, but the Supply and the Export are subject to an Authorization.

Key Escrow Agent (KEA) are subject to prior approval from the Prime Minister. The "Décret no 98-102 du 24 février 1998 définissant les conditions dans lesquelles sont agréés les organismes gérant pour le compte d'autrui des conventions secrètes de cryptologie en application de l'article 28 de la loi no 90-1170 du 29 décembre 1990 sur la réglementation des télécommunications" defines the conditions governing the approval of these organisations. This Decret 98-102 addresses, among others, the duration of a license to operate, the information the KEA has to provide to SCSSI, the information to register, user contract terms, a register of key requests by law enforcement and a separate (classified) one for key requests by security agencies, security measures, and how to handle when ceasing the activity. Interestingly, the KEA employees must have a French security clearance.

The " Arrêté du 13 mars 1998 fixant la forme et le contenu du dossier de demande d'agrément des organismes gérant pour le compte d'autrui des conventions secrètes" set out the procedures and technical provisions required to implement the obligations.

Currently, the only KEA approved by the Prime Minister is the "Service Central de la Sécurité de Systèmes d'Information"(SCSSI) a Prime Minister Office…. (Arrêté du 13 mars 1998 fixant la liste des organismes agréés pouvant recevoir dépôt des conventions secrètes)

C-3 Others types of Cryptography

The Import, Export, Use and Supply of this type of confidentiality devices and services are subject to an Authorization.
A supply authorization for collective use exempts users from acquiring a use authorization. Authorization can be subjected to certain conditions in order to reserve the use of certain types of cryptography to defined user or application categories. Furthermore, the SCSSI have the right to subject the authorization to a mandatory Key Escrow.

OTHERS INTERESTING CONSIDERATIONS

When supplying cryptographic products and services, a notice with the license number has to be included in the documentation provided to the purchaser.

The unlawful supply, import or export is subject to a "contravention de 5eme classe". The unlawful usage of products is subject to a "contravention de 5eme classe" if it is a product subject to authorization and a "contravention de 4eme classe" if it is a product subject to declaration.

When the Authorities will request a key from the KEA, they will pay 400 FF to the KEA for this operation.

Legal Notice

FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you.
In no event shall DIGITAL be liable for any damages whatsoever, and in particular DIGITAL shall not be liable for special, indirect , consequential, or incidental damages, or damages for lost profits, loss of revenue, or loss of use, arising out of or related to any DIGITAL Web Site or the information contained in it, whether such damages arise in contract, negligence, tort, under statute, in equity, at law or otherwise