Collaboration and the Knowledge Economy: Issues, Applications, Case Studies
Paul Cunningham and Miriam Cunningham (Eds)
IOS Press, 2008 Amsterdam
ISBN 978–1–58603–924-0

Federation of Circles of Trust and Secure Usage of Digital Identity

Alexis DAVOUX[1], Jean-Christophe DEFLINE[2], Ludovic FRANCESCONI[3],
Maryline LAURENT-MAKNAVICIUS[4], Kheira BEKARA[4], Romain GOLA[4],
Jean-Baptiste LEZORAY[5], Vincent ETCHEBARNE[1]
[1]Orange Labs, R&D, 38-40 Rue du Général Leclerc, Issy les Moulineaux Cedex 9, 92794, France
Tel: +33 1 45 29 53 86, Email: {adavoux.ext, vincent.etchebarne}@orange-ftgroup.com
[2]Copilot Partners, 11, rue du chevalier de Saint George, Paris, 75008, France
Tel: +33 1 42 86 67 26, Fax: +33 1 42 60 19 09, Email: jcdefline@copilotpartners.com
[3] Groupement des Cartes Bancaires « CB », 31 rue de Berri, Paris, 75008, France
Tel: +33 1 5389 4068, Fax: +33 1 5389 3500, Email: ludovic-francesconi@cartes-bancaires.com
[4] TELECOM&Management SudParis, 9 Rue Charles Fourier, Evry, 91011, France
Tel: +33 1 60 76 44 42 number, Fax: +33 1 60 76 47 11, Email: {firstname.lastname}@it-sudparis.eu
[5]CEV Group, Zone Neptune 2, Rue Henri Claudel, Saint-Lo, 50000, France
Tel: +33 2 33 77 65 00 number, Fax: +33 2 33 77 65 01, Email: jean-baptiste.lezoray@cev-sa.com

Abstract: The joint growths of digital services and identity fraud exploiting poor identity management solutions have led to an identity crisis on the Internet. People struggle to keep control over their fragmented digital identities, and user privacy is not correctly enforced. As countermeasures, new digital identity initiatives include several distinct federated identity models, like Liberty Alliance or InfoCard. Based on the results of a French innovative R&D project called FC² (Federation of Circles of Trust), this paper investigates the ways to create a federated identity architecture compatible with the major existing identity technologies while providing a secure and coherent user experience. In the light of a practical use case involving a bike rental service requiring attributes from its users to complete their registration, the card-based identity selector seems to arise as a major client identity component. The first project results highlight the need for clear and simple user information on service providers about identity exchanges. A 'Simplified Sign-On' procedure for users and the need for digitally certified attributes are also exposed. On the business side, possible future models are sketched with their benefits for the different actors of the identity value chain. Eventually, studying the legal issues related to the federated identity model show that the responsibilities of the different actors should carefully be established within a circle of trust.

Keywords: federated identity, circle of trust, digital identity, user experience, FC², security, identity value chain, interoperability, Liberty Alliance, InfoCard, Higgins

1. Introduction

"Jack234", "Jack M.", "Dr Jack Malone"… These are not the signs of some kind of 'digital schizophrenia' but the multiple digital personas used by a same person on the web. And with the always-growing number of online services and the development of dematerialization processes, digital identity usage has become a key subject for the individual (citizen, customer or simple user) and his digital life. As a key requirement for secure electronic transactions and trusted digital exchanges (e-commerce and e-administration are two examples), digital identity management is a ground basis for the modernization of the society.

As security was not an initial goal in the conception of Internet, the users' identity is not widely normalized, and can rely on multiple different supports like certificates, system accounts, local databases linked to applications, directories... Fragmented and incompatible identity management solutions lead to personal and private information spread across service providers and no longer manageable by the end-user. People barely manage to keep trace of their distinct usernames, passwords, personas and personal attributes on the web. Identity fraud is growing fast: as a consequence, users are losing their trust in the e-services. More specifically, regarding personal data and privacy, consumers remain largely concerned about the usage that can be made with their data [1]. To remedy this situation, new identity management solutions have arisen, like an identity credential that could be used by many organizations for multiple functions. However, a majority of consumers remain divided on which organizations they would mostly trust to do so, and how data should be administered. Furthermore, local legislation would forbid a centralized repository for personal data in some countries.

At this time, different initiatives of identity portability already coexist. Among them, the federated identity model allows the use of digital identities over distinct security domains. It gives the users back control over their personal data disseminated amongst organizations. This model supports multiple identity and service providers. Yet it may vary in the way the actual 'identity federation' is done.

2. Objectives

Based on the previous statements, the following questions arise: how can the various identity management initiatives fit together? Is it possible to provide identity-aware and personalised services while relying on different identity models and respecting the user concerns about their digital identity and privacy?

To answer these questions, this paper proposes a new practical identity federation architecture involving various and multiple identity-aware service providers, aiming to provide a coherent and secure digital experience for the end-user. The adopted model should be interoperable with current major federated identity frameworks (Liberty Alliance [2], InfoCard [3] and Microsoft CardSpace [4] or the Higgins identity framework [5]…). It should also allow the end users to easily access services and securely share their personal data, while considering ergonomics and respect of user privacy as key requirements.

The resulting architecture should meet the user needs in terms of better and simpler identity management. At the same time, it should be considered viable by the actors of the identity value chain like service providers or identity providers. Indeed, it should enhance the development of new identity-based digital services by encouraging the adoption of federated identity management solutions and preventing identity-fraud. Business and legal stakes also have to be carefully considered. This paper analyzes some of them and considers societal issues as well.

3. Methodology

This paper is built upon the early results from a French R&D innovative project called FC² [6] (Federation of Circles of Trust), started in fall 2007. The main goal of FC² is to develop and validate a comprehensive platform allowing new secure digital online services, based on transparent and federated identity management. The actors of this project are small, medium and large companies from the telecommunications and banking industry, software vendors, universities, research institutes, and the French Home Office. The FC² project plans to deploy a platform demonstrating federated identity management solutions, involving services from three different fields of activities: public/governmental services, banking services and telecommunication services. FC² would like to stay as equitable as possible with regard to the identity technologies used.

This paper proposes to share and explain the first project analyses, with a focus on the relation between the user experience and the technical interoperability between different federated identity models. On one hand, consumers would highly welcome any system that may simplify their life, by allowing them to fulfil almost automatically their personal data (identity, banking card number, etc) in the various daily requests of the digital life. On the other hand, they are frightened by the potential usage being made with those same personal data. For a new identity management to succeed, it's therefore crucial to take into account the users' needs in terms of privacy and at the same time simplicity of use.

Eventually, the functional architecture of one of the main FC² scenario is proposed as a support for this reflexion, which leads to glimpses of a possible technical architecture, based on existing identity-related initiatives. Some innovative ideas and proposals are exposed, based on critical features like authentication and SSO, attributes sharing and payment processes.

4. Technology/Business Case Description

One of the use case studied by the FC² project is a functional and technical use case implicating a French public urban bicycle rental service, directly inspired by the "Velib'" success story in the city of Paris. This scenario is divided in two steps: a user registration to the bicycle rental service using a dematerialized procedure, and the use of a mobile service providing the journey best journey by bike to the user destination.

The user has to register to the bike rental service and is faced once again with a very tedious web form to fill. But as a regular user of the FC² platform, he has already entered the needed information (i.e. attributes) into his existing profiles in the different circles: his citizen account, his banking account and his telecommunication operator account. In order to avoid the painful completion of the form by the user, the FC² platform enables the registration website to get these personal attributes stored in various places in order to automatically fill the user form after user approval, even if different identity models and/or technologies are used by the entities involved. As a consequence, the user can easily fill a registration form while enforcing his privacy rights; at the same time, the bike rental service receives user information from trusted sources and offers a nice experience to the user.

Eventually, the user is able to access the mobile cartography website in a convenient but privacy-friendly way. In the use case, he wishes to find the best journey by bike to go visiting his friend. The site should access his geolocation and contact book with the address of his friend to provide an enhanced service. But this attribute sharing step is only allowed according to an access rule predefined by the user or after having explicitly asked 'on-the-fly' for his consent.

The functional description and architecture for this scenario can be seen below for a user called Anne. Each circle of trust, hosting one of Anne's profiles is shown by a different cloud. Arrows between profiles and a service represent the attributes sharing process, while the central circle models Anne's sphere of control on her personal information.

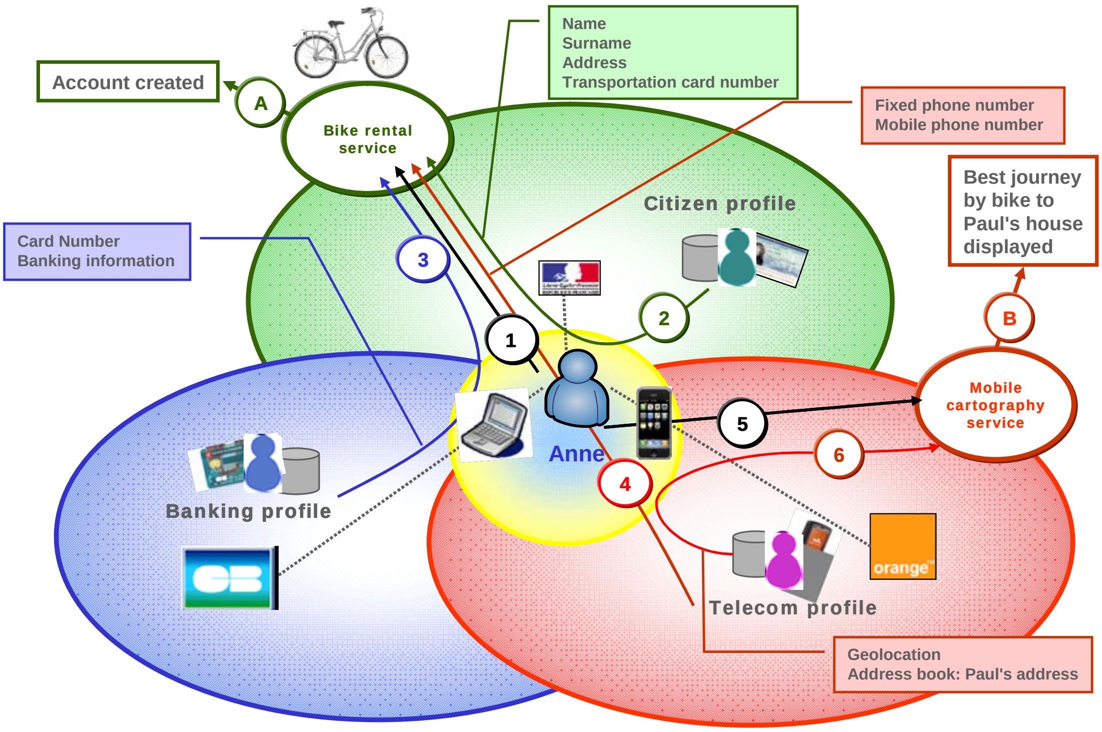

Figure 1: Bike Rental and Mobile Cartography Services Use Case Description

5. Developments

One of the main challenges with this use case is to achieve technical interoperability, while taking into account the key requirements such as ease of use and respect of user privacy. Indeed, the various services involved in this use case rely on different identity solutions. As a French government directive states for identity-aware citizen services, the 'citizen circle', with local and national identity providers, is based on the Liberty Alliance specifications. In this case, the identity federation is based on links established between the user's identities at the server level. Furthermore, it should also be possible for Anne to share attributes from her smart card, especially her CNIE, the future French electronic identity card. On the contrary, the banking services are more likely to be InfoCard/CardSpace-based. In this model, the identity federation is based entirely around the user, more precisely thanks to his identity selector containing his multiple InfoCards. Eventually, the telecommunication services adopt mixed identity technologies. So let's see what we've learnt from the first story-boards, with a particular focus on the user experience.

First, let's consider a Liberty/SAML-based platform. This solution offers a secure exchange framework, has already been deployed in various projects and is well-tested. However, during the registration process, personal information is gathered from three different circles and involves lots of network exchanges. Multiple redirections in Anne's browser can result in an unpleasant user experience and poor performance (especially on mobile devices). This can be partly avoided with the use of some kind of attributes broker, presenting at once all the personal attributes from the different profiles and waiting for the user consent before disclosure. Anne could also use a rich client installed on her machine. This client might rely on the ID-WSF LUAD (Liberty-enabled User Agent or Devices) or Advanced Client profiles. The main task of this client is to take care of authentication and attributes sharing consent interactions, thus avoiding multiple http redirections. Liberty profiles are natively supported and interactions with a smart card can nicely be integrated within the client. But from a technical point of view, these solutions could be problematic when invoking non-Liberty attributes providers (like the banking ones) or dealing with

InfoCards. Hopefully, on the server side, the Concordia project [7] or other initiatives like [8] have provided interesting material to achieve interoperability between Liberty-based services and InfoCard-based services. Thanks to the design of one of their scenarios, Anne can use one of her InfoCard on the Liberty-compliant bike rental service when needed. As a result, Anne would use redirections when invoking Liberty-based attribute providers, and the InfoCard identity selector to collect other attributes. The main drawback of this solution is the discrepancy in the user experience, which is not consistent within the whole registration process and may confuse Anne in the long run.

But from the user experience point of view, the use of card-based identity selectors remains very appealing. Thus using successively several InfoCard could be an alternative. For the bike rental registration scenario, Anne would select three different cards in three different steps, for citizen, banking and telecommunication information. In this case, this card-based only user experience remains consistent. But an InfoCard identity selector like Microsoft CardSpace cannot natively interact with a Liberty circle of trust. However, an open-source identity selector like the one from Higgins may be more flexible. The Higgins identity selector would work with the 'classical' InfoCard infrastructure and would interact with the Liberty infrastructure thanks to a SAML2/ID-WSF interface, still in development at the time being. Eventually, another additional module in the Higgins identity selector could handle the interactions with Anne's smart card or SIM card.

Thinking a little bit further, although the user experience is coherent, the multiple apparitions of the identity selector, each time showing her the suitable cards may not be so user-friendly and could be confusing. An even more attractive solution could be the use of a card-based identity selector to provide at once all the attributes needed. To achieve this goal, the FC² has considered the use of a "meta-card" FC², dynamically built to respond to the attributes requirements of the registration service. Using this meta-card would spare Anne the trouble of selecting multiple cards one after another in her identity selector by providing a simpler and coherent user experience. During the registration process, Anne clicks on the web page on the link "fill this form with my FC² attributes", invoking her identity selector installed on her machine. Then, she selects her meta-card FC², which collects all the attributes needed. The attributes are gathered automatically from the different attributes providers of the different circles: banking information from her bank, contact information from her telecom operator, address from the citizen circle… Then Anne validates within her identity selector the use of her attributes which are transmitted to the service provider. Indeed, this very idea of a "meta-card" can rely on the Higgins modular client/server identity selector, in current development. It allows the user to dynamically "compose" the identity presented to the service. As a consequence, the FC² project has initiated a collaboration with the Higgins project. Some Higgins components would definitely be helpful to provide a nice card-based user experience. However, for this scenario and others, we have to keep in mind that a full web-based experience should remain feasible and smooth enough for the end user not equipped with an identity selector, even if fewer identity features are available.

6. Results

Based on the first societal studies and story-board results, some recommendations are proposed to leverage the adoption and use of an identity federation system. First, the implementation of a brand / label (like the FC² logo for example) personalizes the supplied services and is perceived by the user as a sign of confidence. This confidence can be enhanced by supplying clear and transparent information about the process of sharing information between the various circles of trust and overall by letting the user be in control of which data he wants to share. It is vital for the various service providers to follow simple and harmonized ergonomic principles for identity-based functionalities, which has been considered as a key requirement in the FC² story-boards. Eventually, implemented security requirements and controls should be adapted to various contexts of use.

The FC² consortium is currently designing the architecture of the interoperability platform, taking into account interoperability constraints and user experience requirements. What kind of identity-related services should be offered by such a platform? Let's have a look at three key features: SSO, attributes sharing and the payment process.

Different identity models offer various kinds of web Single Sign-On. But the FC² project has determined that offering SSO between services belonging to different circles of trust on the web wasn't necessarily one of the most desirable features for users. However, offering "Simplified Sign-On", i.e., facilitating attributes sharing could really be helpful for the user Anne. What really matters is that she can easily share her attributes coming from her various profiles when she needs to register to or use a service, while keeping control on them and authenticating herself the fewer times possible. Furthermore, before the actual disclosure of her attributes, only one common consent interaction step should occur. Whatever user experience is privileged, Anne should remain in control of the disclosure of her personal information.

Indeed, Anne can share her attributes hosted on a distant attribute provider, previously provisioned by herself (her address) or provided by a specific service (her geolocation provided by her mobile operator). In both cases, the attributes can be signed by the attribute provider before being used on the service provider side. If the service and the attribute providers have a trust agreement, the attributes can be associated with a certain confidence level, adding more value for the service provider which receives a "certified" attribute from a "trusted" attribute provider. For example, during the user registration step, the bike rental service may need some mandatory information about the user's address to establish a digital contract. As a part of the dematerialization process, the telecommunication operator can provide, after user approval, a signed customer address as dated information whose origin is certified to the bike rental service. Eventually, Anne can also use a smart card to share some of her attributes stored on it, which are pre-signed by a third party (but not modifiable).

Eventually, the registration process ends with a payment step for the subscription fee. The FC² project has specified an innovative way to combine payment and identity management. 3D-Secure [9] is a secure architecture for online payment. Its main goal is to allow the seller to redirect the buyer to his own bank during a payment process so he could authenticate himself and authorize the current transaction. The innovative idea brought by FC² is to combine this system with InfoCard, so the user could use his identity selector to present a proof of authentication from his own bank and his signed banking attributes (i.e. credit card number) in one step to the seller site, eliminating the need of redirection to the buyer's bank and enhancing the user experience.

7. Economic and Societal Significance, Business Benefits & Legal Issues

7.1 Economic and Societal Significance

The general objective of the considered identity management service is to further the sound development of the digital economy. In order to deliver high value services on the Internet, service providers (either merchants or administration) will increasingly need to securely identify their customer / user with full certainty.

For the user, the benefits have to be well understood, thus explained carefully. Indeed identity is at the core of the human being, in a sociological way. Behaviours respond to many different factors, and users adapt to the requests by “negotiating” their personal data. In this context, the ergonomics of identity selectors seem well adapted to address the need of reference to a known environment (“my wallet”) and transparency (choice and consent).

7.2 Intended Business Benefits

From a business point of view, the FC² platform intends to bring added value to all players of the value chain, with a clear focus on the user experience.

From a user perspective, the platform offers time saving, better ease of use, seamless transaction, increased security, trust and confidentiality, as well as ubiquitous access (on any terminal, even without an installed identity selector).

On the service provider side, the service answers most market needs regardless of the industry. Tangible benefits are provided: productivity gains (decrease of allocated resources mostly), better fraud management and therefore lower costs, increase in quality of service, and better image. On top of this, a significant advantage for e-commerce use cases is the decrease in the rate of abandoned transactions, generating new revenues. Indeed, it is estimated that 46% of e-transactions are abandoned before completion [10] and 31% of customers prefer to shop at stores that don't require them to retype their name, address, and card number [11]. Providing this service, added to better ease of authentication, is likely to translate into better conversion rates. Eventually, by introducing new means of certifying personal data, the FC² platform can provide improved legal security (proof management) to the service provider, in order to tackle fraud and litigation issues.

But the business models adopted by the identity providers and other trusted third parties yet remain to be determined, their success relying partly on volume and recurrence of use. Identity providers should be able to monetize their service if the service provider and/or the consumer consider that the delivered value is worth paying for. However, since wide consumer adoption rate is critical, the main assumption is that service providers will probably bear most of the cost of the service if not all of it. In any case, the service provider should have enough incentive to use the service and will make its decisions on the basis of a cost / benefit analysis, taking into account the acceptable deployment cost of the selected solution, and the estimated return on investment.

7.3 Legal Issues

To cope with identity-related risks such as privacy violation, identity theft and fraud, legal and technical expertise should drive decisions enforcing users' privacy, consumption rights, administrative rights and the overall security of the federated identity architecture.

Within the European perimeter, two EU Directives [12] in the data protection and privacy field are relevant to the activities of most participants of the circles of trust. These directives regulate a number of categories of data and impose specific obligations or restrictions on those who handle this information and allocate compliance responsibilities according to the 'role' that any given participant is performing. In France, the law regarding the protection of the personal data has been amended in August 2004 [13] to comply with the Directives of 1995 and 2000.

Consequently, participants of the circle of trust will need to address the types of data that are being handled, what role they are performing in the CoT in respect of this data and, consequently, what obligations or restrictions this places upon them. The directives are likely to have a direct impact upon the necessary legal and contractual framework for a circle of trust. Indeed, the participants may be required to enter into particular types of agreements between each other. These will be dependent on who is performing which role, what data they are handling and for which *p*urpose, and where that data may be transferred. Addressing the who, what, which and where for a circle of trust is therefore an essential first step in developing the contractual framework.

Nevertheless, the diversity of the legal regimes that apply to the FC^2 context introduces high complexity in the legal framework definition. Indeed, administrative, commercial, competition and consumption laws are only a subset of the legal relevant codes. Public life and freedom to access information should be considered along with intellectual properties rights and privacy law. For example, proof management and traceability within a circle of trust can be delicate to implement. Eventually, local particularities should be taken into account: there is a special governmental legal regime that applies to data flowing out of France, especially towards USA. Of course, the impact of data protection and privacy laws may differ for the circles of trust and depends on the business sector and the relationship between the participants.

Service providers and identity providers assume the civil and criminal responsibilities in the event of collections of personal data using fraudulent, unfair or illicit means. Those issues are even more emphasized with the multiplicity of actors participating to the service value chain, mainly as identity providers, or service providers. However, the entities collaborating to the circle of trust do not have the same legal responsibilities. Those actors need clarification of their legal duties in relation to customers, and other players. As an early FC^2 outcome, a first recommendation for the legal setup of a circle of trust is to precisely identify actors in the value chain along with their responsibilities according to the role they play and the risks they take.

8. Conclusions

This paper has indeed investigated the ways to build an interoperable identity federation platform providing a coherent user experience related to digital identity across domains on the web. This platform, regardless of the identity technologies used by the different partners, considers user-friendliness, user privacy and user protection against identity fraud as strong common factors. Simple attributes sharing from multiple sources – different circles, different media, and different levels of trust- radically changes registration processes. As we have seen with the bike rental scenario, the use of a card-based identity selector is attractive for a new enhanced user experience. The Higgins project seems to be a promising framework to investigate.

As many other national or European projects prove it, digital identity management becomes the future pillar of digital life. From a societal point of view, the creation of digital trusted and comprehensible space for end users is at stake. For companies or states, mastering identity management technologies is a strategic domain. Eventually, identity-based business should boost the thriving digital economy. A more precise legal framework definition and a strong political will are also necessary requirements.

First results from the FC^2 project are only a glimpse of the expected results fuelling this topic. Next year, the first implementation and interoperability results should be available, which should let us highlight the first lessons learnt and provide more recommendations.

References

[1] Socio-economical study, FC² project, SP6 official deliverable, April 2008

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

[3] Identity Metasystem , Identity Selector Interoperability Profile V1.0

[4] Microsoft CardSpace, http://netfx3.com/content/WindowsCardspaceHome.aspx

[5] Higgins project, http://www.eclipse.org/higgins/

[6] FC² official website: www.fc2consortium.org

[7] The Concordia Project: http://projectconcordia.org

[8] Ivar Jørstad, Do Van Thuan, Tore Jønvik & Do Van Thanh: "Bridging CardSpace and Liberty Alliance with SIM Authentication", ICIN 2007, Bordeaux, France

[9] 3D-Secure, http://partnernetwork.visa.com/pf/3dsec/

[10] Shop.org/Forrester, "State of Online Retailing 2007"

[11] JupiterResearch/PayPal, "Confidence, Convenience, Choice", 2008

[12] Direction on protection of the personal data, 1995 and Directive on electronic commerce, 2000

[13] V. E. Caprioli, Loi du 6 août 2004 : commerce à distance sur Internet et protection des données à *caractère personnel*, Comm. Comm. Elect., Février 2005, n°2, p. 24-28