Enabling Collaboration Between Heterogeneous Circles of Trust through Innovative Identity Solutions

Jean-Baptiste Lézoray, Marc Pasquet
Laboratoire GREYC: ENSICAEN – Université de Caen – CNRS
Marc.Pasquet@ensicaen.fr - Jean-Baptiste.Lézoray@greyc.ensicaen.fr

ABSTRACT

During the last years, the growth of e-commerce has been considerable due to the increase of user confidence in secure electronic payment. Many web services have been developed and some decided to establish links of confidence, also called circles of trust. A user that accesses a web service in a circle of trust can also access other web services of the circle without additional authentication. In that way, the web services offer is larger and clients' demands more satisfied. Circles of trust are naturally composed of web services from the same type of activity. In this article, we address the problem of federating heterogeneous circles of trust. The main objective is to develop new e-services based on the composition of heterogeneous services. For instance, an application can be the electronic registration of a child to a day-care center: parents will need documents from their bank (in order to pay), from the government (to prove its identity), and from other sources.
The preliminary results introduced here are issued from a French innovative research project called FC² that deals with the federation of heterogeneous circles of trust.

KEYWORDS: Single Sign On, Identity Management, OpenID, CardSpace, Higgins, Circles of Trust, Federation of Circles of Trust.

1. INTRODUCTION

In the early days of the Internet, there was no need of an identity layer. The main issue was not to be identified, but to build a decentralized network that could be operational even in case of a failure of some of the members. The identity topic was fully in charge of the application layer (FTP, RSH, SMTP). Nowadays there is still no native way to deal with identity, or even to prove it, except on the application layer. With WEB 2.0 concepts, the user is central to the architecture, and the problem is amplified. The lack of identity layer has also led to the rise of a concept of anonymity on the Internet, nowadays widely admitted as evidence [1]. On the other hand, there is also a high need of being identified: pseudonyms, avatars and social networks are now part of the common vocabulary on the Internet. The collapse of these two facts has led to a so-called identity crisis:

- The user deals with lots of accounts on different service providers,
- The user has a high temptation to use the same credentials on different services, with the lack of security it implies,
- The user has to manage the spread of his identities between multiple service providers.

To tackle that issue, a market of identity management has grown since the beginning of the XXI^{e} century, both on the standard side (Liberty Alliance, SAML, OpenID, InfoCard...) and on the implementation side (CardSpace, Higgins/Bandit, OpenSSO...).

These solutions handle the problem of user identification and authentication, but they are restricted to a perimeter delimited by the technologies interoperability. Indeed, there is no easy way to deploy a system acting with other heterogeneous deployments. Most of them define a "circle of trust" notion that delimits by definition a restricted perimeter of use. Therefore, these solutions still do not enable an easy cooperation outside of that perimeter.

Some current research projects are trying to solve that issue, with totally different approaches. The project FC² (Fédération de Cercles de Confiance) aims at studying solutions based on a "Federation of Circles of Trust". In order to enable collaboration, with respect to user privacy, new business models based on an identity management system shared between heterogeneous entities (banks, telecoms, authorities, industries,...) are developed. This paper is mainly based on the early results of the FC² project and presents some of the original solutions it provides.

2. MOTIVATIONS

On the Internet, an identity can be seen as a user account. An account on an identity provider basically consists in two concepts: a way to authenticate and data linked to the account. The latter data can generally be classified into two categories: data directly concerning the user (e.g. name, date of birth, phone number, credit card number...), and business specific data (e.g. the emails and the address book on a webmail provider). The value of both these types of data is obvious, but the authentication of users also has a considerable value. If an organization could share its data and authentication capabilities with any partners, it could improve the user experience and help defining new business models.

Such cooperation already exists. In the concept of circles of trust, accounts are located on a single Identity provider that provides service providers with identities they can use at their convenience. Service providers trust the identities issued by the identity provider, and by extension also trust the other service providers. The main drawback of that technique is that identities are somehow localized on a limited area: mainly on a single web site, at best involving a portal. For example, Google uses such a technology on websites of its portal (google, gmail, igoogle, youtube,...). The concept of circle of trust involves a trust between partners, a deep federation of all user accounts, and well-defined frontiers delimiting an homogeneous, limited and finite area for the identities.

If we consider a circle of trust as a limited and homogeneous area, could we make multiple and heterogeneous circles of trust able to communicate, through the concept of cooperation based on identity? The project FC² is investigating ways to build such new business models based on cooperation on the identity side, but without a single and centralized circle of trust.

3. STATE OF ART OF THE IDENTITY MANAGEMENT SOLUTIONS

In this Section, we present a state of art of the current major identity management solutions along with their advantages and drawbacks.

3.1. Identity Management Solutions

Microsoft passport was a centralized identity management system. By using the credentials Passport provides the users with, users were able to connect to any web sites that implemented the system. The system has received extensive criticism due to the fact that it was a fully centralized system, and that it allows Microsoft to have full access to user's data. Windows live ID later replaced passport.

In 2005, Microsoft introduced the concept of information cards (InfoCards in its abridged version) through CardSpace [2]. It is based on the seven laws of identity [3] proposed by Kim Cameron, who was originally a skeptic about Microsoft Passport. He joined Microsoft to implement a new solution that would learn from the previous strategic errors of Microsoft Passport. Information cards put the management of the identity back into the hands of the user. Information cards are a metaphor of business cards or credit cards. The user's set of InfoCard is stored on his local computer. Each card represents one of his digital identities, and contains a set of claims describing it (name, date of birth,…). There are three major entities in those specifications:

- The user, which central to the system,
- The STS (Security Token Service) issues information cards for users, and provides security tokens that prove the identity of the user on request, after authentication: it is an identity provider.
- The RP (Relying Party) is an identity consumer. It provides services to the user.

When a RP, which is generally a web site, needs the authentication of a user, it has to define the security policy it needs (such as protocols, authentication methods, claims and issuer…). Then, the RP sends a request to the identity selector. An identity selector is a piece of software installed on the user's computer, that stores information cards, and that makes the link between the RP and the STS, but under control of the final user (see Figure 1). The user chooses his identity by selecting one of his cards. The STS, after a verification of the user's identity (e.g. with a password), provides the RP an authentication token, including the required claims. InfoCards specifications are based on normalized web services protocols (WS-*). Specifications are public, so there are multiple implementations of identity selectors: CardSpace by Microsoft [2], DigitalMe by Novell [4], or the Higgins Identity selector [5].

Liberty Alliance has another approach. Liberty Alliance is a very complete set of standards dealing with account federation, single sign on, single log out and attributes sharing [6]. The organization, founded in 2001 by Sun Microsystems, is currently composed of several major companies such as America online, France Telecom, IBM, Novell, Sun, etc. A part of the project, ID-FF, was built on top of the SAML 1.0 language [7]. ID-FF specifications and SAML 1.0 have merged to form the

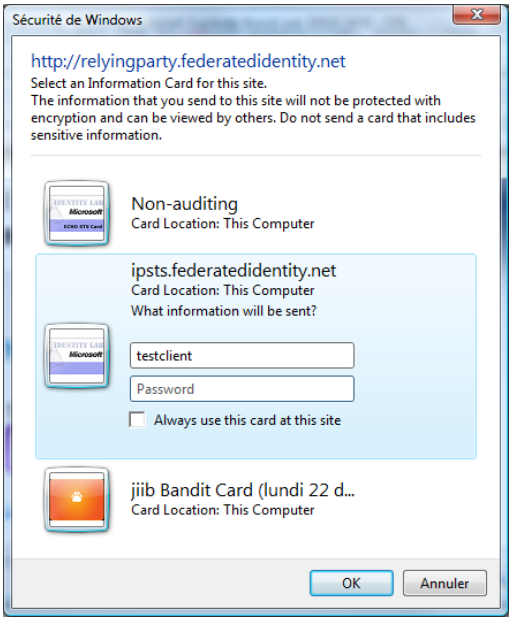

Figure 1. CardSpace is the Microsoft Implementation of the Identity Selector.

new SAML 2.0. The main elements of the architecture defined by the specification are the IDP (IDentity Provider), the SP (Service Provider), the DS (Discovery Service), and the AP (Attribute provider). A SP is a website that provides the user a service (a webmail for example). Specifications are based on profiles of use, such as "Artifact Resolution Profile", "Web Browser SSO Profile", or "Enabled Client or Proxy Profile". The most common profile is the "Web Browser SSO Profile": when a SP needs a user authentication, it redirects the user to the IDP (by an HTTP redirection) with an authentication request. The IDP then authenticates the user, and redirects him back to the SP. Then, the SP connects to the IDP to get the authentication response security token asserting if the user was successfully authenticated. A SP that needs attributes of a user has to ask the DS to get the addresses of the AP.

Finally, OpenID is an open, user-centered standard that enables single sign on and attribute sharing. The OpenID foundation [8] is a non-profit organization in charge of the specifications and of the coordination of the efforts of the community. With OpenID, a user creates an account on an OpenID provider (which is the identity provider), and is attributed an OpenID identifier. An OpenID identifier is a personalized URL referencing an account (e.g. http://openid.orange.fr/lezorayjb is the OpenID for the user "lezorayjb" on the Orange OpenID provider). The user can then use that URL to log in into OpenID enabled websites (service provider). The service provider redirects the user to the OpenID provider, which authenticates the user, and redirects him back to the service provider.

3.2. Interoperability

There are technical solutions to make these technologies interoperable. This Section explores some of them.

OpenID and InfoCard are basically interoperable, as OpenID does not specify any authentication method, whereas InfoCard is one. For example, the web site www.signon.com provides an OpenID whose authentication method is either a basic login-password, or an InfoCard. InfoCard attributes are somehow forwarded by the OpenID provider.

Alrodhan and Mitchell [9] propose a solution for interoperability between InfoCards and Liberty, based on the Liberty LEC profile (Liberty Enabled Client profile). The LEC profile, which is the basis of the SAML 2.0 "Enhanced Client or Proxy Profile", enables a client (browser or other) to have an active role in the authentication process. Their proposal is based on the fact that InfoCard and the liberty LEC profile describe very similar interactions and behaviors. A modified InfoCard Identity selector can translate messages between the InfoCard and Liberty standards, in order to gain access to the Liberty world.

The Higgins project [5] was started in 2005 on the basis of an initial work introduced on 2003, and is since supported by Novell and IBM. It provides a set of open source tools such as an identity layer on top of multiple existing protocols, for integrating identity, profiles, and information sharing.

Each of these technologies has reached a high level of requirements. Some technical solutions enable interoperability, but there is still no solution to provide a universal interoperability between the different technologies.

3.3. Comparative Study

Figure 2 presents a comparison of the identity solutions. By definition, the concept of circle of trust is quite natural in the Liberty Alliance architecture, as the central IDP has to be aware of which SP it trusts. It is an opposite view to the information card and OpenID architectures, where the RP (resp. SP) defines which STS (resp. IDP) it trusts.

However, architectures involving InfoCards or OpenID are still very close to the concept of a circle of trust, for two reasons. First, an identity provider can define a security policy with a strict limitation on the usability of the identities it issues. This may limit the use of identities to trusted (or at least verified) RP, and reject untrusted, unknown or blacklisted ones. Such a system is natively present in InfoCards, and could be easily performed with

	InfoCards	Liberty Alliance / SAML 2	OpenID
Features	Authentication delegation, attribute sharing, …	Authentication delegation, attribute sharing, identity federation, single sign on, single log out, …	Authentication delegation, attribute sharing, single sign on, …
Consistency of the user experience	Very good: the same identity selector manages all the user interactions	The user interface depends on the implementation (no coherence)	There are currently works on how to integrate the user interface on web sites
Ease of use	The installation of the identity selector can be confusing	Good: most of the processes are transparent for the user	The use of a URL as a login is neither easy nor natural.
Integration of new authentication methods	Impossible (the authentication is included in the identity selector)	Possible	Possible
Scope of the identities	No limitations, but the service and identity providers must have compatible security policies to communicate	The use of identities are limited to the circle of trust they belong to, but an identity federation can enable their use on other circles of trust	No limitation on the use of the identities. Any identity issued by any identity provider can be used on any opened compatible service provider
Targeted public	General public	Suits enterprises, portals, and general public	Advanced web users, and general public

Figure 2. A Comparison Between the Identity Solutions

an OpenID provider. Second, some services can require business specific attributes with specific formats. That simple fact will restrict the scope of the usability. As a consequence, the only service providers that will be able to require and use those attributes will be those that are somehow related to the specific identity provider.

In a business specific context, all these solutions finally lead to a coherent and homogeneous kind of circle of trust, as there is no easy cooperation with its outside.

4. THE FC² PROJECT

If we consider circles of trust, identities and attributes are somewhat restricted to them. Some solutions exist to make the technologies interoperable, and there are also solutions to establish "bridges" of trust between circles of trust (if based on the same technology). However, none of these solutions enable a transparent federation of identities between circles of trust, regardless of the technology.

FC² (Federation of Circles of Trust) is a French innovative R&D project that deals with that subject (see [10]). This Section presents the project.

4.1. About the Project

The FC² project started in fall 2007 for three years, with a total budget of 17M€[1]. It involves 20 members, from very different backgrounds:

- Small and medium companies: CEV Group, entrouvert, NTX-Research, …
- Large enterprises from the industry: Orange Labs, EADS, …
- Universities and research laboratories: GREYC, CNAM…
- Prescribers: GIE-CB, French Interior ministry…

The objective of the project is to develop and validate a comprehensive platform allowing new secure digital online services, based on transparent federation of identities. It has for objective to demonstrate the feasibility of new business models based on the joint use of heterogeneous services such as banking, citizen, governmental and telecommunication services (see Figure 3). An objective of the project is to be as equitable as

[1] *The project is a "pôle de compétitivité" project, co-financed by the « Ministère des finances, de l'industrie et de l'emploi », the « DGE », the « Mairie de Paris », and the regions « Basse-normandie », « île de France », and « Hauts de seine ».*

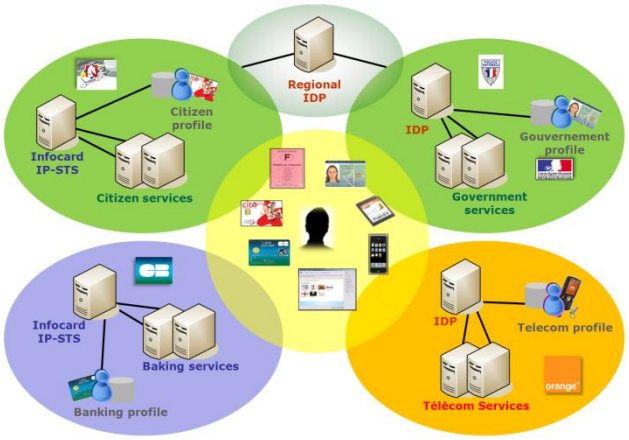

Figure 3. The FC² Project Involves four Distinct Circles of Trust (Citizen, Government, Bank, and Telecommunication)

possible on technologies, so interoperability is a major concern. The FC² project allows cooperation based on the share of identities and attributes from very heterogeneous services, but with strong respect to user privacy

4.2. A Sample Use Case

The project is based on a set of use cases that demonstrate the functional and technical use of the platform. Some of the use cases are for example the opening of a banking account, a car rental service, or the registration for voters' lists.

One of the use cases is the online registration of citizen's children for day cares on the citizen portal of a French city[2]. This use case is presented here as a didactic case, without any reference to the cost of such an architecture. To register a children, a citizen must provide the following information:

- His identity: first name, last name, birthdate, address, etc
- Information about his children: names, birthdates, etc
- His *Quotient familial*[3], which is generally included in the day care charges calculation.
- His credit card in order to pay in advance for the service

On a classical face-to-face procedure, the user would provide these information on a registration form, and proofs of his address (to prove he effectively resides in the town), and of his *Quotient familial* to avoid any misrepresentation that would decrease the price. Then, the user would pay the bill for example by credit card. Some of the latter steps can easily be done with a dematerialized procedure, but two problems still remain. First, the user will have to fill once again the form manually, which can be boring and discouraging for him. Second, there is no convenient solution to provide proofs with an online procedure. The only turnaround would be for the user to be physically present during the registration, which of course is not handy.

Users generally have multiple identities (*i.e.* accounts) on different circles of trusts. A user may have an account on his bank web site, an account on his telecommunication provider portal, an account on a government portal[4], etc. Most of the required data for day care is already available for this specific user, but is spread over all his accounts. Moreover, if a user could enable a service to share some of his personal data with another service, the information could be certified by the source. For example, the *Quotient familial* could be issued directly by the government (after an agreement from the user), and a postal address could be provided and certified by a telecommunication operator.

The FC² platform aims at helping users to share their personal information between different online services, in order to facilitate such interactions.

5. PRELIMINARY RESULTS

In this Section, we go deeper into important parts of the project that are directly related with the enabling of collaboration between heterogeneous entities. Presented solutions are not based on the interoperability of the identity technologies, but rather on tools and methods to enable interactions based on identity between heterogeneous circles of trust. At the time of this article writing, the specification step is over, and the development has just begun. The project FC² will lead to a proof-of-concept platform.

5.1. Two Solutions for a Federation of Circles of Trust

The project investigates two solutions to enable such interactions. Both these solutions will be developed for the proof-of-concept platform.

An **architecture centered on the user**, based on the concept of InfoCards. It is a B2C architecture, as the user

[2] *The municipalities in France manage day cares, so the registration could take place on the web site of a municipality.*

[3] *The French "Income splitting". It is a quotient calculated by the government, on criteria such as the income. It is used to adapt the amount of income tax to the capacities of a household.*

[4] *In France the project MSP, My Public Service, is a portal that offers an interface to the administration.*

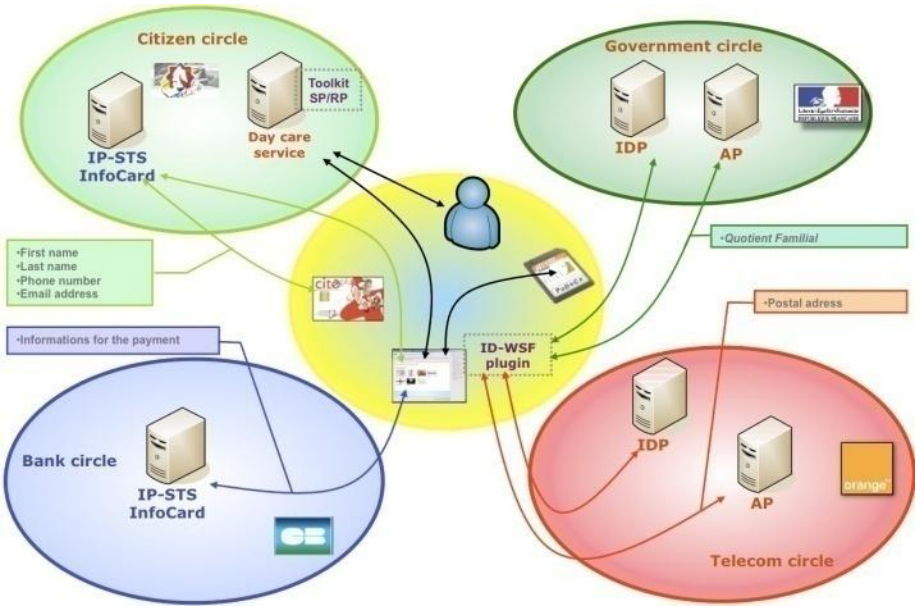

Figure 4. The User Retrieves his Personal Data from the different Circles of Trust Using its Identity Selector to use the Data Care Service

is the link between the service providers. The architecture is completed with a custom FC² identity selector that has to be installed on the user's computer (or device) and that provides access for the users to the different circles of trust (see Figure 4). This selector manages the information cards generated by the identity providers of each circle. Within such architecture, the user is under control of his identity, as he supervises the spread of his information between his accounts. The user can choose to provide or not to provide his cards (and the attached information) to a service provider asking for it. No link between the pool of identities of a user will be feasible without the intermediary of the user. It is clearly with respect to user privacy. Moreover, it provides the user a coherent and comprehensive interface to manage his identities. The custom FC² identity selector will be build upon a modified Higgins identity selector. It will be natively compatible with the InfoCard specifications, and there will also be experimentations on the storage of the database of the user's cards: on the computer, on a portable token or online.

An **architecture centered on the identity provider**, is more a kind of B2B concept, as it is based on a direct federation of the accounts between the identity providers of each circle of trust. Of course, the link is built with the permission of the final user. The major advantage of such architecture is to enable the SSO (Single Sign On) between different circles of trust. Moreover, there is no need of any piece of software on the user side except a standard browser. On the other side, linkages between the different identities of the user could make him feel bad about his federated identities. For example, the linkage, even superficial, between an account on a government portal and a bank portal could generate some (legitimate) questions on the privacy side[5]. However, that concept could be adapted for a professional context, where a user will gain on security and easiness of use.

5.2. Organization

It is not a trivial task to manage a trust link between heterogeneous circles of trust, mostly when there is no superior authority on this link. The organizations can be concurrent and does not necessarily have the same level of requirements in security and availability along with the same objectives, neither the same technologies. However, the number of circles of trust that will be part of the project is somehow limited. In fact, the platform is intended to be limited to a pool of well-identified organizations, someway to keep the trust between the partners and to prevent the integration of unsavory members.

To operate the acceptance of new partners, the management of trust links, and the maintenance of the overall consistency, the platform will need a technical and organizational committee. It will certainly be a board composed of representatives of each circle, but as there is

[5] *In France, privacy is a concern in the public opinion. The recent revelation of the existence of a project of a national database, called "Edvidge", which would contain sensitive information about some people has raised a wave of protests and initiated a global reflection on that subject.*

actually a study on that subject in France, its forms and missions are not yet defined.

5.3. A PKI Bridge

The physical materialization of a trust link between partners can be implemented by a cryptographic system. It enables the ability to provide four main services:

- *Privacy* prevents the access to information by unauthorized entities.
- *Integrity* is a proof that a message was not modified.
- *Message authentication* is a proof of the legit origin of a message.
- *Non-repudiation* is the insurance that the origin of a message cannot be repudiated or refuted.

These services are the technical basis of the trust links. For example, in the use case described in Section 4.2, the truthfulness of the origin of the postal address will be based on the authentication of the source of the message that contains the address. Moreover, if a participant approves to share a sensible data to another, it requires a strong security of the data. That task is complicated, as the actors of the project are very heterogeneous, and have different needs and security policies.

Each circle of trust in FC² has its own hierarchical PKI (Public Key Infrastructure), with a root CA (Certification Authority). Each server of a circle is certified by this CA, so it enables the use of cryptographic tools between the servers of a circle. However, in order to enable the use of cryptography between the circles of trust, we have to make these PKI interoperable.

An intuitive solution could be to add a layer with a global FC² Certification Authority that would certificate the local CA of each circle (see Figure 5).

Another solution could also be to establish a cross certification between the CA of each circle (see Figure 6). Both would enable the communication between all the partners of the project, and the use of cryptographic tools.

However, none of those solutions is suitable. A superior CA is hardly convenient as it would establish a hierarchical structure between the circles of trust. A cross-certification PKI would be hardly maintainable as the number of cross-certifications would expand geometrically with the number of partners. With two partners, two certifications must be exchanged, but with four partners there are twelve certificates to exchange. The number of cross certifications would grow rapidly, and the revocation of a certification will be reasonably unfeasible.

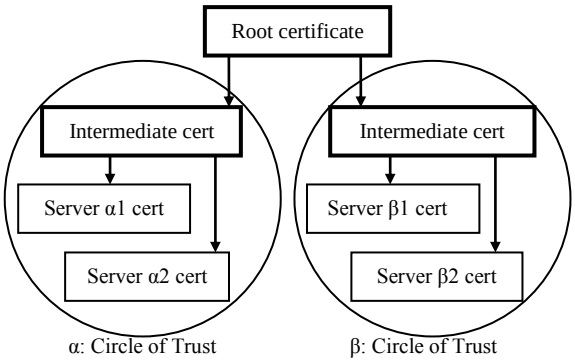

Figure 5. Hierarchical PKI

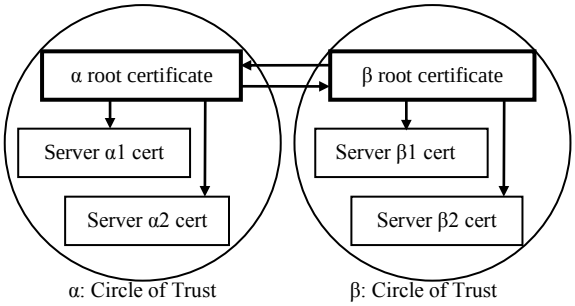

Figure 6. Cross Certification PKI

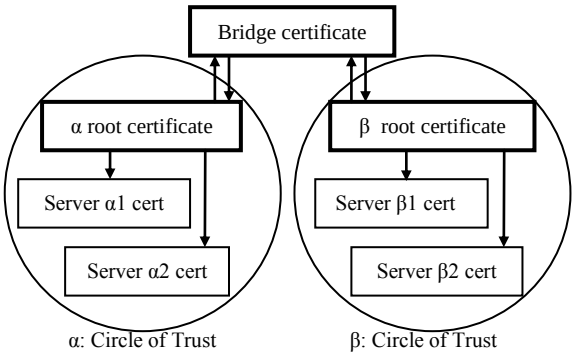

Figure 7. Bridged PKI

The choice for the FC² project is to deploy a PKI Bridge [11] with no subordination link between participants (see Figure 7). A PKI bridge is a technical solution where a central node, the bridge CA establishes cross certifications with the CA of each circle. The Bridge CA is sometimes referred as a "hub CA", as it is not a root CA for the architecture: its reputation is established by the number and the respective reputation of partners establishing trust links with it, by cross-certification, unlike a root certificate in a hierarchical PKI, which is issued by a self-proclaimed certification authority. It enables confidence relations between the partners, it evolves, and the central node can grant or reject the confidence of a partner easily (by revoking the certificates). Instead of twelve certificates to exchange,

there is just one. Furthermore, it reduces the validation chain for the end entity.

The bridge PKI matches the needs for collaboration between circles of trust. It combines the advantages of the two previous solutions. However, as the bridge CA is a central node, it has to be managed by a committee such as the one described in the previous Section.

5.4. A classification of Authentication Methods

Each circle of trust has its own authentication methods to assert user's identities: password, smartcard, certificate, etc. Each of these methods provides a different level of security: some are based on passwords, others on cryptography, or on the strength of the channels. Moreover, the same theoretical authentication method can be implemented in very different ways that could lead to a very different final security.

As an authentication could be used from a circle to provide information to another, the targeted circle has to be aware of the level of security provided by the source circle to ensure the reliability of the information it gets. The FC² project proposes a classification of authentication methods, inspired by existent classifications but adapted to the special context of the project. The classification is based on three levels: *, ** and ***, where * and *** respectively denote the lowest and the strongest levels.

The classification is based on eleven criteria:

- The security of the enrolment system,
- The security of the channel(s) used to give the user its credentials,
- The number of authentication factors,
- The availability and the accessibility of the revocation procedure,
- The use of well recognized and tested protocols (especially on the cryptographic side, if any),
- The use of a cryptographic process (if any) and its strength,
- The sensibility to a steal (eg. a password, or an authentication token),
- The sensibility to a brute force attack,
- The sensibility to an activity logger (key logger),
- The sensibility to a man in the middle attack,
- The sensibility to a phishing attack.

Each authentication method is evaluated on each of these criteria and receives a level between *, ** and *** for each. The global level of security provided by the authentication method is the level of the criteria that has the lowest level.

That evaluation facilitates the communications of information about the reliability of the authentication provided by another circle.

6. CONCLUSION AND PERSPECTIVES

The FC² project deals with the use of identities between heterogeneous service providers, involving different identity technologies. Different technical and organizational solutions for the interoperability of identity technologies will be developed and tested in that context, such as a PKI Bridge or a new classification of authentication methods. The joint use of these solutions will enable to unlock the feasibility of a lot of online services, and help to dematerialize many procedures.

The data interoperability is already a major subject of research nowadays, mostly on the format side. As already stated, from the user point of view, the share of personal (but non public) data between heterogeneous services is one element of highest concern. Therefore, the use of identity as a feature vector will certainly be a major subject of interest in the next few years, as more and more identity systems like InfoCards, OpenID and SAML/liberty system will be deployed on portals.

Those interoperability solutions will also have to keep privacy in mind, as a failure on this side would inevitably lead to a reject by the final user.

ACKNOWNLEDGEMENTS

The authors would like to thank all the national and regional administrations supporting the FC² project and especially the Regional Council of *Basse-Normandy* for their support of the current work.

The authors would also like to thank the members of the FC², and Olivier LEZORAY and Loïck LHOTE for their rereading.

REFERENCES

[1] J.D. Wallace, “Nameless in Cyberspace - Anonymity on the Internet,” *CATO Institute*, Briefing Papers, 1999.

[2] D. Chappell, “Introducing Windows Cardspace,” *Windows Vista Technical Articles*, 2006.

[3] K. Cameron, "The Laws of Identity", *Microsoft Web Services Technical Articles*, 2005.

[4] Novell, The Bandit project, URL=http://www.bandit-project.org

[5] Eclipse, The Higgins project, URL=http://www. eclipse.org/ higgins

[6] Project Liberty, URL=http://www.projectliberty.org

[7] OASIS, Security Assertion Markup Language, URL=http://www.oasis-open.org/committees/security/

[8] The OpenID foundation, URL=http://openid.net

[9] W.A. Alrodhan and C.J. Mitchell, "A client-side CardSpace-Liberty integration architecture," *Proceedings of the 7th symposium on Identity and trust on the Internet*, 2008, pp. 1-7

[10] The FC² consortium, URL=http://www.fc2consortium.org

[11] W.T. Polk and N.E. Hastings, "Bridge Certification Authorities - Connecting B2B Public Key Infrastructures", *PKI Forum Meeting Proceedings*, 2000.

[12] H-B. Le and S. Bouzefrane, "Identity management systems and interoperability in a heterogeneous environment," *Advanced Technologies for Communication*, 2008, pp. 239-242

[13] F. Layouni and Y. Pollet, "Mobile agents and their ontology serving a federated identity", 2008

[14] A. Davoux, J.C. Defline, L. Francesconi, M. Laurent-Maknavicius, K. Bekara, R. Gola, J.B. Lézoray and V. Etchebarne, "Federation of Circles of Trust and Secure Usage of Digital Identity", *Journal of Computer Security*, Vol. 14, Issue 3, 2008, pp. 269—300.

[15] M. Humphrey, J. Basney and J. Jokl, "The case for using Bridge Certificate Authorities for Grid computing", *Software- Practice & Experience*, Vol. 35, Issue 9, 2005, pp.817—826

[16] E. Maler and D. Reed, "The Venn of Identity: Options and Issues in Federated Identity Management", *IEEE Security & Privacy*, 2008, pp 16—23

[17] N. Klingenstein and I.M. Initiative, "Attribute Aggregation and Federated Identity", *International Symposium on Applications and the Internet Workshops*, 2007.

[18] B. Pfitzmann and M. Waidner, "Federated Identity-Management Protocols", *Lecture Notes On Computer Science*, Vol. 3364, 2005, pp. 153

[19] A. Pfitzmann and M. Hansen, "Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management-A Consolidated Proposal for Terminology", *Version v0*, Vol. 27, 2006, pp. 20