Ludovic FLAMENT
Home/Professional address: 13, Rue ZEFFE
62160 AIX-NOULETTE, FRANCE
Email: ludovic.flament@cryptograph-ic.com
Web site: http://www.cryptograph-ic.com
Phone number: +33 (0) 610 514 811

Date of birth: 6th February 1974
Married, two children

Cryptography, PKI, Common Criteria Expert - Owner

PROFESSIONAL BACKGROUND

January 2019 -	**Consultant CSPN (Cryptograph'IC)** • Helping to write Security Target and cryptographic specifications for a firewall editor for a First Level Security Certification (French CSPN)
July 2018 – February 2019	**Consultant CSPN (Cryptograph'IC)** • Helping to write Security Target and cryptographic specifications for a firewall editor for a First Level Security Certification (French CSPN)
November 2018 -	**Consultant Common Criteria evaluation (Cryptograph'IC)** • Project Manager for a VPN client certification • Writing technical documents (Functional, Detailed and Architecture specifications)
January 2017 -	**Consultant PKI (Cryptograph'IC)** • Migration of existing PKI, writing technical (architecture, installation, exploitation …) and organizational documents (Certificate Policy, Certification Practice Statement, Key Ceremony …) • Management of HSM • Dematerialization of certificate request process • Technical expertise for project using certificates • L3 Support
September 2016	**Consultant CSPN (Cryptograph'IC)** • Helping to write Security Target for a network probe editor for a First Level Security Certification (French CSPN)
March 2016 – July 2016	**Consultant cryptography (Cryptograph'IC / WolfSSL)** • Development of new cryptographic functions in wolfSSL cryptographic library: OpenSSL BIO like support, HSM support through PKCS#11.
December 2015 – February 2016	**Consultant cryptography (Cryptograph'IC / Technicolor)** • Development of tool that manage PKI using HSM to secure the keys • Development of cryptographic libraries for code signing and tickets for an SSO solution. Also using HSM to secure keys.
May 2015 – November 2015	**Consultant cryptography (Cryptograph'IC / WolfSSL)** • Development of new cryptographic functions (X.509 extensions, ALPN, IDEA…) and integration in existing tools (OpenSSH) of wolfSSL (formerly CyaSSL) cryptographic library.
November 2014 – June 2015	**Consultant cryptography / PKI (Cryptograph'IC / French Imprimerie Nationale):** • Consultant for a Card Management System on the PKI and Smartcard driver component • Project Manager for a Microsoft mini driver component
July 2014 – November 2014	**Consultant cryptography (Cryptograph'IC / Energy ICT)** • Development of a Java CSP, which delegates some cryptographic operations to a Secure Element Chip integrated on a Data Concentrator product, used to collects data securely from a large number of Smart Meters. • The connection between Java CSP and Secure Element is done by the integration of a PKCS#11 library.
January 2014 – March 2014	**Consultant cryptography (Cryptograph'IC / Ingenico)** • Study on the development of a new service for an editor of security products
November 2013 – January 2014	**Consultant Common Criteria evaluation (Cryptograph'IC / Morpho)** • Writing Security Target of a Smartcard for Common Criteria evaluation

October 2013 **Consultant CSPN (Cryptograph'IC)**

- Writing Security Target for an Antivirus editor for a First Level Security Certification (French CSPN)

July 2013 – October 2013 **Consultant cryptography/PKI (Cryptograph'IC / GMX)**

- Design, development of service that deliver X.509 certificate for payment device
- Service architecture is on client/server model with support of HSM

November 2012 – June 2013 **Consultant cryptographic prototype (Cryptograph'IC / PMU)**

- Design, development of cryptographic API to secure the communications between end-user and central service
- Development of a prototype for industrialization

March 2012 – June 2014 **Consultant for accompaniment on Common Criteria evaluation (Cryptograph'IC / NETASQ)**

During an accompaniment for Common Criteria evaluation of a security product at level EAL3+/QS and EAL4+, these tasks will be accomplished:

- Project management
- Writing and Supervising the writing of technical documents
- Relation and supervision of work done by CC Testing Labs
- Relation with ANSSI (French government)

June 2011 - December 2012 **Consultant for accompaniment on Common Criteria evaluation (Cryptograph'IC / Cryptolog)**

During an accompaniment for Common Criteria evaluation of a security product at level EAL3+/QS, these tasks will be accomplished:

- Project management
- Writing and Supervising the writing of technical documents
- Relation with CC Testing Labs and ANSSI (French government)

March 2011 - March 2012 **Consultant cryptographic API developer (Cryptograph'IC / ING Bank)**

- Design, development of cryptographic API
- Encryption and signature with Hardware Security Module (with PKCS#11)
- Client/Server version for no cryptographic capable OS like mainframe.

December 2010 - January 2011 **Cryptographic expertise of a software (Cryptograph'IC / Orange)**

- Analyze source code
- Test compliancy of algorithms with standard
- Search and test attacks

January 2010 - December 2010 **Consultant cryptographic API developer (Cryptograph'IC / ING Bank)**

- Design, development of cryptographic API
- Encryption and signature with Hardware Security Module (with PKCS#11)
- Client/Server version for no cryptographic capable OS like mainframe.

April 2010 - August 2011 **Consultant for accompaniment on Common Criteria evaluation (Cryptograph'IC / ARKOON)**

During an accompaniment for Common Criteria evaluation of a security product at level EAL3+/QS, there tasks were accomplished:

- Project management
- Supervising the writing of technical documents
- Relation with CC Testing Labs and ANSSI (French government)

November 2008 - December 2009 **Consultant for accompaniment on Common Criteria evaluation / Cryptographic Expert / Team Leader (Cryptograph'IC / NETASQ)**

- Writing and Supervising the writing of technical documents
- Relation with CC Testing Labs and DCSSI (French government)
- Leader of 6 engineers
- Supervision of projects (firmware release)
- Report to direction
- Manage and develop cryptographic evolution of products. This concern services for end user (VPN-SSL, authentication, …) and products itself security (license, update, communication protocol, …).

April 2008 – October 2008 **Consultant for accompaniment on Common Criteria evaluation (Cryptograph'IC / NETASQ)**

During an accompaniment for Common Criteria evaluation of a security product (Level EAL3+/QS and EAL4+), there tasks were accomplished:

- Help for definition of perimeter
- Writing of Security Target
- Writing technical documents
- Supervision technical documents writing
- Relation with CC Testing Labs and DCSSI (French government)

February 2008 **Cryptographie Ingénierie & Conseil (Cryptograph'IC)**

WebSite : http://www.cryptograph-ic.com

Founder and CEO of an independent company specialized on cryptography and PKI services professional. This company will mainly deliver expertise, development, architecture, protocol design, ... for company that will be use cryptography and PKI.

From June 2007 to February 2008 **Cryptographic Consultant: *SONY NSCE company***

Working on Marlin DRM technology for TV products and mainly developed a technological demonstration product.

From June 2001 to June 2007 **Project manager, Cryptographic Engineer**: ***NETASQ company***, French unified security appliances manufacturer (http://www.netasq.com).

Position (from February 2006 to present): Project manager

- Management of engineer team (4 people)
- Supervision of projects (firmware release)
- Report to direction

Position: Cryptography and PKI expert

- Manage and develop cryptographic evolution of products. This concern services for end user (VPN-SSL, authentication, …) and products itself security (license, update, communication protocol, …).
- Manage and develop PKI service
- Participate on the Common Criteria evaluation

From October 1999 to June 2001 **Research and development Engineer**: ***CERTPLUS company*** (renamed Keynectis: http://www.keynectis.com), French certification operator.

Position: development of new service (mainly a key recovery mechanism with smartcard support) for the PKI platform of company

From 1999 to present **Freelance developer of cryptographic library:**

Authorized by the French government for commercial purposes

- Big number computing on Galois Field *GF (p) / p prime*
- Polynomial computing on Galois Field *GF (2^n)*
- Secret sharing: Shamir algorithm.
- Compression before ciphering with ZLIB library.
- Pseudo Random Number Generation: algorithm FIPS186-2, ANSI X9.17 & Mersenne Twister.
- Asymmetric algorithm that use Elliptic Curve (standard IEEE P1363-2000 et P1363a):
  - Signature: EC-DSA & EC-NR
  - Key exchange: ECIES & PSEC-3
  - Authentication: ECSVP-DH & ECSVP-MQV
- Symmetric algorithm:
  - AES (Rijndael), Mars, Serpent, Twofish
  - DES, Triple-DES, CAST5-128, BLOWFISH, RC2, RC4, RC5.
- Hash functions:
  - SHA1: 160, 256, 384 & 512 bits
  - RIPEMD: 128, 160, 256 & 320 bits.
- MAC & HMAC functions:
  - MAC-RIPEMD: 128 & 160 bits.
  - HMAC-SHA1: 160, 256, 384 & 512 bits
  - HMAC-RIPEMD: 128, 160, 256 & 320 bits.

EDUCATIONAL BACKGROUND

June 1999 **Master's Degree in computer science** (University for Science and Technology of Lille - FRANCE)

- Software for polynomials factorization, Berlekamp algorithm.
- Software for digital signature, Nyberg-Rueppel elliptic curve algorithm.

June 1998 **Degree in computer science** (Jean-Perrin Faculty, Lens - FRANCE)

- Software for compression of data, LZW algorithm.
- Software for memory allocation, reallocation, free, …

Computer Science:

- Programming language: **C**, **C++**, **Java.**
- Interpreted language: **Shell UNIX, PERL**, **HTML**.
- Operating system: **FreeBSD, MAC OS-X, Windows, Linux, Sun-Solaris.**
- Cryptography and security:
    - *Cryptographic token:* **smartcard, USB token, SSL accelerators card, Hardware Security Modules, …**
    - *Standards and Protocols:* **PKCS, X509, SSL, IEEE P1363-2000, ANSI X9, PKI, SRP, RFC on cryptographic algorithms, …**
    - *Miscellaneous:* **very good knowledge of OpenSSL and cryptographic algorithms: symmetric, asymmetric, hash function, authentication, …**

Professional activities:

- Conference on SRP protocol, PKI, VPN during meeting/show on security area.
- Article on SRP protocol for the French MISC magazine number 15 (September/October 2004)
- Article on elliptic curve for the French MISC magazine number 19 (May/June 2005)
- Interview on the French magazine MAG-SECURS, number 21 (October/December 2008)
- Commercialization of Secure File Exchange tools (October 2008)

Foreign Languages:

- Fluent in French (mother tongue)
- Working knowledge of English

OTHER ACTIVITIES

Driving license, Personal car
Sports: Fitness, Running, Handball, Badminton, Chess (International ELO), Walk in nature
Hobbies: Photography, Sciences, Economy, antiquities search.