

Ludovic FLAMENT

13, Rue ZEFFE

62160 AIX-NOULETTE, FRANCE

Email : 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, 2 enfants



Expert Cryptographie, PKI, Critères Communs - Fondateur

EXPERIENCES PROFESSIONNELLES

Janvier 2019 -	Consultant CSPN (Cryptograph'IC) <ul style="list-style-type: none">Assistance dans la rédaction d'une cible de sécurité et des fournitures cryptographiques dans le cadre d'une Certification de Sécurité de Premier Niveau d'un produit pour un éditeur de firewall.
Juillet 2018 – Février 2019	Consultant CSPN (Cryptograph'IC) <ul style="list-style-type: none">Assistance dans la rédaction des fournitures cryptographiques dans le cadre d'une Certification de Sécurité de Premier Niveau d'un produit pour un éditeur de firewall.
Novembre 2018 -	Consultant Critères Communs (Cryptograph'IC) <ul style="list-style-type: none">Chef de projet sur la certification CC pour un produit de type client VPNRédaction des fournitures techniques (spécifications fonctionnelles spécifications détaillées, architecture)Assistance dans la rédaction de la cible de sécurité
Janvier 2017 -	Consultant PKI (Cryptograph'IC) <ul style="list-style-type: none">Projet de migration de la PKI en place. POC, rédaction de documents techniques (DAT, Dossier d'installation, Dossier d'exploitation, ...) et organisationnels (Politique de Certification, Déclaration des Pratiques de Certification, Cérémonie des clés, ...)Gestion des HSMDématérialisation des procédures de demandes de certificatsExpertise technique pour les projets nécessitant des certificatsSupport N3
Septembre 2016	Consultant CSPN (Cryptograph'IC) <ul style="list-style-type: none">Assistance dans la rédaction d'une cible de sécurité dans le cadre d'une Certification de Sécurité de Premier Niveau d'un produit pour un éditeur de sondes.
Mars 2016 – Juillet 2016	Consultant cryptographie (Cryptograph'IC / WolfSSL) <ul style="list-style-type: none">Développement de nouvelles fonctions cryptographiques (mécanisme de BIO compatible avec OpenSSL, support HSM via PKCS#11 pour RSA)
Décembre 2015 – Février 2016	Consultant cryptographie / PKI (Cryptograph'IC) <ul style="list-style-type: none">Développement d'un outil permettant de gérer une PKI utilisant un HSM pour la sécurisation des clésDéveloppement de bibliothèques dynamiques permettant la signature de code et de tickets pour une solution de SSO (clés dans un HSM dans les deux cas)
Mai 2015 – Novembre 2015	Consultant cryptographie (Cryptograph'IC / WolfSSL) <ul style="list-style-type: none">Développement de nouvelles fonctions cryptographiques (ex : extensions X.509, ALPN, IDEA ...) et/ou intégration dans des solutions existantes (ex : OpenSSH) de la bibliothèque cryptographique WolfSSL (connue également sous le nom CyaSSL)
Janvier 2015	Consultant Critères Communs (Cryptograph'IC) <ul style="list-style-type: none">Etude de faisabilité d'une certification CC pour un produit de déploiement de configuration de produits réseaux. Etude de l'existant, interviews des salariés, mise en avant des points bloquant, des améliorations à apporter : documentations techniques et organisationnelles, sécurité physique et logiques, ...
Novembre 2014 – Juin 2015	Consultant cryptographie (Cryptograph'IC) <ul style="list-style-type: none">Consultant sur les composants PKI et driver de carte à puce d'un produit de Card Management SystemChef de projet sur le développement d'un mini driver Microsoft

Juillet 2014 – Novembre 2014	Consultant cryptographie (Cryptograph'IC / Energy ICT) <ul style="list-style-type: none"> • Développement d'un Java CSP qui délègue certaines opérations cryptographiques à un élément sécurisé (chip) intégré sur un data concentrator, utilisé pour recueillir des données en toute sécurité à partir d'un grand nombre de compteurs intelligents (ERDF Linky par exemple) • La connexion entre le Java CSP et l'élément sécurisé se fait par l'intermédiaire d'une librairie PKCS#11.
Janvier 2014 – Mars 2014	Consultant cryptographie (Cryptograph'IC / Ingenico) <ul style="list-style-type: none"> • Etude des mécanismes de Tokenization. Réalisation d'une étude comparative des solutions existantes, proposition d'une architecture dans le cadre d'un développement interne.
Novembre 2013 – Janvier 2014	Consultant Critères Communs (Cryptograph'IC / Morpho) <ul style="list-style-type: none"> • Rédaction d'une cible de sécurité dans le cadre d'une certification Critères Communs pour le produit d'un industriel majeur du domaine des cartes à puce
Octobre 2013 – Novembre 2013	Consultant CSPN (Cryptograph'IC) <ul style="list-style-type: none"> • Rédaction d'une cible de sécurité dans le cadre d'une Certification de Sécurité de Premier Niveau d'un produit pour un éditeur d'antivirus
Juillet 2013 – Octobre 2013	Consultant cryptographie/PKI (Cryptograph'IC / GMX) <ul style="list-style-type: none"> • Conception et développement d'un service d'émission de certificats X.509 pour des terminaux de paiement. • Service architecturé sur une PKI interne avec support d'un HSM.
Novembre 2012 – Juin 2013	Consultant prototype cryptographique (Cryptograph'IC / PMU) <ul style="list-style-type: none"> • Conception d'une solution permettant la sécurisation de transactions entre des terminaux et un système central • Développement d'une librairie cryptographique intégrant les fonctions • Réalisation d'un prototype en vue d'une industrialisation
Mars 2012 – Juin 2014	Consultant Critères Communs (Cryptograph'IC / NETASQ) Dans le cadre d'une double évaluation aux Critères Communs (EAL3+ / QS) et EAL4+ d'un produit de sécurité, les tâches suivantes sont réalisées <ul style="list-style-type: none"> • Gestion du projet • Rédaction et pilotage de la rédaction des documents techniques • Relation et pilotage des travaux avec le CESTI et l'ANSSI.
Juin 2011 – Décembre 2012	Consultant Critères Communs (Cryptograph'IC / Cryptolog) Dans le cadre d'une assistance pour une évaluation aux Critères Communs (EAL3+ / QS) d'un produit de sécurité, les tâches suivantes sont réalisées <ul style="list-style-type: none"> • Gestion du projet • Aide à rédaction des documents techniques • Relation avec le CESTI et l'ANSSI.
Mars 2011 – Mars 2012	Consultant développement API cryptographique (Cryptograph'IC / ING Banque) <ul style="list-style-type: none"> • 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)
Décembre 2010 - Janvier 2011	Expertise cryptographique d'un logiciel (Cryptograph'IC / Orange) : <ul style="list-style-type: none"> • 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 (Cryptograph'IC / ING Banque) <ul style="list-style-type: none"> • 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)

<p>Avril 2010 - Août 2011</p>	<p>Consultant Critères Communs (Cryptograph'IC / ARKOON) Dans le cadre d'une assistance pour une évaluation aux Critères Communs (EAL3+ / QS) d'un produit de sécurité, les tâches suivantes sont réalisées</p> <ul style="list-style-type: none"> • Gestion du projet • Relation avec le CESTI et l'ANSSI. • Pilotage de la rédaction de documents techniques
<p>Novembre 2008 - Décembre 2009</p>	<p>Consultant Critères Communs / Expert en cryptographie / Responsable d'équipe (Cryptograph'IC / NETASQ) :</p> <ul style="list-style-type: none"> • 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.
<p>Avril 2008 – Novembre 2008</p>	<p>Consultant Critères Communs (Cryptograph'IC / 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 :</p> <ul style="list-style-type: none"> • 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.
<p>Février 2008</p>	<p>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.</p>
<p>Juin 2007 - Février 2008</p>	<p>Consultant en cryptographie (SONY NSCE) Mission de réalisation d'une démonstration technologique utilisant les DRMs Marlin dans le cadre de vidéo à la demande.</p>
<p>Juin 2001 - Juin 2007</p>	<p>Responsable d'équipe, Expert en cryptographie (NETASQ) <u>Poste (Février 2006 – Juin 2007) :</u> Project manager</p> <ul style="list-style-type: none"> • Responsable d'une équipe de 4 ingénieurs • Supervision des projets • Reporting à la direction <p><u>Poste (Juin 2001 – Janvier 2006) :</u> Expert en cryptographie et PKI</p> <ul style="list-style-type: none"> • 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.
<p>Octobre 1999 - Juin 2001</p>	<p>Ingénieur R&D (CERTPLUS / KEYNECTIS)</p> <ul style="list-style-type: none"> • 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	<p>Développement d'un produit de cryptographie : <i>Produit commercial autorisé par la DCSSI</i></p> <ul style="list-style-type: none"> - 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: Fitness, Running, Handball, Badminton, Echecs (classement international).
Hobbies: Photographie, bricolage, randonnée, économie, sciences.