

Case Study: Entr'ouvert Leads Open Source Innovations in French E-Government

The Company

Entr'ouvert is a free software company whose primary commercial activity is in supporting e-government and e-voting solutions in France.

Headquartered in Paris, Entr'ouvert specializes in digital identity management and developed the first General Public License (GPL), or free implementation, of the Liberty Alliance standards, a library called LASSO. LASSO enables federation of scattered identities and single sign-on.

Entr'ouvert was officially founded in September 2002, as a SCOP (Société Coopérative Ouvrière de Production). A SCOP is run on democratic and transparent principals, extremely important notions to the six founders of Entr'ouvert. This means that the employees/founders own the enterprise in equal proportions. They earn the same wages, and important decisions are voted following the principle "1 employee = 1 vote."

"It's a different way of running a company and it fits our needs," said Pierre Cros, business development manager at Entr'ouvert. "We are very independent and not fond of hierarchy. Working this way is more efficient for us and I think it has an impact on making our products better. Although we love the model, and it's valuable to us, it's not for everyone."

Entr'ouvert is also a member of Libre-Entreprise, a corporate network with more than a decade of experience working in e-government. The Libre-Entreprise network gathers companies with close or complementary specialities, particularly concerning free software. All of them share the same values and structure.

“Using Lasso and the Liberty Alliance standards is the way to couple the needs for a strong authentication with an absolute respect of the user’s private life.”

Pierre Cros,
Business Development
Manager, Entr'ouvert

The Benefits of Open Source Federation Solutions

- The work one group does can be easily and freely leveraged by another.
- Customization costs tend to be lower.
- There's no editor dependence—since the code is free and accessible, the implementer can work any number of companies.
- Free (open source) solutions generally respect standards better than commercial products.

The network is present in France (Biarritz, Lille, Marseille, Montpellier, Mulhouse, Nantes, Paris, Rennes, Tours, Toulouse, Vandoeuvre-lès-Nancy), Belgium (Brussels) and in Canada (Montréal). This network allows Entr'ouvert to introduce wide-ranging and homogeneous commercial solutions, and to benefit from specialized resources in many domains, far beyond the company's own resources.

Liberty Certification

LASSO has been through Liberty's certification program for ID-FF 1.2 and has been awarded the Liberty Interoperable logo. Vendors who have been through this program interoperate cleanly with one another. It raises the probability that their products can be deployed successfully. It also minimizes the finger-pointing that typically goes on in these kinds of environments where one vendor points at the other guy saying, "Well, he didn't implement the specifications correctly." This won't happen. The logo says that vendors will have already proven that they can interoperate in a standards-based environment.

The Challenges

The French government wanted to enable e-services where the individual's privacy was assured. Entr'ouvert took a major role in three projects: Adeline (seamless communication between local and national e-government portals), mon service public.fr (national e-government portal) and the Daily Life Card.

The Solution

In 2003, Entr'ouvert began evaluating ways to enable government e-services, including e-voting. "The only solution we found that was acceptable was Liberty Alliance," said Pierre Cros. "We had the choice at that time between Passport from Microsoft and Liberty Alliance, and the choice was made quite quickly because we knew that Passport really was not a solution for us because it didn't account for privacy—so we decided to try to develop our own Liberty Alliance solution."

Definition of Terms

Identity (n) 1. the most basic element in a high value relationship 2. the individual characteristics by which a person, business, business partner, government agency or other entity is recognized or known

Single sign-on (n) 1. having the capability of accessing an online system once and having that authentication honored by other system entities, often service providers 2. sometimes called SSO

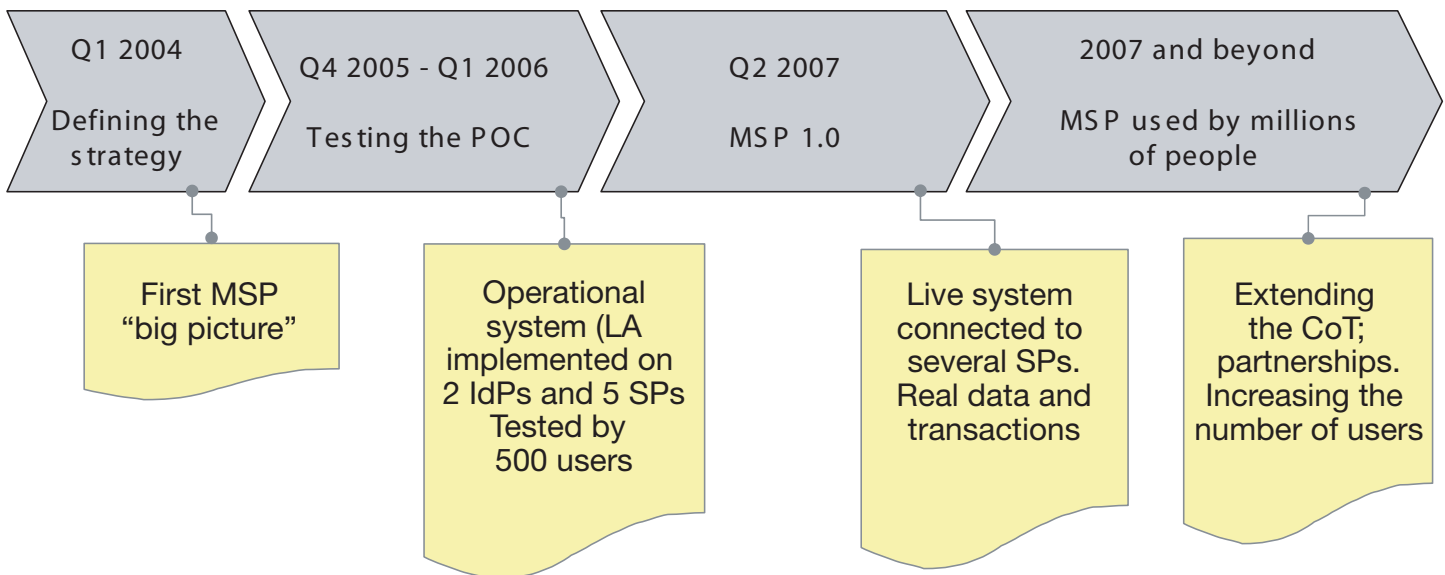
Identity Provider (IdP) (n) 1. a service that authenticates identity; often a trusted party such as a bank, mobile operator, or an

Internet Service Provider (ISP)
Service Provider (SP) (n) 1. a federation partner that provides services to an end user; service providers typically do not authenticate users but instead request authentication decisions from an identity provider

Federation (n) 1. an association comprising of any number of service providers or organizations 2. a model based upon trust in which user identities and security are individually managed and distributed by the service providers or member organizations 3. where the individual organization is responsible for vouching for the identity of its own users and the users are able to transparently interact with other trusted partners based on this first authentication 4. resembles the credit card model in that vendors accept an individual's ability to pay and then that ability is authenticated/verified through a single location

Circle of Trust (n) 1. a trusted group of identity and service providers who share linked identities and have pertinent agreements in place 2. where an individual or a business inputs a password once and minimal necessary credentials are shared among the Circle of Trust's members 3. a step strongly linked to federation, where multiple entities are involved, and there are business, policy and technical relationships in place 4. also known as "trust circle"

From a strategic view to a live system



Liberty Alliance Enables Single Sign-On Without a Unique Identifier

The French government refuses to work with unique identifiers like social security numbers, and this is an issue when deciding what technology to deploy. "Many European countries do not have problems with unique identifiers, but France does," said Cros. "France is very, very sensitive about privacy, and using unique identifiers in computing is forbidden. The beauty of the Liberty Alliance is that it enables single sign-on exchange without having these unique identifiers in circulation."

Entr'ouvert Develops Lasso

Entr'ouvert's open-source solution, LASSO, scrupulously respects the recommendations of the French authorities concerning safety, interoperability and privacy. Lasso is a free software C library that implements the Liberty Alliance standards. It defines processes for federated identities, single sign-on and related protocols. Lasso first focused on implementing the Liberty Alliance ID-FF 1.2 protocols. Work is now underway to provide full support for SAML 2.0 and ID-WSF 2.0 as Lasso will participate in the certification program for those protocols in December.

Contrary to many other implementations of Liberty Alliance, Lasso is not running on a Java/J2EE platform. The integration work is facilitated to a large extent by a service provider that can integrate Lasso within a few days of development, without calling into question its architecture.

"Using Lasso and the Liberty Alliance standards is the best way to couple the needs for a strong authentication with an absolute respect of the user's private life," said Cros.

“Many European countries do not have problems with unique identifiers, but France does. France is very, very sensitive about privacy, and using unique identifiers in computing is forbidden. The beauty of the Liberty Alliance is that it enables single sign-on exchange without having these unique identifiers in circulation.”

Pierre Cros,
Business Development
Manager, Entr'ouvertP

The Liberty Alliance in Action: Three Scenarios

1. The Daily Life Card

One of Entr’ouvert’s best known projects is the Daily Life Card, a multi-service smart card designed for citizens within a particular community. This project, initiated by the DGMA seeks to introduce the greatest possible range of Internet services to French citizens.

Entr’ouvert developed—for Vandoeuvre-lès-Nancy and the “Communauté Urbaine du Grand Nancy”—a scalable, economic, reproducible and reusable solution, based on open standards (Liberty Alliance) and free software (LASSO). The card is called Démocr@tics card. (Vandoeuvre-lès-Nancy is a small town. CUGN is a community of several small towns where Nancy is the biggest.)

“One of the principal challenges here was to set up a secure architecture in a hostile environment,” said Cros. “To do so, you should not trust the card reader, neither the microcomputer, nor the Internet network. This essential security required strong, two-factor authentica-

tion which must be perfectly respectful of privacy.”

That’s the reason why a minimum of personal data is contained on the cards and the servers. The whole range of services works according to the Liberty Alliance protocols thanks to the Lasso Library. “Information sharing for each service is always done under the control of the user,” said Cros. “The fact that there’s not an unique identifier in circulation makes a huge difference.”

Each Web site (service provider) delegates the user identification to a dedicated Web site (identity provider). A single identification allows the citizen to reach all the services (“Single Sign-On”), without transmitting its unique identifier to any service provider. The identity provider does not own any personal data concerning the user. Each service provider treats only the data necessary to his treatments (neither more nor less than before). The service providers can exchange infor-

mation, but only with the explicit agreement and under the permanent control of the user, and without knowing the unique identifier given by the identity provider. “It will basically simplify their relationship with the government administration,” said Pierre Cros. “We anticipate cost savings as the number of users increase.”

2. Adeline

Lasso supports Adeline, a project initiated by the Caisse des Dépôts et Consignations (CDC), a government office that handles a range of citizen activities. In France, a citizen typically connects to his portal to manage different changes in his life, maybe a move or marriage or the birth of a child. The portal provides links to the services he or she needs in this instance, such as health care, license or school registration.

CDC developed a portal for local authorities called Service-Public Local. The Adeline project represents an evolution of this

portal to make local and national e-administration services communicate seamlessly. The Adeline experiment involves five cities and 100,000 citizens.

The primary benefit of Adeline is that it simplifies previously onerous administrative processes through single sign-on and provides a document portal, an area where personal data and information-exchange records are stored. Adeline relies on Liberty Alliance standards including ID-FF, ID-WSF, and probably SAML 2.0 in a close future update. Entr'ouvert is in charge of the Liberty Alliance exchanges within the solution.

“Right now, Adeline is only an experiment, a prototype,” said Cros, “but the design and tech-

nology represents the future of French e-government services. The Liberty specifications are an important part of this future.”

3. Mon Service Public

Mon Service Public (MSP) is a project initiated by the French government. The lead technology contractor on the project is France Telecom, with Entr'ouvert providing an open-source Liberty Alliance frameworks.

MSP has the same goals and objectives as Adeline, but whereas Adeline starts at the local authorities' level, MSP is focused at the national level. Both projects work together now and Entr'ouvert is in charge of the interconnection. MSP is

basically a personalized service that will be accessible from the service-public.fr portal. It will enable every citizen to set up his or her own home page to access all the online public services of concern to him or her, allowing users to access all their official paperwork.

MSP will incorporate the services developed by different administrations (tax accounts, family benefits, etc.) under the control of the DGME (Direction Generale pour la Modernisation de L'Etat. A “personal space” (briefcase/e-safe) can be used for storage of personal data and official documents (diplomas, civil register certificates, etc.) which the user can obtain from the civil service and submit to the authorities to complete other procedures.

ABOUT THE LIBERTY ALLIANCE

Liberty Alliance is a global alliance of companies, non-profit and government organizations developing open standards for federated network identity, interoperable strong authentication and Web services. Liberty Federation and Liberty Web Services provide consumers and organizations with a more convenient, privacy respecting, and secure way to control online identity information. A list of organizations deploying Liberty Federation and Liberty Web Services is available at <http://www.projectliberty.org/about/market-adoption.php>. The Liberty Alliance management board currently consists of representatives from AOL, Ericsson, Fidelity Investments, France Telecom, General Motors, HP, IBM, Intel, Novell, NTT, Oracle, RSA Security and Sun Microsystems. Membership in Liberty Alliance is open to all commercial and non-commercial organizations. A full list of members, as well as information about how to become a member, is available at http://www.projectliberty.org/membership/become_member.php.