FedCohesion: Federated Identity Management in the Marche Region

Serenella Carota[2], Flavio Corradini[1], Damiano Falcioni[1],
Maria Laura Maggiulli[2], Fausto Marcantoni[1], Roberto Piangerelli[2],
Alberto Polzonetti[1], Barbara Re[1], and Andrea Sergiacomi[2]

[1] Computer Science Division
School of Science and Technologies
University of Camerino
62032 – Camerino (MC), Italy
firstname.lastname@unicam.it

[2] P.F. Sistemi Informativi e Telematici
Regione Marche
60125 – Ancona (AN), Italy
firstname.lastname@regione.marche.it

Abstract. Federated identity management is a set of technologies and processes supporting dynamically distribute identity information. Its adoption in Public Administrations maintains organizations autonomy giving at the same time citizens support to access the services that are distributed across security domains.

In this paper, we propose the Marche Region experience for what concern federate identity management focusing on the regional authentication framework, named FedCohesion. It is bases on Security Assertion Markup Language standard and it results from Cohesion re-engineering. It is the old style legacy authentication framework. We first present resulting architecture showing supported identification process and pilot applications. Lessons learned and opportunities have been also presented.

1 Introduction

Identity management represents a critical issue both in public and private sectors. There are many reasons for solving such problem among the others the implementation of e-government services (such as cross-border services provision) in order to enable true mobility for citizens and freedom of movement for business within the single market. It is clear that citizens are the main beneficiaries, however thanks to public private partnership services could work on an interoperable basis. For citizens, who are also consumers and employees, the integration is potentially attractive. At the same time this could contributes to the success of companies and to the increasing adoption of fully interoperable customized and high-value e-government services.

Since many years both European and national governments recognize identity management as a problem. This is recently confirmed by Europe 2020 strategy

A. Kö et al. (Eds.): EGOVIS/EDEM 2012, LNCS 7452, pp. 112–124, 2012.

[1] and related flagship initiatives such as the Digital Agenda for Europe [2]. Implementing the Stockholm Program the European action plan underlines the importance of an European strategy on identity management, including the need of legislative proposals on criminalization of identity theft and on electronic identity and secure authentication systems [3].

Focusing on e-government, identity management is a clearly addressed precondition [4]. In order to satisfy the application of mature European Interoperability Framework [5] moving from organization centric identity management to a federate identity management model [6] is a need. It is stated that the role of federation increases over the time mainly due to the ability of support independency among Public Administrations (PA) too often stressed by different political points of view [7].

Several architectures, technologies and projects related electronic identity management have been developed in Europe [8] [9]. In Italy there is a quite heterogeneous scenario that takes advantage of the already defined national interoperability framework [10] [11]. The most comprehensive example is given bu Secure idenTity acrOss boRders linKed[1] (phase I and II). It contributes to the realization of a single European electronic identification and authentication area establishing interoperability of different approaches at national and EU level, electronic identity for persons, electronic identity for legal entities and the facility to mandate.

Each Italian Region contributes from a bottom up perspective as the main actors in innovation policy making aimed at promoting applied research, innovation and technology transfer programs [12]. Regions develop their own innovation plans, although these need to be approved by the national government to ensure that they are in line with national policies. The regions have political and organization autonomy and at the same time they can aggregate and support local Public Administrations too often not suitable to be self-sustaining.

Among the others Marche Region has developed its own innovation plan. In order to adopt innovation actions an important aspect that we underline is the territory over which the Region spreads out, as it embraces both the high mountains environment of the Apennines, characterized by small towns with a low density of population, a large hill area, where the valleys are full of craft work, and the coastal area, where the most part population and of the industrial development lies. The governance and the technological choices are certainly influenced by the heterogeneity and diversity implicitly represented in the Region. So, working as a community it is an important aspect to spread digital society in such territory as well as to improve the interactions with other PAs outside of the Region and to contributes to the development and the use of fully interactive services. Innovation plan passes troughs IT supporting infrastructure such as those related digital identity. Marche Region reviews its identity management framework, named Cohesion, in order to support federate identity management. The novel framework, resulting from the re-engineering steps, is named FedCohesion. Its application is suitable to enable the creation of a community to

[1] https://www.eid-stork.eu/

support the great number of small and medium PAs and their relationships with citizens and businesses as well as other central PAs and Regions.

In this paper we present the Marche Region experience regarding federate identity management discussing technical and organization issues that drive the re-engineering step from the old style legacy system to the novel and more interoperable authentication framework. Here we will focus on the adopted design choices. As a result lessons learned from the application of a federate identity management system are presented.

The rest of the paper is organized as follows. The next Section presents European and national scenarios on federate identity management, whereas Section 3 introduces technical background. Section 4 presents the starting point in the Marche Region in term of authentication. Section 5 describes the innovation process that engages the Marche Region toward the adoption of FedCohesion. Some development issues are also introduced. Section 6 presents federation into practice. Concluding remarks and further development are discussed at the end of the paper.

2 Digital Identity from Europe to Marche Region

Federate identity management in Europe presents a quite heterogeneous scenarios [9]. It is not the case that every country decided to adopt a federated approach to identity management according to the culture and their relations with the local governments. For the countries that start such process (i) from the organizational point of view there is systematic approach starting from a reference framework to a communication plan and (ii) from technical issues the employment of Security Assertion Markup Language (SAML) [13] is a common requirement.

In Italy the adoption of European Interoperability Framework passes trough the definition of a national interoperability framework for applicative cooperation, named SPC-SPCoop [10] [11]. It represents a bottom-up approach till the adoption with Law decree of the Digital Administration Code. Focusing on federated identity management it is used to authorize and control the access to services over SPC-SPCoop. The federation is needed to reuse the already in-place identity management systems of several regional and national authorities. In such context the biggest project was Interoperability and Applicative Cooperation among Regions (ICAR). It started in June 2006 with 17 partners including 16 of 19 Italian Regions. The ICAR project was co-funded in the second phase of the Italian e-government plan for regionals and local authorities, which addresses the establishment of the so-called SPC-SPCoop. Among the others the project aims as following: “to establish the secure interconnection of regional Public Administration networks following the rules of SPC-SPCoop”. This gives the opportunity to the Regions to start an innovation and shared process for what concern federate digital identity.

Starting from ICAR project several Italian Regions reviewed their policies and systems for digital identity. As an example we cite Umbria Region where a platform has been created for the management of authentication, identity and roles from a federated viewpoint among the various bodies of the Region and with a view to inter-regionals connections within the ICAR platform. At the same time the identity provider for the citizens of the Lombardy Region provides the local bodies in Lombardy with a uniform and standardized infrastructure supporting the identification of users when they seek to access the services delivered by the local bodies. All the other Regions are going in similar directions, but for space reason [14], we cannot cite all of them.

In Marche Region digital identity means organize all the preconditions in order to support citizens to be on-line. Marche Region implements a citizens oriented community considering the municipalities, provinces, health organizations, etc. share common technological enablers and organizational process. This means provide to the community digital identification instruments, personal communication tools and authentication framework. The Region adopts a digital identification instrument such as “Carta Raffaello”, a Regional Service Card. It is a microchip-based card distributed to citizens living in the Marche Region. It is an ideal authentication tool for e-government and e-health services according to the national standard and the requested security levels. “Carta Raffaello” constitutes not only an electronic identification document, but also a certificate of digital signature for the authentication of electronic documents. It is already distributed to regional citizens via Local Registration Authorities. At the same time Marche Region delivery Certified Electronic Mail (Italian acronym PEC, “Posta Elettronica Certificata”) named “Posta Raffaello”. It is an e-mail system, which allows dispatching electronic documents that have legal value and which confirms the dispatch and delivery of electronic documents. It supports citizens digital interactions with Public Administrations. For what concern the authentication framework Marche Region proposes FedCohesion resulting from a re-engineering step of the old style Cohesion framework as following presented. The framework integrates several applications. Just to cite a few we refer to:

Dodibox is a framework able to plan, realize and access to on-line form;

Sigfrido refers to the digitalization of the procedures related to European regional development found in order to avoid manual data input for founds assessment;

SIAR aims to introduce common rules and tools for the agricultural community in order to give them the possibility to apply for European Commission founds according to the regional development program;

CoMarche supports public and private employers in the communications with the centre for employment related to new job, extension of work period or firing;

GIUSTO enables on-line communications related to creation, sign, transmission, storage, verification and confirmation of documents submitted by regional employees requesting holidays, temporary absences, etc.

Summing up, Table 1 proposes some data regarding diffusion of digital identity device and services in the Marche Region.

3 Technical Background

Identity Management systems involve at least two types of entity, namely Identity Providers (IdP) and Service Providers (SP). An IdP is an entity in charge of user authentication and of managing all identity relevant information concerning users. An SP, on the other hand, is responsible for the specification and enforcement of the access control policies for the resources it offers. Federated identity management is a set of technologies and processes that let computer systems dynamically distribute identity information and delegate identity tasks across security domains [7].

As a result of the federation, organizations are now able to create identity-based cross-border applications. It can also offer users cross-domains Single Sign-On (SSO), which lets them authenticate once and thereafter gain access to protected cross-boundary resources. With SSO users can use the same authentication credentials for a seamless access to federated services, within one or multiple organizations. The notion of federated identity has been recently extended to include not only users login names, but also user properties, also referred to as user identity attributes.

From a technological point a view there are several standards that support federated identity making administrations partnership-ready [9]. We can cite Microsoft Live ID, Security Assertion Markup Language, Liberty Alliance, Information cards and WS* and OpenID. In particular, SAML defines the user credential (assertions) format that will give to an authority the possibility to assert something regard a subject, without take in consideration the specific authentication methods. The fact that a second authority recognizes or not such assertion depends on the trust with the first one. The standard also defines the protocols to be used to send this assertion, the binding and the profile. It defines also the metadata structure that guarantees trust relationships between federated authorities.

Table 1. Diffusion of digital identity in Marche Region (From 2007 to 2011)

Raffaello Card	
Number of distributed card	45.000
Help desk interactions (in a month)	175
Number of Local Registration Authorities	145
Raffaello Mail	
Diffusion	46.000
Help desk interactions (in a month)	75
Number of Sended PEC	274.000
Number of Received PEC	301.000
FedCohesion	
Number of Users in the Registry	61.000
Number of Integrated Systems	50

4 Cohesion Regional Authentication Framework

Since many time Marche Region supported authentication via a homemade framework named Cohesion. The framework guaranties different levels of security, as following presented.

- Level 1 = User ID and password (identity is based on what the users knows). It is the most common and simple authentication system to administrate, it offers a lot of advantages, for example it does not need special hardware devices but it also presents many disadvantages, the association between the identity of people and authentication data is not guaranteed. Typically, this method is used to trace the activity of the user (profiling) and it grants a low protection level services access.
- Level 2 = User ID, password and personal code (identity is based on what the consumer knows and a further security code). It is an authentication system that has a security level higher than the system above described. In this case, a further security code is assigned to the requester that must use to access the service.
- Level 3 = Smart cards (identity is based on what the consumer own). It is an authentication system based on physical support that guarantee the association between real identity and authentication data into smart cards. The security level can be further increase by a personal code that ensures the person from loss and robbery.

Cohesion provided intra-organization Single Sign-On functionalities and Profiling services. SSO permits regional employees, in a transparent way, to access to the reserved areas of the portals secured by the framework without the needed of authentication every time making authentication credentials and user profiling available to different application domains. Indeed, the user authentication verification is delegated to the Cohesion service; it validates the profile in respect to the access role. Profiling system is dedicate for the coordinated management of information on the users with credentials, logically divided in a static and in a dynamic subsystem, containing a series of attributes able to indicate the preferences of the user when accessing the services rather than informative areas on portals. A part of the attributes that compose the user base profile is requested during the registration in one of the portals, and another part is communicated after explicit request when a service is used.

In term of architecture Cohesion is composed by two main elements (Figure 1): the SSOLibrary, which implements the SP functionalities at service level, and the Cohesion IdP guarantees user authentication exchanging encrypted data with the SSOLibrary using a proprietary exchange protocol. In particular, the IdP have two main modules: Cohesion SSO that takes care of retrieving the user profile and manage the Single Sign-On functionalities, and System Authenticator (SA) that is responsible to check user credentials and authenticate the requester.

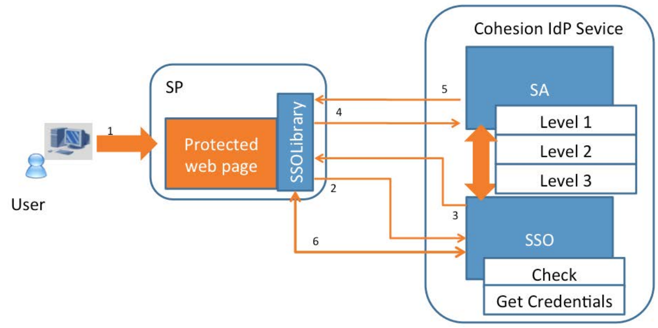

Fig. 1. Cohesion Architecture

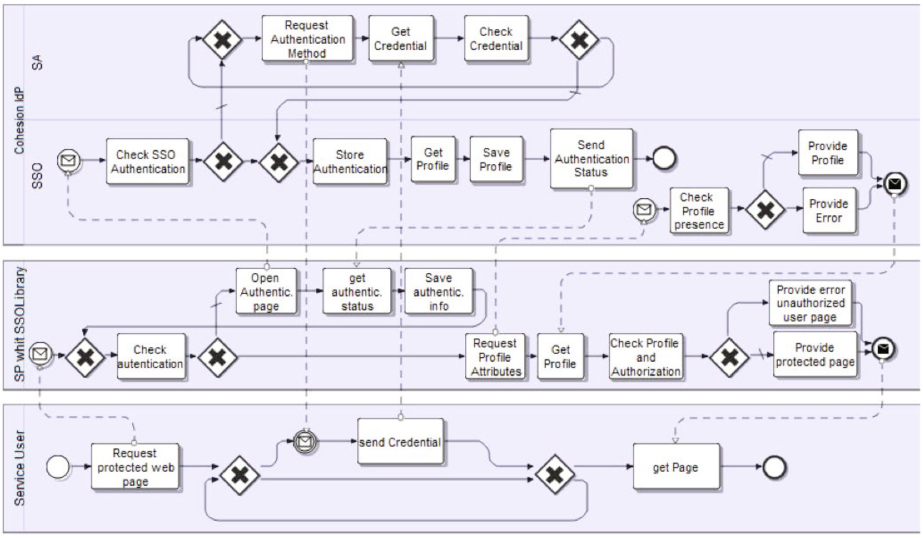

Fig. 2. Cohesion Process using BPMN language

According to such architecture authentication flow is following organized (Figure 2):

1. The user asks for a service secured by Cohesion;
2. The SSOLibrary receives such request and it interacts with SSO in order to check if the user is already authenticated;
3. The SSO gives back to the SSOLibrary the ID session, if the user is already authenticated the process go to the step 6 otherwise go to the step 4;
4. The SSOLibray forwards the authentication request to SA;
5. The SA gives back to the SSOLibray session ID;
6. The SSOLibrary using the session ID asks for credential via a secured channel and obtains it in order to give access to the service.

Even if several advantages are available mainly due to the mature and well tested Cohesion infrastructure, the main disadvantage is the lack of support regarding standards for federation. This is a need for the Marche Region in order to be in the wide community. Cohesion does not rely on SAML neither on other standards for federation, rather than it guarantees Single Sign On functionalities through an ad hoc flow secured by Microsoft Web Services Enhancement. The proposed scenario gives the ground to a re-engineering resulting in the FedCohesion framework as following described.

5 From Cohesion to FedCohesion

During the years Marche Region have made substantial investment on Cohesion framework so the choice of re-engineer prevailed over substitution with others framework SAML 2.0 compatible like Shibboleth [15] [16]. The main objective of the re-engineering step was moving from a legacy system to the SAML based [13] in order to support federation. It is important to underline that the upgrade to the standard SAML was made starting from zero, based on the standard XSD definition, without rely over existing commercial or open solutions. Resulting architecture is show in Figure 3.

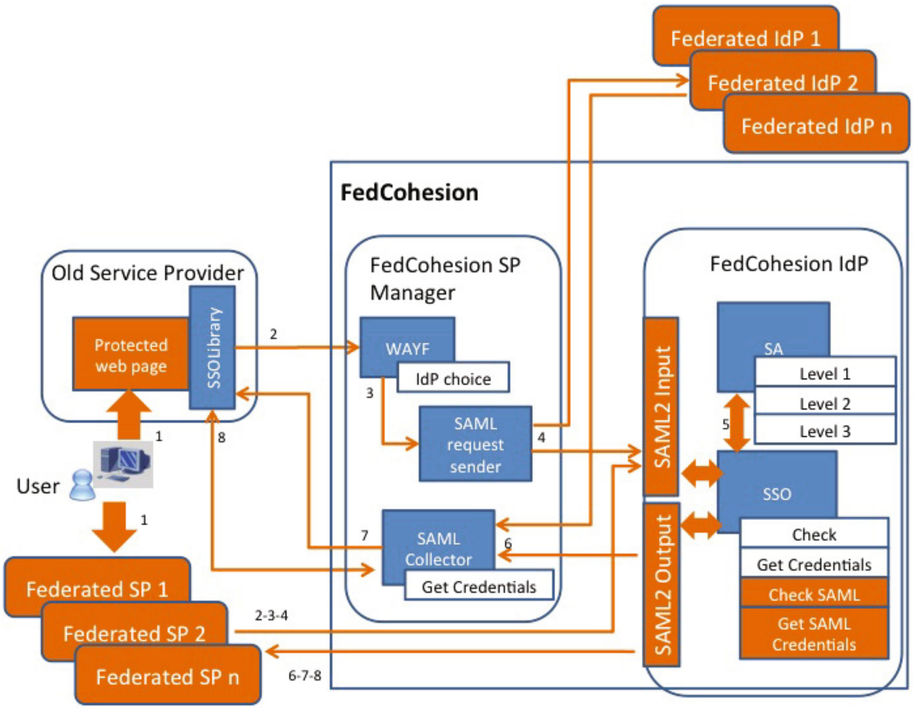

Fig. 3. FedCohesion Architecture

From an architectural point of view starting from a feasibility study, we realize that the easiest solution is propose a new SSOLibrary in order to support SAML standard and add two modules at the site of IdP to manage SAML requests and responses. Such ideal scenario fails if we consider backward compatibility. With this solution every service provider has to reinstall and reconfigure the SSOLibrary, so we decide to review the solution.

To reach the federation objective and be in line with regional requirements we decide to design and develop a module to centrally manage the old Service Providers that integrates the SSOLibrary and introduces specifics components to support SAML requests and responses. This module implements decoupling functionalities between the old Service Provider and the novel SAML based Fed-Cohesion IdP. The SAML collector converts IdP SAML response in the format supported by SSOLibray. Moreover to made the SSOLibrary ablest to work with the new environment we have replicated, in the Service Provider Manager, some interfaces already available in the Cohesion IdP such as Get Credentials functionality. The SAML request sender converts input requests from SP to SAML format. In order to fully and properly support functionalities, metadata are created for each component (IdP and Service Provider Manager). We also introduce ad hoc input-output interfaces for FedChoesion IdP. They are able to manage SAML input requests, convert them to the format internally recognized, and give back the user profile in the SAML response format. In particular, we have implemented Single Sign-On and Single Log-Out Protocols as part of the SAML Core standard.

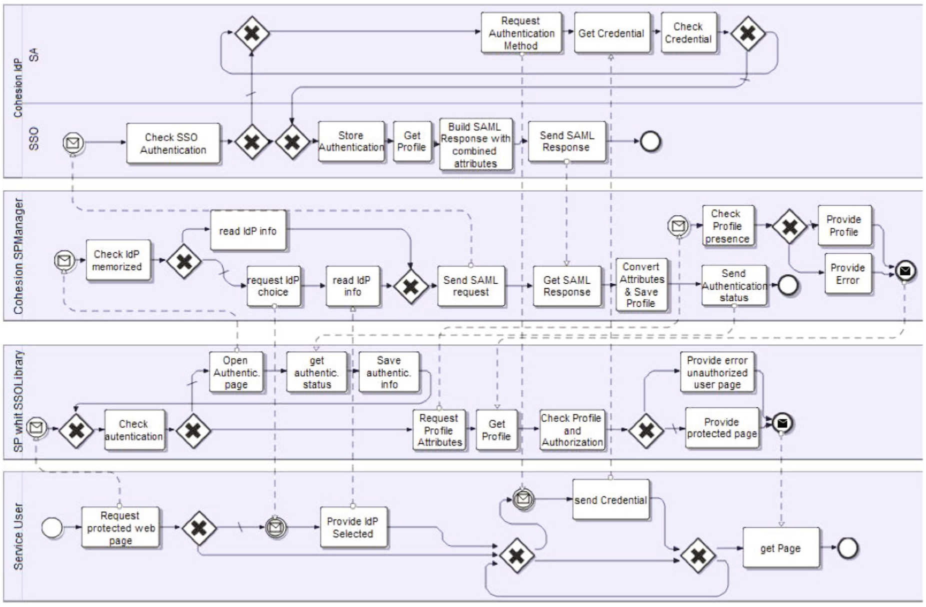

Fig. 4. FedCohesion Process using BPMN language

According to such architecture authentication flow is organized as following (Figure 4):

1. The user asks for a service secured by FedCohesion;
2. The SSOLibrary forward the request to the "Where are you from?" page where the user chose the IdP suitablest to authenticate him/her;
3. The "Where are you from?" page gives the control to the SAML manager that creates a SAML request and send it to the IdP;
4. If the IdP chosen by the user is FedCohesion him/her is redirect to the SAML request control page and SSO evaluate if session ID;
5. If session ID is available the process go to the step 7;
6. The control is redirected to SA where the user can choose a way to authenticate him/her;
7. SA gives the control to SSO that register the authenticated user and gives back the SAML response to the SAML Collector module that evaluates the response and if it is correct convert the credential into the SSOLibray compatible format;
8. SAMLCollector sends to SSOLibrary the session ID and call GetCredential functionalities;
9. The SSOLibray calls back the functionality GetCredential and it obtains the credentials, so that the user is authenticated and he/she can access service.

As already mentioned the proposed solution makes transparent to old service providers the re-engineered result. Thanks to the centralized metadata configuration all the old service providers can take advantage of the new functionalities, like federation, still using the old SSOLibrary. As a consequence the Service Provider Manager acts on behalf of such old service provider. So, every Service Provider that communicates with the Service Provider Manager must be registered and authorized by the Region that plays the role of technological intermediary and administrator respects to the authentication system governance.

In order to recognize and authorize external authorities in the community, both the IdP and the Service Provider Manager in FedCohesion share a common metadata where all the information regarding the federation is placed. As an affect if we add one more IdP, it will appear in the "Where Are You From?" page where the user asking for a resource can choose the federated authority suitable to support his/her authentication.

In order to be consistent respects to future development a novel version of SSOLibray is also available it works over SAML standard implementing the same core protocol used in the Service Provider Manager. Also in this case federation management is centralized with distributed metadata management for each SP.

6 Federations into Practice

FedCohesion represents an opportunity for PAs in the Marche Region, it can be reused by all the PA and make federation a reality in the Marche community as an authentication framework based on strict legal bases. The framework serves

82.247 citizens interacting with PAs for different services. FedCohesion functionalities have been successfully tested with well know Italian federations: IDEntity Management (IDEM) of the GARR network and INF3 federation of the Italian National Region resulting from the national ICAR project.

IDEM is an Italian federation born mainly to give professors, students and researchers a single way to access services provided by academics authorities. Many Italian universities have taken part as other research institutes, becoming one of the biggest Italian federation. Thanks to the close relationship between Marche Region and University of Camerino we decide to start such process and we conclude successfully compatibility tests. To pass the test FedCohesion profile attributes where update in order to support *LDAPv3*, *Cosine*, *inetOrgperson*, *eduPerson* attributes.

The INF3 task of ICAR project was born to add federation support for the other tasks INF1 and INF2 about applicative cooperation. It introduces in the authentication framework the concept of portfolio that is a SAML ready attribute manager, logically places between the IdP and the SP. This give the user the possibility to choose which attributes, obtained from IdP, want to send to SP and merge attribute obtained from different IdP, in a single SAML assertion. This gives the user the possibility to protect their privacy (the user know what info he share) and reduce redundant user data over different IdPs (the user attribute is present only on the authority that can certify this attribute). To made this functionalities work in FedCohesion we have integrated the INF3 software component in order to act as SP from the point of view of FedCohesion IdP and as IdP from the point of view of the FedCohesion SP. So when the users call a service protected by FedCohesion it will be forwarded to this component, than to the IdP, then back again to this component and finally to the SP that will authorize or not the user to access the resource.

7 Conclusion and Future Work

In this paper we present the experience of the Marche Region for what concern federate identity management. The solution presents several advantages. On one site it reduces the wide phenomenon of identity proliferation implementing the sharing principle. On the other site it enables interoperability among administrations in the Marche Region and it supports cross-administrations service delivery. Moreover it opens the ground to wide federations both at Italian and European level.

In the future we are planning to maintain and evolve the current version of FedCohesion improving its adoption. A comparative study made with Shibboleth the de facto standard architecture for the SAML protocol show some areas of improvement in our framework. Full support of SAML protocols is analysed and planned with reference to attribute authority and SOAP binding. The integration with INF3 software component shows overlapping functionalities with the service Provider Manager. Both have a decoupling function and we intend to join and implement all the INF3 functionalities directly in FedCohesion Service Provider Manager Module.

Finally, in the last years we recognize an increasing practice in the use of social network credential to access different kind of services provided by different entities. As an example we cite that using Google or Facebook credentials is it possible to access a lot of service. In the next future this could be a reality also for PA services in the Marche Region community thanks to the capabilities of FedCohesion. This may contribute to close the gab between availability and use of e-government services. As matter of fact, even if they are developed and provided using up-to-date technologies, they are not so widely used by citizens. Many official European Union statistics, such as those provided by Eurostat, generally testify such a situation. On the other site there is a wide diffusion social network among citizens. Citing some Facebook data as an example, after 7 years from its creation 600 millions are the users registered in the social network all over the world. In Italy the users registered in Facebook are 18 million versus 25 million that are the Italian Internet users. So we believe that the integration between e-government and social network could be a way for PA to be as close as possible to the citizens.

References

1. Communication from the commission to the European Parliament, the Council, t.E.E.: Europe 2020: A european strategy for smart, sustainable and inclusive growth. Technical report, European Commission, Brussels (2010)
2. Communication from the commission to the European Parliament, the Council, t.E.E., Committee, S., the Committee of the Region: A digital agenda for europe. Technical Report 245, European Commission, Brussels (2010)
3. Communication from the commission to the European Parliament, the Council, t.E.E., Committee, S., the Committee of the Region: Delivering an area of freedom, security and justice for europe's citizens action plan implementing the stockholm programme. Technical Report 171, European Commission, Brussels (2010)
4. Reddick, C.G.: Management support and information security: an empirical study of texas state agencies in the USA. EG 6(4), 361–377 (2009)
5. European Commission: European Interoperability Framework (EIF) Towards Interoperability for European Public Services (2011)
6. Lips, M., Pang, C.: Federated identity management systems in e-government: the case of italy. Technical report, Victoria University of Wellington (2008)
7. Maler, E., Reed, D.: The venn of identity: Options and issues in federated identity management. IEEE Security & Privacy 6(2), 16–23 (2008)
8. Fioravanti, F., Nardelli, E.: Identity management for e-government services. In: Digital Government. Integrated Series in Information Systems, vol. 17, pp. 331–352. Springer, US (2008)
9. Baldoni, R.: Federated identity management systems in e-government: the case of Italy. Electronic Government (2012)
10. Baldoni, R., Fuligni, S., Mecella, M., Tortorelli, F.: The Italian e-Government Service Oriented Architecture: Strategic Vision and Technical Solutions. In: Proc. of 6th International EGov. Conference, pp. 79–88 (2007)
11. Baldoni, R., Fuligni, S., Mecella, M., Tortorelli, F.: The Italian *e*-Government Enterprise Architecture: A Comprehensive Introduction with Focus on the SLA Issue. In: Nanya, T., Maruyama, F., Pataricza, A., Malek, M. (eds.) ISAS 2008. LNCS, vol. 5017, pp. 1–12. Springer, Heidelberg (2008)

12. Uyarra, E.: What is evolutionary about ‘regional systems of innovation’? implications for regional policy. Journal of Evolutionary Economics 20, 115–137 (2010), doi:10.1007/s00191-009-0135-y
13. OASIS: Security assertion markup language, SAML (2002)
14. ForumPA, CISIS: RIIR rapporto sull’innovazione nell’italia delle regioni 2010 (2010)
15. Pfitzmann, B., Waidner, M.: Federated identity-management protocols. In: Security Protocols Workshop, pp. 153–174 (2003)
16. Morgan, R., Cantor, S., Carmody, S., Hoehn, W.: Federated security: The shibboleth approach. EDUCAUSE Quarterly 27(4) (2004)