

---

## **Federated Identity Management Systems in e-Government: the Case of Italy**

---

**Roberto Baldoni**

Università degli Studi di Roma "La Sapienza" di Roma  
Dipartimento di Informatica e Sistemistica "Antonio Ruberti"  
Via Ariosto 25, 00185 Roma, Italy  
E-mail: baldoni@dis.uniroma1.it

**Abstract** Federated Identity Management (FIdM) systems are at the heart of any on-line service in a public, private or hybrid autonomous cooperating system. This paper reviews and compares several existing approaches for building FIdM systems in the specific sector of e-Government by showing identity management schemes employed by several countries representatives of different realities by size, geographical location and Public Administration traditions. The paper analyzes then the case of Italy by introducing the ongoing effort for defining and developing a nationwide e-Government Enterprise Architecture in order to guarantee a flexible approach for integrated application services, respecting local and central administrations' autonomy. The paper finally focuses on the FIdM aspects employed within the Italian Enterprise Architecture.

**Keywords:** Federated Identity Management; information security; management support; SAML; Enterprise Architectures; SAML; e-Government; public sector; Italy

**Reference** to this paper should be made as follows: Baldoni R (xxxx) 'Federated Identity Management Systems in e-Government: the Case of Italy', *Electronic Government, An International Journal*, Vol. x, No. x, pp.xxx-xxx.

**Biographical notes:** Roberto Baldoni is a Professor of Distributed Systems at the University of Rome "La Sapienza" and Director of the Joint-Lab on Security Research of Sapienza Innovazione the technology incubator of the University of Rome "La Sapienza". Roberto Baldoni does research (from theory to practice) in the fields of distributed, pervasive and p2p computing, middleware platforms and information systems infrastructure where he published more than two hundreds paper on peer-reviewed fora. He has been PI of many national and european research projects on egovernment including SEMANTICGOV, EG4M and EUPUBLI.com. He participated to the working group for the definition of the next generation systems for italian e-government (Servizio Pubblico di Cooperazione) and contributed both to the text of the Italian Law 82-05 "Digital Code of the Public Administrations" and to the Technical Rules for Interoperability in Italian e-Government (Law Decree of the Italian Prime Minister of April 1st 2008).

## 1 Introduction

Both in public and private sectors, organizations nowadays are building IT infrastructures to improve their business capacity and we are noticing a constantly growing inter-organizational integration (cooperative autonomous systems). One reason is a growing interest in using on-line environment to deliver and improve their added-value services by, for example, orchestrating services delivered by different autonomous organizations. The keypoint to enable this process is to set up a system to authenticate and to authorize users before providing such services and this should be done without increase significantly organization's operational costs [Reddick (2009)]. Systems managing such procedures are called Identity Management (IdM) systems.

As described by Lips and Pang (2008), historically three different models have been scoped out for designing IdM systems: Organization Centric IdM, User-Centric IdM and Federated IdM :

- Organization Centric IdM: centralized cross domain IdM. The organization keeps and manages personal information on the users also across sectors.
- User-Centric IdM: User has the control over his/her personal information;
- Federated IdM: involves the identity of a user's personal information stored across different IdM systems.

All these three approaches can be developed on a web-based infrastructure and can provide users with the capability of authenticate only once to get into a cooperative autonomous system (Single Sign-On). However as pointed out by Greenwood (2007) organization Centric IdM is based on hierarchically managed rules to check identities which is difficult to deploy in a systems of autonomous actors. User centric IdM is mainly focussed on the tradeoff between identity disclosure and privacy. In that sense for some aspect it could be considered as a complementary approach to Organization Centric IdM and Federated IdM.

As remarked by Windley (2005), federated IdM seems to be the appropriate approach for handling authentication and authorization in a cooperative autonomous system where each local system has its own IdM with independent identity schema and with the ownership on the identities it posses. Permissions to release personal information in the cooperative system are governed by agreements done among the different organizations and these agreements are actually trust relationships that form the "circle of trust" in the cooperative system. This way to operate allows thus to conjugate Identity interoperability with autonomy. In a Federated Identity Management System there are two main kinds of entities: service providers (SPs) and identity providers(IdPs). While SPs offer services to users who satisfy the policy requirements associated with these services, IdPs manage user authentication and user identity relevant information. Each organization, in that schema, may play both roles and they usually authenticate users SSO technology. With SSO, users can log on with the same username and password for seamless access to federated services within one or multiple organizations. Federated identity includes not only user's login names, but also user properties, or user identity attributes. Considering identity providers as normal service providers, the privacy preserving mechanism should be able to retrieve user identity attributes from different SPs [Baldwin et al. (2008)].

In this paper we will first review existing proposals for IdM systems including Microsoft Passport (2008), SAML (2002), Liberty Alliance (2008), WS-Federation (2009), Shibboleth (2008), OpenID (2008), also pointing out the weaknesses of each of them. Then we will look at a specific example of cooperative autonomous system in the public sector, namely e-Government. The case of e-Government is particularly challenging for federated IdM systems due to the heterogeneity of procedures, data and infrastructures among local and central Public Administrations that might be exacerbated from the political viewpoint and from local autonomies. From an ICT management point of view, decentralization, for example, generates different points of decision, possibly leading to different ICT choices as well as different organizational processes. These diversities can make tremendously difficult the implementation of political objectives at the inter-regional or national level sharing local and central competencies. Federated IdMs is thus a necessary vertical mechanism to implement interoperability policy at nationwide level [Gottschalk and Solli-Saether (2008)].

We survey the current situation of systems for Authentication and Authorization in several countries: New Zealand (2008), United Kingdom (2005), Austria (2009), Denmark (2009), Hong-Kong [Interoperability Framework Coordination Group (2008)]. These countries are representatives of different realities by size, geographical location and by tradition of public administrations, namely Continental EU, Scandinavian and Anglo-Saxon (with different cultural influences. i.e., European, Australian and Chinese). The paper analyzes the case of Italy by introducing the ongoing effort for defining and developing a nationwide enterprise architecture, namely SPCoop - "Sistema Pubblico di Cooperazione" [Public Cooperative System]. Additionally, we investigate the federated IdM system adopted in the Italian Enterprise Architecture and we list a few ongoing projects in the area. Finally we compare the Italian approach to federated IdM systems with the other countries as an example of a large country with grounded Mediterranean traditions in public administrations.

## **2 Federated Identity Management (FIdM) Systems: Existing Approaches**

Identity federation makes a company or an institution partnership-ready. For example, as a company opens its network and applications to partners, suppliers, employees, and customers, identity federation can ease integration, reduce deployment costs, and speed the rollout of new offerings. This section will review several approaches used in FIdM and will conclude with a table summarizing the main characteristics of each approach (Figure 1).

### *2.1 Microsoft Passport*

Microsoft Passport (2008) is the first implementation of FIdM systems and it addresses the issue of making more secure and simple on-line shopping when a transactions involves multiple sites. It provides two different services namely Single-Sign-In and Wallet. The first one allows users to have a single name and password to sign-in into a set of sites that adhered to Passport federation, while the second one is useful for having fast and convenient on line purchases within a Passport federation. Through this approach any user may control what information has been provided to some Web site and even in which way this information is used. It is designed to help federation members both

in carrying on online business transactions, in increasing revenue and in building strong relationships with customers, because of streamlining purchases, privacy promotion.

## 2.2 *Security Assertion Markup Language (SAML)*

SAML (2002) is an XML-based standard for exchanging authentication and authorization data between security domains. SAML is a standard managed by OASIS security Services Technical Committee. In SAML there is the notion of Service Provider and Identity Provider where the latter produces assertions and the former consumes such assertions [Liberty Alliance (2008); Pfitzman and Waidner (2003)]. SAML 1.0 defines a security token format (the assertions) and even “profiles” that describes how to use these assertions to provide Web Single Sign-On. SAML 2.0 gives users and consumers the possibility to have authentication and sign-on on Internet-based services and on e-commerce applications, using a network or a domain once from any device and then apply to different web services from multiple web sites. In this approach it is requested user authentication just once at the login and it can support privacy controls decided by the customer.

SAML assumes the principal (i.e., the user) has been enrolled with at least one identity provider that it is encharged to provide a local authentication service to the user itself. However, SAML does not describe the implementation of those local services, that means SAML it is not interested in how the local service authentication are implemented. Therefore a service provider delegates to an identity provider the identification of each principal and it trusts the identity provider’s assertions. In fact, when a principal requests some service, the identity provider passes a SAML assertion to the service provider. From this point on, the service provider is able to decide regarding the service erogation, on the basis of that assertion.

## 2.3 *Liberty Alliance*

Liberty Alliance (2008) is a business alliance, formed in Sept 2001, with the goal of establishing an open standard for federated identity management. Global membership consists of consumer- facing companies and technology vendors as well as policy and government organizations. The board includes SUN, Fidelity, BT, CA, AOL, Nowell, NTT, Oracle. The Liberty specifications are based on extensions to SAML 1.1 that enable important features for multilateral federation, such as global signout and account linking. One of the main outcome of Liberty is to influence SAML standard and, as a matter of fact, OASIS incorporated the Liberty extensions into SAML 2.0 in March 2005.

Liberty basic concepts are: (simplified) Single Sign-On, Single Lockout and “circle of trust”. SSO allows a user to sign-on once at a Liberty enabled site and to be seamlessly signed-on when navigating to another Liberty-enabled site without the need to authenticate again. Single logout provides synchronized session logout functionality across all sessions that were authenticated by a particular identity provider. Finally, Identity Providers and Service Providers federate by creating circles of trust around each other. These trust circles are based on technological, operational, and legal agreements that the Identity and Service providers put in place before they offer federated services to users.

## 2.4 *WS-Federation*

Announced in July 2003, WS-Federation (2009) provides similar identity federation services than the Liberty Alliance and SAML 2.0 specifications, such as SSO, global logout and session management, circle of trust and the use of pseudonyms for user privacy. WS-Federation is supported by Microsoft, IBM, VeriSign, BEA and RSA Security [Goodner et al. (2007)]. The major difference between WS-Federation and Liberty Alliance is in the underlying technologies. WS-Federation relies on components that Liberty doesn't support. These include WS-Trust, which describes a trust framework for Web services interoperability; and WS-Policy, which describes the capabilities of security and business policies for entities that participate in a Web services transaction. Carrier for this information exchange is SOAP. WS-federation is compliant with SAML standard even though it is not a part of. It should be noted that at three years after the WS-Federation specification, it has not achieved much adoption in the mainstream FIDM community.

## 2.5 *OpenID*

OpenID (2008) has arisen from the open source community. It has been developed to address identity problems that were not easily solved by the existing approaches as remarked by Recordon and Reed (2006). OpenID provides a way for recognizing people that uses the same technology framework for websites identification. Distribution of OpenID (user or provider) is for free and it is not required any kind of registration or approval by any organization. As Microsoft Passport, also OpenID provides the user the possibility to have a unique username even for different websites, allowing an easier way to have online transactions on an internet scale. As a matter of fact, OpenID framework is emerging as a viable solution for Internet scale user-centric identity federated infrastructure.

The main OpenID features are about the fact that it is open, decentralized and free framework for user centric management of digital identity. This approach uses already existing technologies (such as URI, HTTP, SSL) and takes into consideration the fact that users are creating identities for themselves at any time, using blogs, poststream, profile page, etc. Using this approach, it will be easy to change an already existing identity, based on these existing URI, to an account which could be used as sites which support OpenID logins. In OpenID there are no central authorities. This means that it is not required any registration or approval for both OpenID Providers and Relying Parties. A generic user may select to use the preferred OpenID Provider, maintaining its Identifier in case it switches from this Provider.

## 2.6 *Shibboleth*

Shibboleth (2008) is an open source software package for web single sign on either across or within organizational boundaries. Using Shibboleth, websites are free to make informed authorization decisions for individual access of protected online resources, preserving privacy. This software uses federated identity standard, above all OASIS' Security Assertion Markup Language (SAML), to have single sign-on and attribute exchange framework. Additionally, Shibboleth guarantees extended privacy functionality, giving the browser user and their home site the possibility to control the attributes released to each application.

Even in Shibboleth it is possible to identify service providers and identity providers. Shibboleth provides not only single sign-on functionality, but also it may help in controlling access to either campus based or licensed resources. Shibboleth in cooperation with some identity management system release the necessary information required by service partners to authorize the user. Shibboleth has much in common with SAML. Shibboleth uses SAML formats and binding protocols whenever possible and appropriate. As an example Shibboleth uses SAML's attribute statement and assertion format.

### *2.7 Shortcomings of Existing Approaches*

In Hommel and Reiser (2005) a list of shortcomings to existing FIDM has been detailed including limitation to web service technology, persistent data storage and the presence of a common data schema for attributes. None of the existing approaches to FIDM could be applied to services that either are not yet available or could not be completely erogated, e.g. email and file storage. Although there are web interfaces for both, it is much more used the access through conventional protocols. Additionally, as there is no support for such legacy protocols, it is mandatory a user registration and system provisioning. Although the service provider may ask any information attribute about user identity from the user's identity provider while the service is being used, none of these approaches forecast to notify the service provider later on about changes in this data. Another important point is the fact that there are many problems related to privacy control and federation security, in fact although a public key infrastructure is very useful, for example in supply chain management, it is not easy to realize in practice: in fact it will require huge resources for setup and maintenance.

## **3 Federated Identity management Systems: The case of e-Government**

"Federated Identity" is a set of mechanisms through which organizations can share identity information between security domains. As a result of federation, organizations are now able to create identity-based applications (such as federated single sign-on) that enable increased access to cross-boundary information. Federated identity provides organizations with several advantages. Federation means that local identities and their associated data are linked together through higher-level mechanisms, although they remain in place. This allows for efficient management, control, and movement in a radically distributed world. Federated identity guarantees thus a flexible mechanism that can be used for user authentication from partner organizations.

Identity federation therefore makes sense for a broad range of private and public organizations. For example, in the former context, a computer game developer might federate with a large number of mobile phone companies to offer downloads to subscribers. In fact, federation and SSO are particularly desirable for mobile providers, where logging on to multiple sites using a cell phone's keypad becomes highly burdensome for consumers. The public context boils down to make easier to receive services from networked organizations of the public sector towards users. Several examples of these services will be described in the rest of the paper.

As remarked in McKenzie and Crompton (2008), the difference between a public and a private sector lies in the fact that public institution must look into much broader issues, such as inclusion, consistency and interoperability as it serves an entire population

	<b>Microsoft Passport</b>	<b>SAML</b>	<b>Liberty Alliance</b>	<b>WS-Federation</b>	<b>Open-ID</b>	<b>Shibboleth</b>
<b>Type of Distribution</b>	Specs, implementation and distribution are not free	Specs are free to implement in products and services	Specs are free to implement in products and services	Specs free to review. Implementation and distribution costs unknown	Specs, implementation and distribution are free distributed by the community	Specs are free to implement in software and services
<b>Services</b>	<ul style="list-style-type: none"> <li>• Single-sign-in wallet</li> </ul>	<ul style="list-style-type: none"> <li>• Single-sign-on</li> <li>• Single logout</li> <li>• Opaque identifiers for privacy</li> </ul>	<ul style="list-style-type: none"> <li>• Single sign on based on SAML token</li> <li>• Single logout</li> <li>• Opaque identifiers for privacy</li> <li>• Trust based on legal and business agreements</li> </ul>	<ul style="list-style-type: none"> <li>• Single sign on based on WS trust token</li> <li>• Single logout</li> <li>• Opaque identifiers for privacy</li> <li>• Information sharing based on UDDI</li> </ul>	<ul style="list-style-type: none"> <li>• Single sign on</li> <li>• Single logout</li> <li>• User controlled privacy</li> </ul>	<ul style="list-style-type: none"> <li>• Single sign on based on SAML trust token</li> <li>• Single logout</li> <li>• Attribute check for licensing of software application</li> </ul>
<b>Scalability</b>	Small federations	Fully scalable	Fully scalable from Liberty 2	Fully scalable	Fully scalable	Small federations
<b>Attribute exchange</b>	Available	Available	Available from Liberty 2	Available	Available	Available
<b>Third party for attribute certification</b>	Not available	Available	Available from Liberty 2	Available	Available	Available

Figure 1 Comparison among different approaches to Federated Identity Management.

and not specific demographic sector as private companies do. Identity management in e-Government could lead to efficient and accountable online service delivery, law enforcement and national security. As a consequence, in recent years, several governments have approved directives for the improvement of e-Government services and identity measures to access citizen's individual information/records on government and related sites; these context has realized the develop of many different challenges in e-Government. For example Liberty Alliance's output reflects collaboration by a number of organizations involved in all areas of government, including local and national agencies, government standards groups, and IT vendors and contractors that drive public/private sector implementations and partnerships. However, not every country decided to adopt a federated approach to identity management, some of them adopted other schemes according to the culture and their relation with the local governments. In the next sections we will review several decisions adopted by different governments that are more advanced in handling digital identities and that represents countries with different sizes (in terms of populations) and belonging to different traditions in public administrations, namely Mediterranean, Continental EU, Scandinavian and Anglo-Saxon with European, Australian and Chinese influence. A summary of the comparison is then depicted in Figure 3.

### 3.1 *New Zealand*

New Zealand (2008) ranks the 14th place in e-readiness, according to *The Economist's* Intelligence Unit and IBM Institute for Business value. E-government plan has the following goals:

- "By 2007, information and communication technologies will be integral to the delivery of government information, services and processes.
- By 2010, the operation of government will be transformed as government agencies and their partners use technology to provide user-centered information and services and achieve joint outcomes.
- By 2020, people's engagement with the government will have been transformed, as increasing and innovative use is made of the opportunities offered by network technologies".

New Zealand has launched an e-Government Interoperability Framework (e-GIF). "The e-GIF is a set of policies, technical standards and guidelines covering ways to achieve interoperability of public sector data and information resources, information and communications technology (ICT), and electronic business processes. It creates the ability for any agency to join its information, ICT or processes with those of any other using a predetermined framework based on 'open' (i.e. non-proprietary) international standards. So far, the e-GIF covers four areas of e-government activity where the ability of agencies to interoperate is essential. These are: Interconnection (of information systems); Information Sharing and Exchange; Access (to information and systems); and Service delivery (inter-agency business protocols)".

Therefore the identity management problem is part of the NZ e-GIF. Technically it is based on an own version of SAML called NZ SAMS. NZ SAMS is one of the main parts of NZ e-GIF authentication standards and provides detailed guidance for agencies

to follow when designing their authentication systems. The Secure Messaging working group, comprising representatives from New Zealand government, agencies and domain experts, is drafting NZ SAMS. The first version was centered on authentication. Subsequent versions will focus on identity attributes and authorization. When applicable, identity federation may incorporate Single Sign-On (SSO). SSO is realized through a Government Logon Service (GLS), a pseudonymous identity provider that let people access to many government service. Identification is performed through an Identity Verification Service (IVS) which makes a verified identity assertion to government agency service providers in a user controlled manner.

### 3.2 *United Kingdom*

United Kingdom (2005) has recently developed a system for identity management and an e-GIF. The latter defines the technical policies and specifications governing information flows across government and the public sector. These cover interconnectivity, data integration, e-services access and content management. The former offers services directly or programmatically that is through the Government Gateway web site or via the UK Central Government Portal Directgov [Lips and Pang (2008); Taylor et al. (2007)].

A citizen, to use any Gateway service, would need to register first. This usually requires to provide full name, email address and the choice of a password. Each member will provide even known facts for the individual services that are being enrolled for, such as Unique Tax Number or National Insurance Number. At the enrolling moment, it will be required to provide these known facts for each service, in order to verify them against the existing data. This system is based on existing data held in government databases, in fact each registered citizen will receive at home a PIN, using the postal address already present in the government organization [Lips and Pang (2008); Taylor et al. (2007)]. The Registration and Authentication Framework provides different authentication levels depending on each specific service. There are four levels that goes from the "no authentication needed" to the "digital certificate and biometric authentication required".

Third party organizations are involved in identity management processes as providers of digital certificates in online service transactions with individuals. Also, third party organizations are involved in providing authentication schemas [Lips and Pang (2008); Taylor et al. (2007)].

### 3.3 *Austria*

Austria (2009) e-Government strategy is based on the following principles: proximity to citizen, convenience through efficiency, confidence and security, transparency, accessibility, usability, data protection, cooperation among public administrations, sustainability, interoperability and technological neutrality. After emanating this principles, the Austrian Government promulgated the Austrian e-Government act that also defined the guidelines for identity management. In particular the Central Register of Residence (CRR) was launched in 2002.

Austria uses a national-identity-number-based-system, affording many privacy risks through the technical design of the system, which has many distinct similarities to the one New Zealand adopted years later. Austria's source PIN and pseudonymous-sector-specific PIN realize the function of authentication for Austrian citizen card holders to a

sector agency in a similar way done by New Zealand. Citizen uptake of Austria's system hangs in the balance because the system depends on the complexities of a smart card, and the market penetration of smartcard readers in Austria remains relatively low [Lips and Pang (2008); McKenzie and Crompton (2008)].

In 2000, the Austrian Federal government decided to introduce smart card technology to increase citizens' access to public services. The first Austrian Citizen Card was issued in February 2003. Since then, the Citizen Card idea has been enlarged to other kinds of cards, for example ATM cards, public servant ID documents. The two most important requirements for the Citizen Card are the provision of identification and a secure electronic signature in accordance with Austrian Signature Law requirements. Speaking about possible services provided by this card, we may cite on-line tax declaration, digitally signed criminal record.

### 3.4 *Denmark*

Denmark (2009) is at the very top level in e-readiness in the last three years, according to Economist Intelligence Unit (2007) and IBM Institute for Business value and e-government. Since 1986 its citizens have been digitally registered and there are nationwide registers for housing, livestock, income data and other areas. The government has the objective that by 2012 all relevant written communication among companies, citizens and the public sector should be electronic [Nielsen (2007, 2008)]. To make a step further, in 2006 Parliament decided that open standard use must be mandatory in public sector solutions; in the same year it has been established that a citizen portal should be realized, replacing the municipal portal and the governmental portal. One of the main points in this shift is that individuals usually have been engaging with multiple agencies and multiple log-ins, and, in order make easier this scenario, rises the need to have a better integration among different services, that could mean even a better integration between public and private sector.

Danish profile includes Web Single Sign-On(SSO) using redirect/POST binding with attribute mapping and persistent pseudonyms. SOAP binding is also included to provide single log-out and attribute query [Nielsen (2008, 2007)]. Finally, attribute profiles are used to describe extra attribute sets that can be exported as part of authentication assertions or attribute assertions. It has been planned to have a Web SSO in order to have Digital Signature for allowing citizens and employees to log in; additionally, there is a Government-to-Government SSO meaning that each authority shall have its own authentication point, for instance, as a web service.

### 3.5 *Hong Kong*

Hong Kong announced a plan for e-Government in 2001 aimed to achieve the following points: facilitating a digital economy, promoting advanced technology and innovation, developing Hong Kong as a hub for technological cooperation and trade, "enabling the next generation of public services and building an inclusive knowledge society. This e-Government plan is mainly based on two basic pillars: the Hong Kong's Smart Identity Card System (SMARTICS) and a Public Key Infrastructure both introduced around 2000. As a part of the "enabling the next generation of public services" in late 2007 the Hong-Kong portal has been launched providing around 1200 on-line services. To achieve this objective the Government of the Hong Kong Special administrative region

published the "Analysis Underpinning The HKSARG Interoperability Framework Recommendations" that defines rules for interoperability of data and services in cooperative contexts [Interoperability Framework Coordination Group (2008)]. The book analyzes more than 70 problems of interoperability and for each of them, describes its level of maturity and, in the affirmative, select the available standards and make a recommendation. In the context of federated identity management, reviewed three standards: SAML v2.0, WS-Federation and Liberty Alliance. SAML has been selected as recommended standard with the following rationale:

*Platform neutrality.* SAML abstracts the security framework away from platform architectures and particular vendor implementations. Making security more independent of application logic is an important tenet of Service-Oriented Architecture.

*Loose coupling of directories.* SAML does not require user information to be maintained and synchronized between directories.

*Improved online experience for end users.* SAML enables single sign-on by allowing users to authenticate at an identity provider and then access service providers without additional authentication. In addition, identity federation (linking of multiple identities) with SAML allows for a better customized user experience at each service while promoting privacy.

*Reduced administrative costs for service providers.* Using SAML to 'reuse' a single act of authentication (such as logging in with a username and password) multiple times across multiple services can reduce the cost of maintaining account information. This burden is transferred to the identity provider.

*Risk transference.* SAML can act to push responsibility for proper management of identities to the identity provider, which is more often compatible with its business model than that of a service provider.

WS-Federation and Liberty Alliance have been considered as promising, but extensive adoption in the market, major project implementations and interoperability amongst different products remain to be seen.

#### **4 E-Government Italy's standpoint**

Before 1999, the scenario of the ICT in the Italian public administrations (PAs) was very heterogeneous: there were sectors of excellence in some central PAs as far as basic and advanced interoperability is concerned, and other central or regional PAs that acted as almost isolated systems. In this context, the "Nationwide Cooperative Network" (referred to as RUPA in Mecella et al. (2001)) was established by the Italian Cabinet in order to provide security and basic interoperability services (e.g., directory, e-mail, WWW) to the central PAs. But, even if RUPA created a centralized system's vision (about interoperability) and generated big savings for the central administrations. Nevertheless, during the years it became clearer that basic interoperability is not sufficient, and there was a real need for advanced interoperability and application cooperation/integration between back offices.

In 2001, the reform of the Italian Constitution attributed new possibilities for action to Regional authorities. From an ICT management point of view, this process of decentralization of competencies and diversification of ICT solutions that, on one hand, helped to define and to actuate in a rapid way political objectives at the regional or local level. On the other hand, this decentralization generated different points of decision,

possibly leading to different ICT choices as well as different organizational processes. This can bring rapidly to the proliferation of different regional interoperability infrastructures with the consequent high risk of inefficiency at National level. This would make tremendously difficult the implementation of political objectives at the inter-regional or national level. Many examples of such National strategic objectives can be found in the areas of healthcare, employment, register offices, tax offices, etc. As a result, this process of competence decentralization, instead of turning out in an advantage for the country, it can lead to a lack of interoperability among the PAs with the consequent loose of competitiveness and efficiency of the country.

Given this context, the issue was to set-up an organizational process that would allow the development of nationwide application cooperation/integration between back offices and then involve citizen in the loop. In 2003, the National Centre for IT in Public Administration, CNIPA, started the coordination of a nationwide bottom-up consensus operation, from basic telecommunication services to advanced application cooperation. CNIPA is a government agency which depends on the Italian Cabinet. CNIPA supports and implements policies delivered by the Minister for reform and innovation in Public administration. Different working groups were started with the participation of over 300 representatives of central and local PAs, Universities and research centers and Italian ICT companies. The outcome has been a set of about 30 documents describing a technical and organizational nationwide system for network, communication, basic interoperability, cooperation and security services among administrations. This system consists of SPC - *Sistema Pubblico di Connettività* [Public Internetworking System] and, on top of it, of SPCOOP for the application cooperation among PAs.

#### *The Legal Interoperability Framework.*

In parallel to the bottom-up process for the definition of SPC and SPCOOP, the Government issued in February 2005 a Law Decree, namely the digital administration code (CAD), Law decree n. 82/05, that defined the legal interoperability framework, CAD defines rules regarding the digitalization of the PAs, grouped in the following sectors: (i) The rights of citizens and enterprises on Public Administration (ii) Citizens and enterprises must be placed at centre of PAs services (iii) Digital signatures and legal validity; (iii) Contracts, payments and accounting deeds (iv) Development, acquisition and reuse of software in PAs. Moreover, as far as SPCOOP and SPC is concerned, CAD establishes its scope, the sectors of interest, the governance, the technical rules of the Italian Enterprise Architecture, and the subsidiarity principles among National authorities and local ones. Additionally, CAD establishes two important principles:

- the cooperation among administrations is exclusively carried out on SPCOOP, with its tools and according to its technical rules; it has *legal* value and no further decree or official publication (e.g., on the Gazette) is needed (e.g., when defining standard XML formats for data exchange);
- the public ICT managers need to organize their information systems, including organizational and management aspects, in order to accommodate SPCOOP rules.

#### *The Italian Enterprise Architecture.*

SPCOOP is not only a software framework, but also a technical and organizational platform whose aim is to create the conditions for a long-lived *legally valid* cooperation

among administrations. It is based on four pillars which are leading-edge in terms of technologies, best practices and organization: (i) formalization, and successive publication, of *service agreements* between PAs; (ii) definition of a federated identity management system for access control; (iii) definition of the metadata about the effective data to be used for cooperating, of the semantics and of domains' ontologies; (iv) open and continuous update of the SPCOOP model, by taking into account the latest progress in technologies and standards.

#### *Accompanying Measures.*

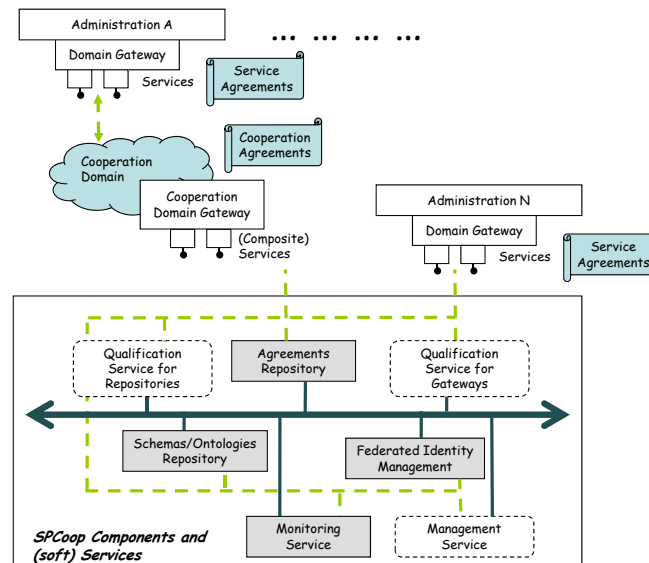
56 regional projects on e-Government, focused on network and interoperability infrastructures, has been launched, for an overall amount of 100MEuros. These projects will provide best practices as well as reference implementations of the different SPC and SPCOOP elements, in order to direct the bottom-up approach. The biggest project is ICAR (Interoperability and Application Cooperation among Regions), started in June 2006 with 17 partners including 16 out of 19 Italian Regions. The expected results from these projects are: the compliance of large horizontal projects with SPCOOP; the complete definition and advertisement of about 50 service agreements, and the beginning of the definition of about another 100 service agreements; the definition of the core of an upper ontology and of two specific domain ontologies; finally the definition of metric for service-level agreement, the design of a SLA monitoring system and the reference implementation of all the components.

#### *4.1 Overview of SPCoop Enterprise Architecture*

The model proposed for SPCOOP is based on the following principles:

- The PAs cooperate through the supply and the use of *application services*; these services are offered by the single administration through a unique (logic) element belonging to its own information system called *Domain Gateway*. In this way the complete autonomy of the single administration is guaranteed, as far as it concerns the implementation and management of the provided application services, as they can be based on any application platform, being it pre-existent or new, as long as they are supplied through the Domain Gateway. The fruition of the application services is carried out through the exchange of messages, whose format is formally specified in the Italian standard referred to as *e-Gov Envelop*. Such a standard is basically an extension of SOAP.
- Sets of administrations which need to cooperate in order to provide composite application services form a *Cooperation Domain*; the services supplied by such a domain are *externally* described through Service Agreements, and *internally* by a specification describing how the different PAs concur to compose the final service, referred to as *Cooperation Agreement*.

It emerges that the cooperation model of SPCOOP is organized as a Service Oriented Architecture (SOA) ?; but even if the basic aspects related to a SOA are well defined under a technological point of view, conversely it is necessary to extend the advanced aspects in order to make the architecture suitable to the specific e-Government scenario. The reader should note that all the service architectures/SOAs (e.g., W3C and



**Figure 2** The components and (soft) services of SPCOOP.

ebXML/OASIS standards) need a neutral element, technically called *service directory*., with the goal to mediate between the different subjects cooperating for the service supply/use; the SPCOOP framework includes a set of infrastructural components to be used to simplify these operations (e.g., retrieving a service through automatic categorization, managing digital identities, etc). They are represented in Figure 2:

**Agreements Repository** is the software component used to register and to maintain the Cooperation/Service Agreements. It can be considered as the “database” of the cooperation. This component offers functionalities for the registration, the access, the update and the search of the agreements. The UDDI standard is the core of this component; however this standard does not offer all the required functionalities, therefore it has been extended.

**service agreement** A service agreement is a well-specified XML document that regulates the relationships of an application service between a supplier and a client in the following aspects: (i) service interface, (ii) conversations admitted by the service, (iii) access points, (iv) Service Level Agreements (SLAs), (v) security characteristics and (vi) descriptions of the semantics of the service. The formal and well specified nature of the service agreement has been done to support the development and the life-cycle of services in a (semi-)automatic way. Moreover, the public nature of the service agreement makes easier the establishment of domain ontologies that allows to aggregate services with similar semantics. Finally, in the context of a set of public administrations (i.e., a Cooperation Domain), services can be composed and orchestrated, thus generating other services described in turn by service agreements.

**Schemas/Ontologies Repository** is the software component offering functionalities to deal with the service and information semantics, in order to find out services that are more suitable to provide required functionalities. This component acts as a structure to store ontologies and conceptual schemas, offering functionalities of registration, access, update and reasoning on them.

**Federated Identity Management** is used to authorize and control the access to application services over SPCOOP; the federation is needed to reuse the already in-place identity management systems of regional and national authorities. Integration is to be done through specific interfaces supporting SAML v2.0.

**Monitoring Service** is in charge of monitoring the respect, by the different services, of the Service Level Agreements (SLAs) declared in the Service Agreements. Its development is planned for the future (i.e., it has not been included in the currently active tender), as standards and technologies for the definition and the enforcement of SLAs (e.g., WSLA or WS-Agreement) are not yet considered mature.

In addition to the previous components, a set of (soft) services, i.e., functionalities that need to be provided through different tools (either software or managerial) in order for the infrastructure to be effective, have been defined: (i) qualification services for both the repositories and the gateways, i.e., coded procedures for certifying that the components are compliant with the SPCOOP technical rules; (ii) the management of the whole infrastructure. The interested reader can refer to Baldoni et al. (2008) for additional technical details on the enterprise architecture.

#### 4.2 Federated Identity Management

Federated Identity Management is used to authorize and control the access to application services over SPCoop; the federation is needed to reuse the already in-place identity management systems of regional and national authorities. Integration is to be done through specific interfaces supporting SAML v2.0 [Carmignani and Ticconi (2008)]. The model takes three information domains into consideration: in the first one, the user of the service indicates the entity which requests the service, being the user either an application or a human user. The second information domain is denoted as "providing services domain" and it involves many different components, such as Service Providers, Identity Providers, Attribute Authority (for the validation of the attributes that are part of the user profile), External Attribute Authority (site that is not part of the federation, but that certifies external attributes, such as Professional Registry) and Profile Authority. In this domain there is the notion of Federation Gateway that is a logical part of the service provider component and represents the single point of contact for all resource accesses. Its role is to decouple the Service Provider authorization services and federation complexity, offering functionality of either "Proxy SAML" or "SAML Gateway". Also, it provides the end user with the list of possible certification entities for getting the service. The third information domain contains the infrastructural services to enable the cooperation in the previous information domains. The main components are authority registry (a register storing all the identity providers and all the profile's authority), attribute authority registry (a register storing relationships among roles and certifiers). Both of them create trust relationships among the identity providers and profile's authorities enabling previous information domains.

Many possible scenarios related to the architecture studied by SPC can be envisaged, let us show just some examples, the reader may refer to Carmignani and Ticconi (2008) for additional examples. It is possible to contact one or more Attribute Authorities to certificate attributes outside the assertion wallet presented by the user but necessary to achieve the authorization for using the service. If the user has already been authenticated in the front-end service, the front end service checks if the assertion wallet contains all the attributes necessary to invoke the service; to check if more attributes are necessary, it contacts the Attribute Authority Registry Service to get Attribute Authorities' URI for validation of the additive attributes. Once the attribute's set is completed, the request is sent. The back-end service verifies the authorization (Policy Enforcement) and provides the service.

### *4.3 Ongoing Projects on Federate Identity Management*

We will describe briefly three large national projects focusing on the usage of the FiDM system, namely the ICAR project, the National Land Registry Project and National Personnel Education Registry Project. The first is a pilot project while the second and the third are operative projects funded by the Italian Cabinet.

The ICAR project is made up of three different tasks, spanning from the application level to the infrastructure level [Pianciamore and Meschia (2008)]. The first task concerns physical and logical infrastructure enabling interoperability and cooperation between application services; the second task is about service level monitoring and assurance; finally, the third task is related to authentication and identity management services. In this project there is no a single global authority, but there are different authorities, each one that may certify subsets of attributes related to a certain subject; the same attribute could be certified by different authorities. Here accessing a service means that there shall be an interaction with trusted identity Providers in order to obtain a token authentication; then the attribute retrieved shall be certificated by authorities that could be even different. Profiles enable attribute aggregation, because a profile is a view on the user attribute set, a user profile contains attributes and corresponding certified values, each attribute in a profile is linked to a specific certifying authority.

The National Personnel Education Registry is a system that manages service and salary information of 1.5 millions public administration employees that work in the Education area from primary to high schools of the Italian educational system. At the time of this writing each of the 18.000 schools located in Italy has the possibility to join the federation with two accounts. In a few years every employee from Professors to Staff will have the own account. The federation is formed among the Ministry of Economics and the Ministry of Education that in its turn has a local authority one for each of the 109 provinces in Italy. A user authenticates itself with the local authority of the Ministry of Education, then through SAML interfaces it can authenticate to the central system of the Ministry of the Public Administration and then to the Ministry of Economics to get the personal information. The project aims to reduce the delay concerning the preparation of the monthly salary form for each public administration employee and to allow on-line consultation of this information to employees. This delay is currently two months.

The National Land Registry is a system that, among the others, register title to land in Italy and record dealings (for example, sales and mortgages) with registered land. This registry is maintained by the Italian Land Register Agency. The service provided

by the registry is deployed over the 109 Italian provinces and each province has an average of 10 offices in the province territory. The principal aim of the Land Registry is to maintain and develop a stable, effective land registration system, to guarantee title to registered estates and interests in land and to enable confident dealings in property and security of title by providing ready access to up-to-date and guaranteed land information. In order to provide this service a federation of Identity is needed to join together all the local offices of the Agency needed to feed the system with updated information. Also the federation has to include professional categories like notaries, lawyers etc as well as other PA institutes, e.g., Tax Agency, Ministry of Justice etc, that need to browse this information with the necessary level of privacy. The National Land Registry uses the FIDM functions of Web Browser Single Sign On (SSO) Profile. The federated system authenticates the user while the authorization profile is verified in the Italian Land Register Agency system.

#### *4.4 Comparison with other Countries*

In the previous sections we have showed how some countries are affording the problem of identity federation management, the table shown in Figure 3 briefly summarize this comparison.

In one of the rows of the table it is also reported the e-readiness ranking of the countries considered in the table. Note that this ranking takes into account not only technical details such as interoperability, identity management etc, but also Connectivity and technology infrastructure, Digital Divide, Business Social and Cultural environment, Legal environment, Government policy and vision and Consumer and business adoption. Data are reported from Economist Intelligence Unit (2007). From the Table it can be seen that each country has adopted a SAML-based approach to Federated Identity Management and even that digital certification is used almost in each country (the only exception is New Zealand). Some countries have developed a portal such as UK, Denmark and Austria, while others did not have followed that solution yet. Denmark is the first country adopting a user-centric portal, namely MyPage Denmark (2009); Nielsen (2007, 2008). Austria introduced a system based on NationalID, that has not been yet used in the other countries we have examined.

As far as Italy is concerned, SPCOOP represents an important asset for innovation for the whole country. Interestingly around SPCOOP several communities have emerged to realize evolving versions of the framework and to create a SPCOOP “culture” in the PAs. Such a community is led by administrations, with the active participation of industries and universities. However, at the time of this writing, SPCOOP lacks of a clear governance of the e-government framework. There is as an example no repository, as for the other countries, where all documents related to the e-Government framework are stored and regularly updated in the context of a clear long-term vision. Additionally, no other country seems to look into the problem of quality of service in telco infrastructure as Italy does in the context for example of SPC. Other countries only regulates interoperability between processes and data while leaving to the administration the burden of managing internet connections. Quality of service in telco infrastructure is definitely an important issues but probably restricted to some specific network of the public administrations, bringing this to all the public administrations is most likely an overkill.

It is also interesting to remark that the Mediterranean PA tradition focus more on federation and interconnection of back offices belonging to different PAs rather than

		<b>New Zealand</b>	<b>United Kingdom</b>	<b>Austria</b>	<b>Denmark</b>	<b>Italy</b>	<b>Hong Kong</b>
<b>Technical Issues</b>	<b>Portal/Dashboard</b>	available	available (government portal)	Available (government portal)	Available (citizen portal)	Available (government portal)	available
	<b>Employment of SAML</b>	requirement	Not a requirement	Not a requirement	requirement	requirement	Recommended from 2009
	<b>Digital Certifies</b>		available	available	available	available	Available
	<b>NationalID</b>			Available			Available
	<b>Third party attribute certification</b>	Foreseen in the next release	Available	Not available	Not available	Available	Recommended from 2009
	<b>Focus on telco technologies for egov</b>	No	No	No	No	Yes	No
<b>Organizational Issues</b>	<b>Dissemination of information</b>	web site available with all specs/vision	web site available with all specs/vision	Multilingual web site available with all specs/vision	Web site available with all specs/vision (in Danish)	Information spread out (little information available in English)	Multilingual web site available with all specs/vision
	<b>Infrastructure based vs user based</b>	User-based	User-based	User-based	User-based	Infrastructure-based	Infrastructure-based
	<b>Government interoperability Framework</b>	New Zealand e-Gif Standars	Transformational Government ; UK GovTalk	Promoulged under the Austrian egov act	Defined through a collaboration agreement	Decree Law	defined
<b>e-readiness ranking 2007</b>		14th	7th	11th	1st	25th	4th
<b>Public Administration Tradition</b>		Anglo-Saxon (Australia)	Anglo-Saxon (Europe)	Continental European	Scandinavian	Mediterranean	Anglo-Saxon (Chinese)
<b>Size (Est. population in 2009, millions)</b>	<i>Large (&gt;20)</i> <i>Medium (5-20)</i> <i>Small (&lt;5)</i>	small	large	medium	medium	large	medium

**Figure 3** Country-by-country approaches to Federated Identity Management.

including immediately the citizen in the loop. This is in contrast with Anglo-Saxon and Scandinavian PA tradition where the citizen is usually put at the center of PA innovation.

## 5 Conclusion

This paper reviewed the notion of Federated identity management in the particular context of e-Government. The paper has reviewed most important approaches to Federated IdM systems and surveyed the technical choices taken by some countries representing all major Public Administration tradition, namely Anglo-Saxon, Scandinavian, Mediterranean and Continental EU. The paper has also discussed the specific case of the Italian Enterprise Architecture explaining the process that prepared the definition of such architecture. The technical choices taken by Italy in FIdM has been also discussed and motivated by presenting some ongoing large projects.

As final remarks, we can notice that despite the diversity in PA traditions all countries we examined converged towards the selection of SAML as the way to federate identities. For a subset of these countries, this is actually a requirement. One point that needs definitely additional research is the interaction among FIdM and organizational structure of the federated organizations. All these Federated IdM approaches are indeed based on the assumption that syntax and semantic for each attributes is known during the design time of the federation. This becomes a killer issue in practice when setting up a federation particularly when the number of organizations increases. A sort of data Integration Approach, typical from database systems, should be applied in FIdM to map attributes and roles of one organizations into another one. These organizations can indeed have different schemas on distinct organizational structure. This means passing from FIdM to organizational interoperability.

## Acknowledgments

The author would like to thank all the persons involved in the working groups that have contributed to the development of SPCOOP, and in particular Francesco Tortorelli and Stefano Fuligni of CNIPA. The author is indebted with Francesco Tortorelli and Luca Nicoletti (Ministry of Economics) for sharing information concerning the National Land Registry Project and National Personnel Education Registry Project respectively. The author is also grateful to Massimo Mecella with whom he shared most of the work defining the service agreement framework in SPCOOP. Finally the author would like to thank the anonymous reviewers for suggestions and comments that greatly improved contents and presentation of the paper.

## References

- Austria (2009), [www.digital.austria.gv.at](http://www.digital.austria.gv.at)
- Baldoni, R., Fuligni, S., Mecella, M., and Tortorelli, F. (2008) 'The Italian e-Government Enterprise Architecture: A Comprehensive Introduction with Focus on the SLA issue', *Proceedings of the 6th International Symposium on Service Availability*, pp.1–12.
- Baldwin, A., Casassa Mont, M., and Beres, Y., and Shiu, S. (2008) 'Assurance for Federated Identity Management', *HP Labs Technical Report 2008-25*".

- Carmignani, A., and Ticconi, N., (2008) "Federated identity management service model in Italy (in italian)", *Servizio Pubblico di Connettività e Cooperazione*".
- Denmark (2009), [www.denmark.dk](http://www.denmark.dk)"
- Economist Intelligence Unit (2007) 'The 2007 e-readiness rankings Raising the bar', *The Economist*.
- Goodner, M., Hondo, M., Nadalin, A., McIntosh, M., and Schmidt, D., (2007) 'Understanding WS-Federation' [msdn.microsoft.com/en-us/library/bb498017](http://msdn.microsoft.com/en-us/library/bb498017).
- Gottschalk, P., and Solli-Saether, H. (2008) 'Stages of e-government interoperability ', *Electronic Government, an International Journal*", Vol. 5, No.3 pp. 310 - 320.
- Greenwood, D., Dempster, A.P., Laird, N.M. and Rubin, D.B. (2007) 'The context for Identity Management Architectures and Trust Models', *Proceedings of the OECD Workshop on Digital Identity Management*.
- Hommel, W., and Reiser, H. (2005) 'Federated Identity Management: Shortcomings of existing standards', *IFIP/IEEE International Symposium on Integrated Network Management*".
- Hommel, W., and Reiser, H. (2005) 'Federated Identity Management in Business to Business Outsourcing', *Proceedings of the 12th Annual Workshop of HP Open View University Association*".
- Interoperability Framework Coordination Group (2008) 'Analysis Underpinning The HKSARG Interoperability Framework Recommendations (Version: 7.0)', *Office of the Government Chief Information Officer of Hong Kong*.
- Liberty Alliance Project (2008) [www.projectliberty.org](http://www.projectliberty.org).
- Lips, M., and Pang, C. (2008) 'Identity Management in Information Age Government Exploring Concepts, Definitions, Approaches and Solutions', *Technical Report of the Victoria University of Wellington*".
- McKenzie, R. and Crompton, M. (2008) 'Use Cases for Identity Management in E-Government', *IEEE Security and Privacy*".
- Mecella, M., and Batini, C., (2001) "Enabling Italian E-Government through a Cooperative Architecture", *IEEE Computer*, 34(2): 40-45.
- Microsoft Passport (2008) <http://support.microsoft.com/kb/277759/en>.
- New Zealand e-government (2008) [www.e.govt.nz](http://www.e.govt.nz).
- Nielsen, S.P. (2008) 'Federation of the Danish Public Sector' [www.projectliberty.org](http://www.projectliberty.org).
- Nielsen, S.P. (2007) 'A Review of the Danish Public Sector Federation' *Burton Group Catalyst Conference*.
- Openid (2008) [www.openid.net](http://www.openid.net).
- Pfitzman B., and Waidner M. (2003) 'Federated Identity Management Protocols- Where User Authentication May Go', *In 11th Cambridge International Workshop on Security Protocols*".
- Pianciamore, N., and Meschia, F., (2008) "'ICAR-INF3: inter-regional identity federation in Italy', *2nd European Identity Conference*".
- Recordon, D., and Reed, R., (2003) 'OpenID 2.0: A Platform for User-Centric Identity Management', *Proceedings of the second ACM workshop on Digital identity management*, pp.11-16.
- Reddick, G. C. (2009) 'Management support and information security: an empirical study of Texas state agencies in the USA', *Electronic Government, an International Journal*", Vol. 6, No.4 pp. 361 - 377.
- Security Assertion Markup Language (2002), [www.oasis-open.org/security/docs](http://www.oasis-open.org/security/docs).
- Shibboleth (2008) <http://shibboleth.internet2.edu>.
- Taylor, J., Lips, A., and Organ, J., (2007) 'Information intensive government and the layering and sorting of citizenship', *Public Money and Management*".
- E-Government Unit (2005) UK Government Gateway.

e-Government Unit (2005) 'e-Government Interoperability Framework Version 6.1', *UK Cabinet Office*.

Windley, P.J., (2005) 'Privacy Enhancing Identity Management', *Digital Identity*", O'Reilly.

WS-Federation (2009), <http://www.ibm.com/developerworks/library/specification/ws-fed/>"