IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 1, January 2011
ISSN (Online): 1694-0814
www.IJCSI.org

A user-centric PKI based-protocol to manage FC² digital identities

Samia Bouzefrane[1], Khaled Garri[1] and Pascal Thoniel[2]

[1] CEDRIC Laboratory, Conservatoire National des Arts et Métiers
292 rue Saint Martin, 75141, Paris Cédex 03, France

[2] NTX Research
111 avenue Victor Hugo, 75116 Paris - France

Abstract

The proliferation of e-services (e.g. e-commerce, e-health, e-government) within the emerging digital Identity Management Systems make Internet an undeniable convenient and powerful tool for users. However in this environment, users are required to manage several digital identities and a great number of personal data. As such, simplification of users' involvement is highly needed while increasing the users' confidence, and guaranteeing security. This paper proposes a low-cost authentication solution which leads to a reduction of users' identities, even across several circles of trust, while maintaining high-level security. This solution is suitable for FC², a platform dedicated to manage digital identities within circles of trust.

Key words: *Identity management system, public key infrastructure, federated identity, circle of trust, digital identity, security.*

1. Introduction

With a boom in online services generally accessed through a lot of login-password couples, Internet users are having an ever increasing number of digital identities.

Indeed, Internet was not originally designed with the digital identity idea and, some solutions have been proposed to deploy digital-identity management architectures using existing standards and protocols such as InfoCard standard that is a user-centric approach or Liberty Alliance standard that is based on the notion of identity federation.

A typical identity-management architecture requires basic components like an identity provider (IDP) that authenticates the user in a secure manner allowing him to access to a service provider (SP) and an attribute provider (AP) to supply the user attributes to any authorized agent while not compromising privacy.

FC² (Federation of Circles of Trust) [1] is a French project initiated by several companies jointly with government and academic actors. It takes into account the following points: the user must have control on his personal data, a great number of certificates must be provided at low cost, multiple services may belong to distinct groups and accessible via various material supports like usb key, smart card or a mobile equipment. FC² tries to bring a solution to these requirements by implementing a comprehensive platform that allows new secure electronic services based on a transparent and interoperable federated identity management.

In this context, a new PKI[1]-based protocol, called "2.0", has been proposed to guarantee secure access to electronic services at low cost.

Based on three levels, FC² project integrates:

- An international PKI that delivers and manages server certificates for identity providers, service providers and attribute providers.
- An internal PKI deployed by each registration authority (associated to each circle of trust) for all its agencies.
- A "user" PKI that addresses final users.

Our contribution, in this paper, concerns the "user" PKI that integrates an entity called "electronic notary" used instead of a certification authority, allowing the registration of new users (citizen/consumer/professional) within a registration authority that may be a proximity agency (telecom agency, banking agency) viewed as a trust third party. The proposed crypto-system is based on the same principle whatever asymmetric algorithm is used. The local registration authority delivers a "public key certificate" to the user along with a private key using his usb key, his smart card or his cell phone. The local

[1] Public Key Infrastructure

registration authority uploads user's "public key ownership certificate" to its central electronic notary server through a secure channel. Thus, anyone, any IDP, any application and any process can request this electronic notary server to authenticate the digital identity of the user. This trusted user is now able to access, at any time services belonging to distinct circles of trust, federated by FC² system in a transparent manner.

The topic of trust and PKI management has been addressed during the last few years like in [7], [8], [9], [10]. For example, John Linn in [7] presents and compares several trust models and applied for use with public-key certificate infrastructures based on the X.509 specification, including subordinated hierarchies, cross-certified CA, hybrid CA, bridge CAs, and trust lists. More recent works deal with identity management systems and focus on the use of PKI within a federated architecture like in Liberty Alliance [11]. Another work on Liberty Alliance targeted a pan-European multi Circle of Trust environment [12].

On the other hand, Windows CardSpace delivered with recent versions of .NET Framework manages identities according to a user-centric approach [13]. A more sophisticated work introduces a formal semantics based calculus of trust that explicitly represents trust and quantifies the risk associated with trust in PKI and identity management [14]. However, all these research works targeted a particular identity management system. Since CardSpace and Liberty Alliance are not interoperable, Jorstad et al. in [15] tried to integrate the current SIM authentication used in GSM with both Liberty Alliance and CardSpace such that it can be used for Internet services. Unfortunately this work is limited to mobile equipments and is not used with other physical supports.

The PKI-based approach proposed in this paper allows managing different circles of trust defined in FC² project while each circle may adopt any identity management system independently from the system used by other circles of trust. Moreover, with our solution the user may access to FC² services after registration and authentication phase thanks to any physical support (smart card, USB key, cell phone, etc.) he has.

In the rest of this paper, Section 2 recalls the objective of FC² platform. Section 3 describes the user-centric PKI-based approach that is proposed to access electronic services of different circles of trust while guaranteeing security at low cost. Section 4 details the way keys and certificates are generated and used. Section 5 explains the role of each involved actor through distinct use cases. Section 6 outlines the implemented software architecture, before concluding in Section 7.

2. The FC² project

The FC² project (see Figure 1) is a French R&D cross-sector initiative including companies, government and academic actors.

The project started on July 2007 and ended on June 2010. It aimed to:

- Define and implement interoperable identity federation architecture schemes, fully agnostic versus underlying technologies (Liberty Alliance [2], Microsoft/Cardspace [3], Higgins [4], Open-ID [5], etc.),
- Implement a dedicated infrastructure for service providers enrolment and support,
- Provide strong authentication and privacy management services,
- Provide a high level of protection against digital identity attacks,
- Provide a simple and convenient user experience, targeting user empowerment and trust as well as universality of use across a large variety of end-user devices,
- Create innovative business models, acceptable and/or adoptable by all players in the value chain,
- Provide the needed technologies and processes to master identity management technologies on a large scale basis, from national/government level to corporate/enterprise level.

The R&D developments within the project targeted especially the problems of Federated Identities in a cross-sector environment, encompassing the e-government, local administrations, telecommunications and financial domains.

Regarding the FC² issues, the interoperability of various identity-management technologies and the user privacy have been addressed through research works undertaken by FC² partners, like in [5] and [6].

In this paper, we focus on the access to on-line services within a federated identity platform while allowing secure, low-cost, and user-centric properties.

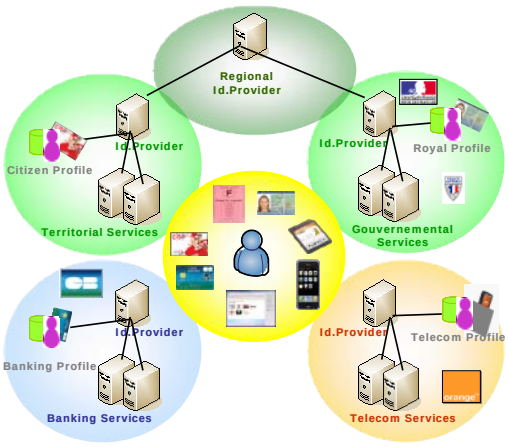

Fig.1. FC² architecture

3. PKI 2.0

3.1 The FC² context

As for any PKI, the main objective is naturally to ensure data exchange confidentiality, integrity and authenticity along with strong authentication of the actors. The non-functional objectives are the fact of allowing the materialization of trust within FC² framework, between distinct circles of trust and the user. It was decided in FC² project, not to impose higher certification authority nor hierarchy between the circles of trust, but to provide a security solution that may be collaborative between the actors, and that may be evolutionary, flexible for the integration of new partners (circles). The PKI-based solution that is deployed uses three levels:

• *A bridge PKI*: to which is assigned a certificate that is auto-signed or delivered by a known *CA* which signs for a given circle of trust the certificate of the internal *CA*.

• *An international PKI*: to deliver the public certificates of identity providers and attribute providers when communicating with users or electronic notaries.

• *An internal PKI*: with a root certificate auto-signed and a certificate signed by the bridge *CA* certificate; this PKI signs the certificates of the identity and attribute providers for their inter-circle communication, and those of each registration authority and each electronic notary when communicating each other.

3.2 PKI 2.0 principle

Our contribution concerns a protocol called PKI 2.0 to register new users within the FC² platform. It consists of two parts. The enrolment phase involves the registration of new users and the generation of keys and certificates. The verification phase that assumes the publication of new public-key ownership certificates on an electronic server acting as a notary that checks the validity of the user certificates.

The first step concerns the Registration Authority (*RA*) that allows registering new users. The *RA* must have multiple proximity agencies distributed over the territory. In the real world, the *RA* and the proximity agencies are the following according to the circle of trust considered: In the governmental circle, the *RA* corresponds to “les Notaires de France” and the proximity agencies are notaries. In the banking circle, the *RA* is the bank and the proximity agencies are the banking agencies. In the telecom circle, the *RA* is the telecom operator and the proximity agencies are the local telecom agencies.

RA has the role of checking the identity of the user, and of executing a dedicated procedure to deliver finally an auto-signed public-key certificate and a "public-key ownership certificate". In such model, the cost is low since that certification authorities are not necessary.

In our solution, the user holds his key pair and his certificates (certificate of public-key and certificate of public-key ownership) generated by the proximity agency called the Local Registration Agency (*LRA*). The certificate of public-key ownership published by a *LRA* on the Electronic Notary (*EN*) server is used to check the validity of the auto-signed certificate of public key. To distinguish them from the certificates generated by a server, they are called “customer” certificates. The user can use his certificates for encryption, authentication or signature.

This protocol avoids the use of a certification authority to the benefit of the *EN* server. No certificate from registration authority is necessary since the user certificate is auto-signed. However, the *LRA* checks the certificate generation and insures the secured publication of the corresponding ownership certificate on the *EN* server. The auto-signature of a certificate does not bring any guarantee on its validity, it only insures to be in compliance with the standard X509v3 so as to be used by existing applications. In fact, the certificate validity is obtained on-line by requesting the *EN* server.

4. PKI 2.0 keys and certificates

In this section, we explain how keys and certificates are generated, and how the enrolment is performed.

4.1 Key-pair generation

To have a PKI 2.0 certificate, each user must have a pair of keys. The key generation can be done according to different ways:

- personal way: the user runs locally a software tool provided by FC². This software corresponds to an identity selector installed on his machine or his cell phone.
- decentralized way: the user goes physically to a Local Registration Agency that generates keys for him.
- centralized way (not recommended): a *RA* - one by circle of trust - generates the keys for each person.

At this stage, the user has two keys: a public key K_{pub} and a private key K_{priv}.

4.2 Certificates Generation

The PKI 2.0 recommends for each user two pairs of keys, one pair is dedicated for self authentication and electronic signature and the other pair for encryption. These pairs of keys have to be stored in secure way, especially for the private keys.

The public-key certificates X509v3 are auto-signed and stored in plain text. The first one is an authentication/signature certificate whose legal value rises from European directive 1999/93. The second one is dedicated to encryption.

The generation of certificates can be also carried out according to a personal, centralized or decentralized way. However, the decentralized procedure is the optimal way since it allows the generation of a public-key certificate and a public-key ownership certificate that guarantees the authenticity of the latter. These certificates are added to the information system for the first time during the enrolment phase.

4.3 Enrolment operation

The user enrolment process is done directly within a Local Registration Agency (*LRA*) according to three steps:

- *First step: checking user identity*

The user presents one or more identity documents to the registration agent that physically authenticates user. This face-to-face step is easy to realize within FC² project thanks to the LRA that are distributed over the territory.

- *Second step: Generating public-key certificate*

Once the user identity is checked, the registration agent launches the public-key certificate generation after having generated the corresponding key pair. This certificate contains: third party nationality (FR), third party type (registration agency), third party circle of trust, time-stamping (validity period of the certificate), user identity, public key, auto-signature (with the user private key). Once the certificate is generated, the registration agent must register it on the user physical device (USB key, smart card or cell phone).

- *Third step: Generating certificate of public-key ownership*

PKI 2.0 principle is that the consumer/citizen is responsible for certifying the ownership of his public key without involving any certification authority. For this purpose, PKI 2.0 adds a new certificate, called "public-key ownership certificate". This certificate does not contain the user public key. Instead, it contains the hash value of the public key (by using a hash function like MD5, SHA-1 or RIPE-MD). Hence, a certificate of public-key ownership contains: nationality of the third party (FR), type of the third party (registration agent), third party circle of trust, time-stamping, user identity, public key hash value. Once generated, this certificate is encrypted with the user private key.

The following section describes the different entities involved in the infrastructure.

5. Principal actors and use cases

PKI 2.0 gathers the following actors: *LRA*, *EN* servers, service providers, and finally users. The local agencies and servers of each circle of trust have an internal PKI which delivers the necessary certificates to establish a SSL communication. The electronic-notary servers have also certificates issued by a known certification authority for communication between them and users or service providers. Figure 2 illustrates the general architecture of the PKI 2.0 including the main actors and the interactions between them.

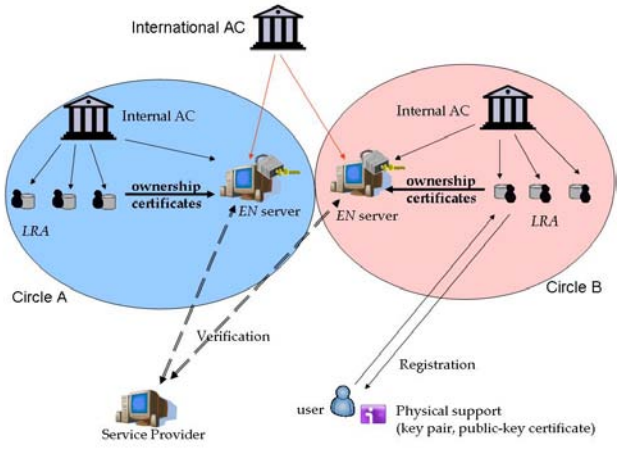

Fig.2. PKI 2.0 Architecture overview

4.4 Main actors

User entity

The user, as consumer or citizen, is linked to a circle of trust. First of all, he has to register himself within a *LRA* to access the system, it's the enrolment phase. Afterwards, he will be able to communicate with the system to manage his

own account (update, revoke or renew). Of course, he is also able to check any public-key certificates on any EN servers delivered by any RA of any circles of trust.

Local Registration Agency
This entity manages clients' enrolment by generating certificates and publishing and deleting of public-key ownership certificates onto the *EN* server.

Electronic Notary server
The *EN* server contains a register of ownership certificates. It is requested by other actors to authenticate the public-key certificates. Indeed, it stores the public-key ownership certificates published by *LRA*. The communication by a *EN* and a *LRA* is secured thanks to SSL certificates delivered by an internal PKI. *EN* server is requested to verify the users public-key certificates delivered by its own *LRAs*.

Service Providers
The service providers correspond to the web sites where users are identified using their public-key certificate. These providers ask *EN* to check the public-key certificates used by users to access the provided services.

Identity providers
The identity provider, one per circle of trust, stores public-key certificates of PKI 2.0 generated by *LRA*. The publication of these certificates is done automatically thanks to a software module integrated within the user identity selector.

5.1 Use Cases

New users enrolment
As stated before, this step is the first one allowing the user to access to FC² platform. It is performed by the user within a *LRA*. First of all, the user is authenticated by presenting an identity document. Once authenticated, several steps may be carried out in order to issue the public-key certificate, that is, to:
- register the user in a database which contains the list of users. The information stored in the data base are: Common Name, gender, date of birth, postal address and e-mail. These data items are inserted automatically into the certificates generated as in the following steps.
- generate the public-key certificate, that is auto-signed with the private key of the user.
- register the public-key certificate (in . *P12* and *.cer* formats) on the physical device of the user.
- generate the public-key ownership certificate under *.P12* format, and finally encrypt this certificate using the private key of the user.

Publication of public-key ownership certificate
The public-key ownership certificate allows checking the authenticity of the public key through the hash value of this latter that is inserted into the certificate. This certificate must be published onto the *EN* server. This is done thanks to SSL communication with the *NE* server. The SSL authentication is done mutually by using SSL certificates generated by the internal PKI. Once the mutual authentication is achieved successfully, a message is sent to *EN* with the following information:

$$\left\{Id_{LRA_i}, M, \{H(M)\}_{Kpriv_{LRA_i}}\right\}_{Kpub_{EN}}$$

Where Id_{LRAi} : is the identity of the *LRA i*,
M : the message contains the ownership certificate encrypted with the private key of the user, and other information like : serial number, version, signature algorithm.
H(M) : the hash value of *M*. All these information are encrypted with the public key of *EN*.
The use of the signature enables us to guarantee the message integrity. The encryption with the public key of *EN* guarantees confidentiality since that only the appropriate *EN* will decrypt the message. Upon receiving the message, the *EN* begins decrypting the message using its private key, and then checks the signature. For this purpose, the *EN* reads the identity of the sending *LRA* because it has a register of all the public-key certificates of his local agencies, indexed with their serial number. Then, *EN* begins extracting the certificate that contains the public key of the concerned *LRA*, in order to verify the signature. *EN* computes the hash value of *M* and compares it to the one received. If they are equal, *EN* stores the certificate of ownership in its database, otherwise an error message is notified to the *LRA*.

User account management
This task concerns the update, delete and read operations carried out on the user account. The update may concern the modification of some personal information or even the generation of a public-key certificate with the new information. The account deletion implies the deletion of the public-key ownership certificate within *EN*. In this case, the *LRA* sends the following message to inform *EN* about the revocation:

$$\left\{Id_{LRA_i}, M, \{H(M)\}_{Kpriv_{LRA_i}}\right\}_{Kpub_{EN}}$$

Where *M*={serial number of public-key certificate, removal}
The renewal of the public-key certificate is necessary after removal.

Public-key certificate verification

This operation allows user, identity provider, or service provider to check a public-key certificate in real time, in order to access an Internet service or to exchange data with another actor. The verification process is done as in the following:

- request a *EN* server whose the address is in the certificate using a SSL communication and authentication with the concerned *EN*
- the public-key certificate is sent to the already authenticated *EN*
- then *EN* extracts the serial number that is also the serial number of the public-key ownership certificate,
- *EN* looks at the public-key ownership certificate in its data base,
- if the public-key ownership certificate is found in the data base, *EN* tries to decrypt the public-key ownership certificate with the public-key extracted from the given/received public-key certificate,
- if the public-key ownership certificate has been successfully opened, *EN* extracts the hash value from the public-key ownership certificate, and compares it with the one computed with the public key contained in the received certificate. If they are equal, the verification is successful.

As described in the following section, an implementation of PKI 2.0 has been performed.

6. Software architecture

We implemented the PKI 2.0 by developing three modules: the first module proposes a tool for the *LRA*. It allows to manage user accounts and to control the publication of ownership certificates on the *EN* server. As an example, Figure 4 illustrates the case of adding a new user into a circle of trust. The second module is devoted to the *EN*, it is composed of two programs: one to answer the publishing requests from his Local Registration Agencies, and the other to answer the check requests from any service providers and any users. The third module is devoted to external customers (users, IDP and service providers) that want to check a public-key certificate of PKI 2.0 (see Figure 3).

7. Conclusion

Our PKI-based solution seems to be an answer to the FC² needs in terms of security. This proposal is a user-centric system that fulfills the requirements of a large number of users at low costs. Moreover, the PKI 2.0 solves the problem of managing multiple digital identities by allowing the use of only one or few identities within several circles of trust, by replacing Certification Authorities by Registration Authorities that have proximity agencies easily accessible to citizens/consumers.

As a perspective to our work, we aim to develop the module of checking as a plugin to Web browsers.

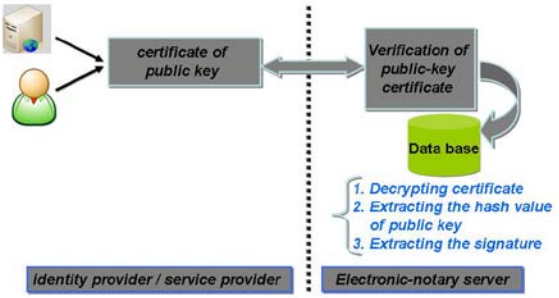

Fig.3. Checking a public-key certificate

Acknowledgments

This research is part of the project called FC2 (Federation of Circles of Trust -www.fc2consortium.org). Khaled Garri has been partly financially supported by the DGCIS (Direction Générale de la Compétitivité de l'Industrie et des Services). We are thankful to students Nesrine Jlidi, and Mohamed Mammeri, who contribute in the implementation of the software tools.

References

[1] Consortium, FC². Fédération de Cercles de Confiance et usages securisés de l'identité. http://www.fc2-consortium.org/.

[2]Liberty Alliance Project, Available: http://www.projectliberty.org/

[3] http://www.eclipse.org/higgins/

[4] http://openid.net/

[5] H.-B. Le et S. Bouzefrane "Identity management systems and interoperability in a heterogeneous environment", in **Int. Conf. on Advanced Technologies for Communications**, Hanoi, oct., pp. 243-246, IEEE, 2008.

[6] A. Davoux, J.-C. Defline, L. Francesconi, M. Laurent-Maknavicius, K. Bekara, R. Gola, J.-B. Lezoray, V. Etchebarne, "Federation of Circles of Trust and Secure Usage of Digital Identity", in **eChallenges e-2008**, Stockholm, Sweden, October 2008.

[7] J. Linn, "Trust Models and Management in Public-Key Infrastructures," RSA Laboratories, Tech. Rep., 2000. ftp://ftp.rsasecurity.com/pub/pdfs/PKIPaper.pdf

[8] M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized Trust Management," in Proceedings of the **1996 IEEE Symposium on Security and Privacy**, May 1996, pp. 164–173.

[9] U. Maurer, "Modeling a public-key infrastructure," in Proceedings of the **4th European Symposium on Research in Computer Security** (ESORICS 96), ser. Lecture Notes in Computer Science, vol. 1146, September 1996, pp. 325–350.

[10] Radia Perlman "An Overview of PKI Trust Models", **Journal of IEEE Networks**, Nov/Dec. 1999, pp. 38-43.
[11] Liberty Alliance Project, "Liberty Alliance Trust Models", draft version 1.0-14, 13 April 2003.
[12] Dao Van Tran, Pal Lokstad, Do Van Thanh, "Identity Federation in a Multi Circle-of-Trust Constellation", Report of Telektronikk 3/4.2007, pp. 103-118.
[13] Windows CardSpace "Geneva", http://connect.microsoft.com/site642/content/content.aspx?ContentID=10104
[14] Jingwei Huang, David Nicol, "A calculus of trust and its application to PKI and identity management", Proceedings of the **8th Symposium on Identity and Trust on the Internet**, 2009, Pages: 23-37.
[15] Ivar Jorstad, Do Van Thuan, Tore Jonvik & Do Van Thanh, "Bridging CardSpace and Liberty Alliance with SIM authentication", Pages: 12-25 , Proceedings of the **9th Symposium on Identity and Trust on the Internet**, 2010.

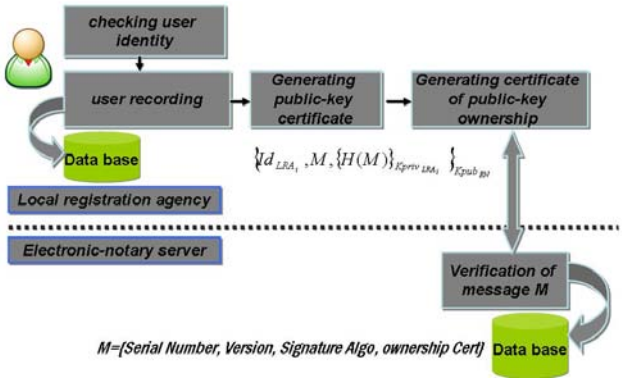

Fig.4. Adding a user in a circle of trust

Samia Bouzefrane is an associate professor at the CNAM (Conservatoire National des Arts et Métiers) in Paris. She received her Ph. D. in Computer Science in 1998 at the University of Poitiers (France). She joined the CEDRIC Laboratory of CNAM on September 2002 after 4 years at the University of Le Havre. After many research works on real-time systems, she is interested in smart objects. She took part in the MESURE project to evaluate the performance of Java Card platforms, which has received on September 2007 the Isabelle Attali Award from INRIA during "e-Smart" Conference. Furthermore, she is the author of two books: a French/English/Berber dictionary (1996) and a book on operating systems (2003). Currently, she is a member of the ACM-SIGOPS, France Chapter.

Pascal Thoniel holds a Master of Finance from IEP Paris (Sciences Po). After 10 years of experience in Business IT, Pascal has created NTX Research in 1997, a company specialized in Information Systems security. Pascal has 15 years of experience in IT Security : IT Security Audit and Policy designer, inventor XC Technology (strong authentication and confidentiality - patented), inventor of a new user-centric approach for PKI. NTX Research plays also an active role in the FC² project.

Khaled Garri is a PhD student from the SEMpIA team (embedded and mobile systems towards ambient intelligence) of the CNAM in Paris. He has a Master's degree. In addition to FC² project, he is working currently on embedded systems security.