

**Ludovic FLAMENT**

13, Rue ZEFFE

62160 AIX-NOULETTE, FRANCE

Email : [ludovic.flament@cryptograph-ic.com](mailto:ludovic.flament@cryptograph-ic.com)Site web : <http://www.cryptograph-ic.com>

GSM : +33 (0) 610 514 811

Date de naissance : 6 Février 1974

Marié, 1 enfant



## Expert Cryptographie, PKI, Critères Communs - Fondateur

### EXPERIENCES PROFESSIONNELLES

- Depuis  
Mars 2011 **Consultant développement API cryptographique (ING Direct)**
- Réalisation d'une API cryptographique pour le chiffrement et la signature de message de paiement bancaire
  - Support de l'utilisation de HSM (Hardware Security Module)
- Version en mode Client/Serveur pour les OS ne supportant pas les fonctions cryptographiques (Mainframe)
- Depuis  
Juin 2011 **Assistance pour une évaluation Critères Communs (Société confidentielle)**
- Dans le cadre d'une assistance pour une évaluation aux Critères Communs (EAL3+ / QS) d'un produit de sécurité, les tâches suivantes sont réalisées
- Gestion du projet
  - Rédaction et pilotage de la rédaction des documents techniques
  - Relation avec le CESTI et l'ANSSI.
- Décembre 2010  
- Janvier 2011 **Expertise cryptographique d'un logiciel (Société confidentielle) :**
- Analyse du code source
  - Test de conformité des algorithmes implémentés avec les standards
  - Recherche de vulnérabilités et tests d'attaques
- Janvier 2010  
- Décembre 2010 **Consultant développement API cryptographique (ING Direct)**
- Réalisation d'une API cryptographique pour le chiffrement et la signature de message de paiement bancaire
  - Support de l'utilisation de HSM (Hardware Security Module)
  - Version en mode Client/Serveur pour les OS ne supportant pas les fonctions cryptographiques (Mainframe)
- Avril 2010  
- Août 2011 **Assistance pour une évaluation Critères Communs (Société confidentielle)**
- Dans le cadre d'une assistance pour une évaluation aux Critères Communs (EAL3+ / QS) d'un produit de sécurité, les tâches suivantes sont réalisées
- Gestion du projet
  - Relation avec le CESTI et l'ANSSI.
  - Pilotage de la rédaction de documents techniques
- Novembre 2008  
- Décembre 2009 **Assistance pour une évaluation Critères Communs / Expert en cryptographie / Responsable d'équipe (NETASQ) :**
- Rédaction et pilotage de la rédaction des documents techniques
  - Relation avec le CESTI et la DCSSI.
  - Responsable d'une équipe de 6 ingénieurs, supervision des projets
  - Supervision et développement des évolutions des produits. Ces évolutions étant pour les produits eux-mêmes (licence, mise à jour, protocole de communication, ...) et pour les utilisateurs (VPN-SSL, authentification, ...).
  - Supervision et développement d'un service de PKI embarqué sur les produits.
- Avril 2008 –  
Novembre 2008 **Assistance pour une évaluation Critères Communs (NETASQ) :**
- Dans le cadre d'une assistance pour une double évaluation aux Critères Communs (EAL3+ / QS, EAL4+) d'un produit de sécurité, les tâches suivantes sont réalisées :
- Aide à la définition du périmètre
  - Rédaction de la cible de sécurité et d'une partie des documents techniques
  - Pilotage de la rédaction de documents techniques
  - Relation avec le CESTI et la DCSSI.

- Février 2008 **Cryptographie Ingénierie & Conseil ( Cryptograph'IC )**  
 WebSite : <http://www.cryptograph-ic.com>  
 Fondateur et dirigeant d'une société de services spécialisée dans les domaines de la cryptographie et PKI. Cette société propose de l'expertise, du développement, de l'architecture, du design de protocole, ... pour les sociétés désirant utilisées des fonctionnalités cryptographiques.
- Juin 2007 - **Consultant en cryptographie : société SONY NSCE**  
 Février 2008 Mission de réalisation d'une démonstration technologique utilisant les DRMs Marlin dans le cadre de vidéo à la demande.
- Juin 2001 - **Responsable d'équipe, Expert en cryptographie** pour la société **NETASQ**  
 Juin 2007 (<http://www.netasq.com>).  
 Poste (Février 2006 – Juin 2007): Project manager
  - Responsable d'une équipe de 4 ingénieurs
  - Supervision des projets
  - Reporting à la direction
 Poste (Juin 2001 – Janvier 2006) : Expert en cryptographie et PKI
  - Supervision et développement des évolutions des produits. Ces évolutions étant pour les produits eux-mêmes (licence, mise à jour, protocole de communication, ...) et pour les utilisateurs (VPN-SSL, authentification, ...).
  - Supervision et développement d'un service de PKI embarqué sur les produits.
  - Certification EAL2+ du produit et notamment des fonctions cryptographiques évaluées au niveau EAL4 avec une Qualification Standard de la DCSSI.
- Octobre 1999 - **Ingénieur R&D** : société **CERTPLUS (KEYNECTIS)** : <http://www.keynectis.com>,  
 Juin 2001 Opérateur de certification.  
 Poste : Développement d'un nouveau service, recouvrement de clefs cryptographiques en ligne sur des cartes à puces, dans le cadre d'un projet pour un grand compte.
- Depuis 1999 **Développement d'un produit de cryptographie :**  
*Produit commercial autorisé par la DCSSI*
  - calcul sur les grands nombres sur les corps de Galois  $GF(p)$  /  $p$  nombre premier
  - calcul sur les polynômes dans les corps de Galois  $GF(2^n)$
  - Partage de secret : Algorithme de Shamir
  - Compression avant chiffrement avec la librairie ZLIB
  - Algorithmes de génération de nombres pseudo aléatoire : FIPS186-2, ANSI X9.17 & Mersenne Twister.
  - Algorithmes asymétriques utilisant les courbes elliptiques (standard IEEE P1363-2000 et P1363a) : EC-DSA, EC-NR, ECIES, PSEC-3, ECSVP-DH, ECSVP-MQV
  - Algorithmes symétriques : AES (Rijndael), Mars, Serpent, Twofish, DES, Triple-DES, CAST5-128, BLOWFISH, RC2, RC4, RC5.
  - Fonctions de hash : MD5, SHA1(160,256,384,512bits), RIPEMD(128,160,256,320bits).
  - Fonction de MAC & HMAC : MAC-RIPEMD: 128 & 160 bits, HMAC-MD5(128 bits), HMAC-SHA1(160,256,384&512 bits), HMAC-RIPEMD(128,160,256&320 bits).

## EDUCATION

- Juin 1999 **Maîtrise en informatique** (Université des Sciences et Technologies de Lille)
  - Projet de développement de l'algorithme de Berlekamp (factorisation de polynômes).
  - Projet de développement de l'algorithme de signature Nyberg-Rueppel, utilisant les courbes elliptiques.
- Juin 1998 **Licence en informatique** (Faculté Jean-Perrin de Lens)
  - Projet de développement de l'algorithme LZW (compression de données).
  - Projet de développement des fonctions d'allocation mémoire (malloc,realloc,free,...)

### **Connaissances Informatiques :**

- Langages de programmation : C, C++, Java.
- Langages interprétés : Shell UNIX, PERL, HTML.
- Système d'exploitation : FreeBSD, MAC OS-X, Windows, Linux, Sun-Solaris.
- Cryptographie et sécurité :
  - o *Tokens cryptographiques* : smartcard, USB token, cartes accélératrices SSL, Hardware Security Modules, ...
  - o *Protocoles et standards* : PKCS, X509, SSL, IEEE P1363-2000, ANSI X9, PKI, SRP, RFCs relatives à la cryptographie, ...
  - o *Divers*: très bonne connaissance d'OpenSSL et des algorithmes cryptographiques : symétrique, asymétrique, fonction de hash, authentification, ...

### **Activités professionnelles :**

- Conférences sur le protocole SRP, les PKI, les VPN.
- Article sur le protocole SRP pour le magazine MISC, numéro 15 (Septembre/Octobre 2004)
- Article sur les courbes elliptiques pour le magazine MISC, numéro 19 (Mai/Juin 2005)
- Interview dans le magazine MAG-SECURS, numéro 21 (Octobre/Décembre 2008)
- Lancement d'un produit d'échange de fichiers sécurisés (Octobre 2008)

### **Langue étrangère :**

Anglais : lu, parlé, écrit

### **DIVERS**

Permis de conduire, voiture personnelle.

Sports: Jogging, Handball, Badminton, Echec (classement international).

Hobbies: Bricolage, randonnée, lecture de magazines économiques et scientifiques, cinéma, philatélie.