

# Digital Identity into Practice: The Case of UniCam

Damiano Falcioni, Fabrizio Ippoliti, Fausto Marcantoni, and Barbara Re

Computer Science Division  
School of Science and Technologies  
University of Camerino  
62032 – Camerino (MC), Italy  
{damiano.falcioni,fausto.marcantoni,barbara.re}@unicam.it,  
fabrizio.ippoliti@studenti.unicam.it

**Abstract.** Identity management is a set of technologies and processes supporting identity information. Its adoption in Public Administration, in particular in the domain of university, maintains organization autonomy giving at the same time students and staff support to access the services that are delivered. In this paper we present a project lead by University of Camerino with the Italian Banking Group UBI and the Namirial Certification Authority. The project consists in the issue of Enjoy my UniCam card allowing users to have, on a single physical card, several functionalities about facilitated banking account, university services and digital signature certificate. First results about the testing phase are presented as well as the next steps of the project.

## 1 Introduction

Over the time, managing personal identity on-line has become a serious issue. It has become increasingly important in terms of personal security, partly because organisations are now highly networked when it comes to information. Digital Identity (ID) is spread among different organisations. Small amounts of information cannot reveal enough about people to impact on us in a negative way but, when using the internet extensively, we can find several more information than expected [1]. So, depending on the context, person may be represented by different “partial identities”. For example, a person may use one or more partial identities for work and others in spare time, e.g., with the family, doing sports, or dealing with companies like a bank, an Internet service provider, or a supermarket [2].

The project is based on a prepaid card named “Enjoy”, that made possible the creation of a project led by University of Camerino (UniCam)<sup>1</sup> in collaboration with the Italian Banking Group UBI and the Namirial Certification Authority. This initiative has also made possible the creation of a digital scenario “Enjoy Ecosystem”, resulting from a collaboration of five Italian universities and

---

<sup>1</sup> <http://www.unicam.it>

many UBI local branches. Aim of the paper is to present the UniCam experience in digital identity management (IdM). The goal is to create a card for students, faculty and administrative staff that allow you to have, on a single physical card, several functionalities such as bank services, academic services and digital signature, letting the owners to save time and increase their satisfaction toward the university. The “all-in-one” solution has been chosen to guarantee safety, privacy and trust.

In order to complete the project, several issues have been addressed and solved. From the political point of view, the project is a valuable means of bringing innovation in UniCam. About the legal point of view, it also allowed the adoption of the Italian Digital Administration Code. For what concerns the organisational issues, an agreement was signed among UniCam, Italian Banking Group UBI and Namirial Certification Authority, it regulates terms and conditions in order to achieve the whole project objective. Finally, about the technical aspects, a new system was implemented. It is integrated with all the other existing infrastructures in the university, supporting different technologies. For instance, to set data flows among stakeholders, some web services have been implemented and SFTP (Secure Shell File Transfer Protocol) server has been integrated. Finally, from the administrative point of view, the use of Enjoy My UniCam card allows a remarkable simplification of the paperwork.

Section 2 presents a brief state of art about eID solutions in Europe and in Italy. Section 3 discusses the whole Enjoy my UniCam card project, with a deep description of actors, system architecture and processes. Section 4 introduces all the features of the card. Section 5 describes the services available with Enjoy my UniCam card. Finally, Section 6 concludes the paper.

## 2 Background: Digital Identity from Europe to UniCam

Over the years smart cards are being increasingly applied in the Public Administrations (PA). They provide great value to the use of services and they provide users identification and authentication.

For what concerns the eID solutions, limiting our analysis to government initiative, the European situation shows as the most adopted ones are implemented with smart card technology [3]. The majority of the European eID smart cards are national ID cards (in 13 countries) or tax cards. 6 other countries have already planned similar initiatives. The second most popular choice is password-based system (9 countries). Less adopted solutions are based on One Time Passwords (OTP) or Mobile Subscriber Identity Module (SIM) cards. Furthermore, in some cases, PA is assisted by private companies or the initiative is only private. The most common services offered by the European eID solutions are about tax declarations, pension and healthcare. In most cases, it also offers to the user the possibility to digitally sign documents.

The European Commission, through the Community Research and Development Information Service, founded several projects about Digital Identity and related subjects. They are financed in the 6<sup>th</sup> and the 7<sup>th</sup> Framework Programme

funded by European Research and Technological Development respectively from 2002 until 2006 and from 2007 to 2013. In the 6<sup>th</sup> one, **FIDIS** (Future of Identity in the Information System, <http://www.fidis.net/>) was funded between April 2004 and June 2009. It aimed to integrate European research regarding technologies in order to support identity and identification; interoperability of identity and identification concepts; ID-theft, privacy and security; profiling and forensic implications. The achieved results regard integrated approaches to research; legal, socio-economic, usability and application requirements; public architecture and specifications. Further projects have been funded in the 7<sup>th</sup> Framework Programme such as: PrimeLife (Privacy and Identity Management in Europe for Life), GINI-SA (Global Identity Networking of Individuals - Support Action), DigIDeas and FutureID. Each of them has been funded by the ICT programme except DigIDeas which was funded under the programme IDEAS. **PrimeLife** (<http://primelife.ercim.eu/>) was funded from March 2008 to June 2011. It is the successor of the project PRIME (PRivacy and Identity Management for Europe, <https://www.prime-project.eu/>). PrimeLife mainly focused on: addressing the problem of digital footprints in the emerging Internet, in communities, and Web2.0 and through user-centric and configurable technology; making results of the projects PRIME and PrimeLife widely usable and deployed through standards, open source and education; advancing the state of the art about privacy and identity management. **GINI-SA** (<http://www.gini-sa.eu/>) was funded between June 2010 to May 2012. It aimed to investigate and establish the foundations for the architectural, legal, regulatory requirements, as well as the provisioning and privacy enhancing aspects, of a framework of user-centric identity management services. GINI-SA was based on the assumption that individuals, i.e. citizens, consumers, users of any related services, should be able to manage their own identity data and provide it in an open and flexible manner. The **DigIDeas** project (<http://www.digideas.nl/>), funded between October 2008 and September 2013, examines the social and ethical aspects of digital identities in the context of an increasingly digital world. The overall aims of DigIDeas are to increase understanding of the social and ethical aspects of digital identity management, to further theorize the concept of identity, and to contribute to the quality and social/ethical acceptability of technological developments. **FutureID** (<http://www.futureid.eu/>) is the most recent research project and it will finish in November 2015. The FutureID project builds a comprehensive, flexible, privacy-aware and ubiquitously usable identity management infrastructure for Europe, which integrates existing eID technology and trust infrastructures, emerging federated identity management services and modern credential technologies to provide a user-centric system for the trustworthy and accountable management of identity claims. Every stakeholder involved in the eID value chain, will benefit from the availability of a ubiquitously usable open source eID client that is capable of running on arbitrary desktop PCs, tablets and modern smartphones.

For what concerns more application oriented project we can refer the Information and Communication Technologies Policy Support Programme (ICT-PSP)

as part of the Competitiveness and Innovation framework Programme (CIP). They are SSEDIC (Scoping the Single European Digital Identity Community), STORK (Secure idenTity acrOss boRders linKed) and STORK 2.0 (Secure idenTity acrOss boRders linKed 2.0). **SSEDIC** (<http://www.eid-ssedic.eu/>), funded from December 2010 to December 2013, it is a network with the goal to provide a platform for all the stakeholders of eID, to work together and collaborate to prepare the agenda for a proposed Single European Digital Identity Community. The network will identify the actions and the timetable for the Digital Agenda and the successful launch of the European Large Scale Action, as well as to provide a multi stakeholder planning resource to assist its implementation. **STORK** project (<https://www.eid-stork.eu/>) was funded from June 2008 to June 2011. It implemented an EU wide interoperable system for recognition of eID and authentication that should enable businesses, citizens and government employees to use their national electronic identities in any member state. Project goals were: develop common rules and specifications to assist mutual recognition of eIDs across national borders; test, in real life environments, secure and easy-to-use eID solutions for citizens and businesses and interact with other EU initiatives to maximize the usefulness of eID services. **STORK 2.0** (<https://www.eid-stork2.eu/>), funded from April 2012 to April 2015, is going to contribute to the realization of a single European electronic identification and authentication area. It is based on the results of STORK, establishing interoperability of different approaches at national and EU level, eID for persons, eID for legal entities and the facility to mandate.

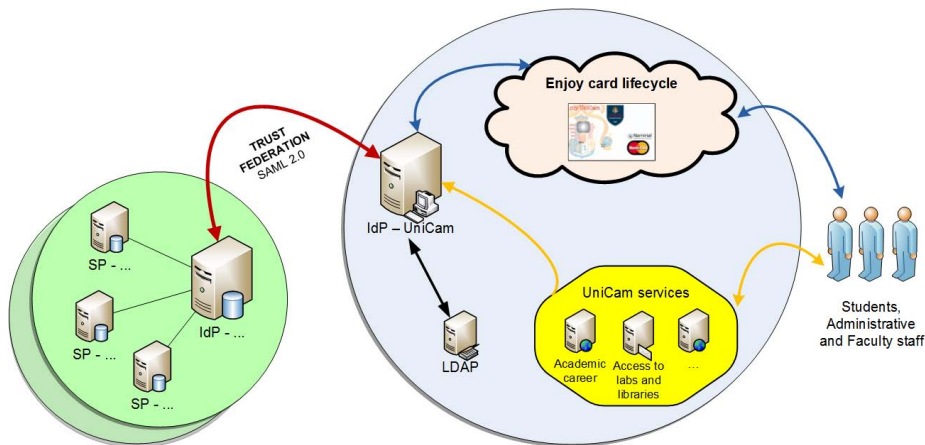
For what concerns the Italian scenario, we refer to the Italian Digital Administration Code. The National Card of Services (“Carta Nazionale dei Servizi” - CNS) and the Electronic Card of Identity (“Carta di Identità elettronica” - CIE) are the standards. In the last years, CNS model has been adopted by several Italian regions in order to realize Regional Card of Services (“Carta Regionale dei Servizi” - CRS) that are standard CNS. In most cases CRS are integrated with the Regional Health Card (“Tessera Sanitaria Regionale” - TS-CNS). At the end of 2012, regions have already been distributed to citizens over 20 million cards for access to services. The most massive distribution was of the Lombardy Region, which has completed distributing the card to all the population. The card are used to access health and government services such as enabling digital signatures. For what concerns identity enabling infrastructures, we cite ICAR (Interoperability and Applicative Cooperation between Regions) and IDEM (IDentity Management for federated access). **ICAR** project (<http://www.progettoicar.it/>) supports implementation of an interregional federated authentication system aimed to define and implement a federated authentication system at interregional level. **IDEM** (<https://www.idem.garr.it/>) is the first Italian Federation of Authentication and Authorization Infrastructure (AAI) involving Institutions of the scientific and academic community and service and content providers on the web. The main purpose of the IDEM Federation is to make easier and more secure user identification and authorization to access to the services in the university country. Thanks to the federated approach, successfully developed in the

ICAR and IDEM projects, users can more easily access to networked resources provided by different organizations [5][6].

### 3 Enjoy My UniCam Project

#### 3.1 Overview

Even if the paper focuses on the role of Enjoy My UniCam card, it's important to have a wider point of view considering the whole Enjoy My UniCam card project in Fig. 1. Every UniCam user can be identified and authenticated by the Enjoy My UniCam card. In this way, it's possible to benefit of the various services making available directly by UniCam. The basic idea allows to establish a trust federation, respecting the SAML 2.0 standard<sup>2</sup>, between UniCam Identity Provider (IdP) and IdP of other organisations. The infrastructure is based on Shibboleth<sup>3</sup>: an open-source project that provides Single Sign-On capabilities and allows sites to make informed authorization decisions for individual access of protected on-line resources in a privacy-preserving manner. The Shibboleth software implements widely used federated identity standards, principally OA-SIS' Security Assertion Markup Language, to provide a federated single sign-on and attribute exchange framework. By doing so, users of an organization can use the services offered by the new federated organization and vice versa. All data are managed in full compliance with current privacy policies. Some personal information are exchanged between different actors.



**Fig. 1.** The whole Enjoy My UniCam card project

<sup>2</sup> <http://saml.xml.org/saml-specifications>

<sup>3</sup> <http://shibboleth.net/>

### 3.2 Stakeholders

Following we sum up the main stakeholders involved in the project.

- University of Camerino is the services and cards provider, it manages control and data flow.
- UBI is a banking group which has a wide coverage, with about 1,800 branches, on the whole national territory. It assigns an International Bank Account Number (IBAN) to each person requesting Enjoy My UniCam card, offering its banking services. The group is also responsible for the emission of the card. About control and data flow management, UBI performs some operations in order to obtain and exchange data flows with UniCam and Oberthur.
- Oberthur is a company and it deals with the creation and issuance of personalized cards, according to the explicit applicant request and after obtaining the confirmation that the applicant has the right to get the card.
- Namirial Certification Authority is a computer company and web engineering that has found its own specific place in the field of IT and it's one of Certification Authority recognized by Italian Public Administration. In the project, Namirial is responsible for the issuance, management and termination of the digital signature certificates.

The stakeholders exchange information between their systems, according to the architecture represented in Fig. 2, where it is possible to see also the components diagram of the system.

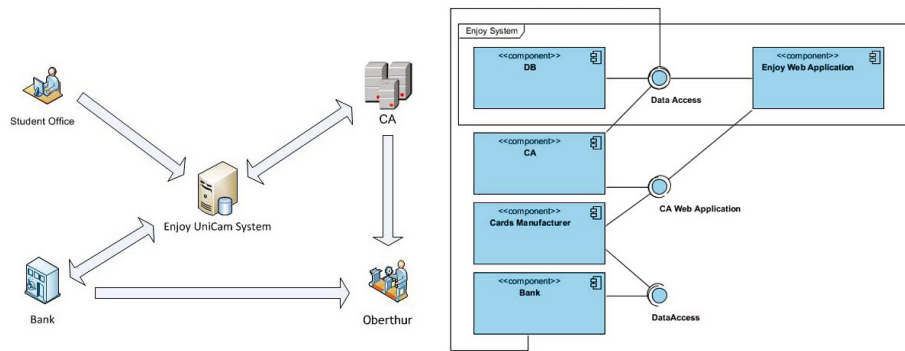
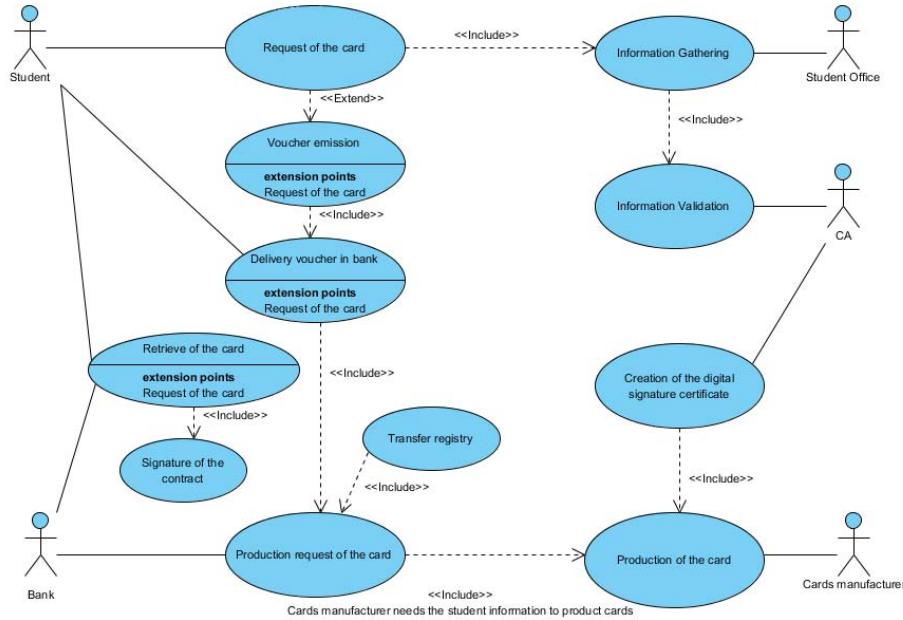


Fig. 2. Enjoy My UniCam system architecture and component diagram

### 3.3 Implemented Process

Following the main business process supported by Enjoy My UniCam, in Fig. 3 we provide the use cases diagram of every processes about the process to obtain the card.



**Fig. 3.** Use cases diagram about request, emission and delivery of the card

**Request of the Card - Student Office.** For the students interested in the Enjoy My UniCam initiative, Student Office collects the students data and their pictures to be used for the card production. During the registration phase, UniCam uses the Namirial web portal to insert the student data, which performs the necessary checks of formal correctness. Based on these data, Namirial produces digital signature certificates and makes them available to Oberthur. Finally, the Student Office issues a voucher to present to the bank, which proves to be eligible for the card request. The voucher is recognized by UniCam and UBI like an official document.

**Request of the Card - Bank Branch.** The student goes to a branch authorized to issue cards, presenting the voucher given to him/her by UniCam during request phase. The bank employee collects the voucher and performs the following tasks:

- Identification of the users and insertion his/her data in the system;
- Request of the card in the system;
- Ask the student to subscribe the necessary contracts;
- Notifies the student when approximately the card will be ready and also that he/she will receive an envelope containing the Personal Identification Number (PIN) and the invitation to come to the branch to get the card.

Every day, via the SFTP server, UBI provides UniCam a file with a list of requests for cards issuance. UniCam acquires via SFTP the file, completes with

the additional information and for each record includes a photograph to be printed on the card. According to UBI needs, UniCam adds in the photograph file properties the information about the fiscal code and the IBAN assigned to the holder.

**Production of the Card.** UBI transmits the requests, the personal data necessary for the production of cards and photographs of the owners to Oberthur, which performs the following activities:

- Customization with UniCam logo, Namirial logo and photo of the owner;
- Insertion of digital signature certificates in the cards, that are available on the Namirial web portal.

When the card is produced, on behalf of the UBI shipping office, Oberthur sends:

- The cards to the bank branches from which the request was made;
- The envelopes containing the PIN and the notification that the card is available in the bank, to the students' home address.

**Activation of the Digital Signature Certificate.** The issuance process of digital signature certificates involves the following steps:

- Namirial concludes a LRA agreement (Local Registration Authority)<sup>4</sup> with UniCam for the issuance of signature devices;
- Namirial provides UniCam of its web portal, with which a UniCam application refers to validate the data of the applicant;
- After the UniCam registration is complete and, data has been validated from Namirial web application, digital signature certificates are made available for Oberthur, without UBI participation;
- Oberthur loads the digital signature certificates on the cards, realizing the customization and sends them to the UBI branches.

**Delivery of the Card.** When the card and PIN have been produced, the student receives at his/her home address the PIN and the invitation to go to the bank branch to receive the card. When the student is at the office, he/she was handed the envelope containing the card and the delivery device signature module. The student signs the module and UBI sends it via mail to Namirial. Every day Namirial will call a procedure to communicate to UniCam the information acquired. At this point Namirial sends directly to the students' home address PIN and Personal Unblocking Key (PUK) of the digital signature certificate.

**Reissue of the Card.** In case of theft or loss of card, the student must:

- Request the freezing of money services in the way specified in the contract documents: that is calling the customer service or going directly to the bank branch;

---

<sup>4</sup> An LRA (Local Registration Authority) is an agent of the Certifying Authority who collects the application forms for digital signature certificates and related documents, does the verification and approves or rejects the application based on the results of the verification process.



- Request the freezing of digital signature certificate, as specified by Namirial in the documentation attached to the envelope containing PIN and PUK;
- Go to the Student office to request the release of a new voucher with which to present the replacement request of the card at the bank branch, in order to maintain the same IBAN;
- Go to the bank branch where the student originally requested the issuance of the first card, showing the new voucher. In this way the replacement request is processed as a standard procedure for a new Enjoy My UniCam card.

The process then follows the normal process of issuing a card. The voucher is a prerequisite, without which the student can't request the card. It's the only document obtained from the Student Office, certifying the students have the right to become cardholders.

**Early Extinction of the Card.** If a student loses the right to ownership of the card (e.g. in the case of drop-out), the Student office must inform the student that, before closing the relationship with the University, he must go to the bank branch to return the Enjoy My UniCam card, according to the usual banking regulations about the extinction of the cards.

## 4 Device

Starting from the basic information that can be found on any prepaid card, Enjoy My UniCam card has some customizations. On the front, the card is personalized with the UniCam Logo, Namirial logo and the holder photograph. On the back, instead, the card has only one customization: an indication of the code needed to handle the blocking activity of digital signature certificates.

The card used for the project is a card produced and commercialized by Oberthur Technologies<sup>TM</sup>, named *ID-One Cosmo V7*. All interfaces of communication are available: it can be used in the following ways: Dual, Contact (Interface ISO 7816 T=0/T=1), Full-Contactless (ISO 14443 Type A and Type B).

Implementing Java Card<sup>TM</sup> and GlobalPlatform Industry standards and featuring on-board applications, it has been specifically designed for identity and government market needs. It implements the most recent cryptographic mechanisms implemented, such as 3DES, AES, RSA and Elliptic curves. It also has 128 KB of free memory to load applications, as the UniCam services.

Anyone can understand how many risks need to be addressed in a project of this size, but the first and the most important one is about security. In particular, digital signature certificates, having legal value, must not be altered. This is the reason why the ID-One Cosmo card has been used, it's the only one to satisfy very high security standards.

- **Common Criteria EAL5+:** The *Evaluation Assurance Level* (EAL1 through EAL7) of an IT product or system is a numerical grade assigned following the completion of a Common Criteria security evaluation, an international standard in effect since 1999. The EAL5+ grade means the ID-One

Cosmo has been certified as “Semiformally Designed and Tested”. As a result, we obtain that, even if an untrusted application were loaded and run, safety won’t be compromised as the digital signature certificate remain valid.

- **FIPS 140-2 level 3:** The *Federal Information Processing Standard* is a U.S. government computer security standard used to accredit cryptographic modules. The standard provides four increasing, qualitative levels of security intended to cover a wide range of potential applications and environments. The security requirements cover areas related to the secure design and implementation of a cryptographic module. These areas include cryptographic module specification; cryptographic module ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; design assurance; and mitigation of other attacks [4].

Compliance with these two international standards is a prerequisite for the legal value of the digital signature certificate. This is supported by Enjoy my UniCam card.

## 5 Supported Services

The card allows the students to have, in a single physical device, several functionalities, in different areas: bank and university services.

- **Bank services.** The card is technically a prepaid card with an associated IBAN. It is valid for 5 years and it has not fixed fee. It allows you to make the usual banking operations, with special facilitations, such as paying anywhere displaying the MasterCard™ symbol in Italy and abroad, making free withdrawals at every Bancomat cash machines in Italy, making and/or receiving transfers using home banking, paying bills and making RID payments and so on.
- **UniCam services.** The card allows the student to be recognized in UniCam facilities giving the possibility to access to laboratory and library, pay the meal at the canteen, register for exams, display and summary of the academic career, require internships and thesis, enrollment to university sports center.
- As already mentioned, the card contains a **digital signature certificate**, with legal value, with which you can digitally sign documents. In order to use the UniCam services about the request of particular documents or, for example, to require thesis, it’s possible to fill the document directly from your laptop and then, finally, sign it with digital signature certificate. In this way the document will have official and legal value.

UniCam also participates in the IDEM Federation. So organizations in IDEM become Identity Provider: identities of own users can be exchanged, providing appropriate safeguards and always respecting the privacy of users [7][8][9]. With Enjoy my UniCam card it will be possible, in every university or organization

participating to IDEM, to access to any service available such as libraries, logging in in computer labs, connecting to universities WiFi networks, which are often present in squares and public areas of faculties, and so on.

## 6 Conclusion and Future Works

In this paper we present the experience of the University of Camerino about the multi-services card. The adopted solution presents several advantages. On one hand, it avoids the possibility to have many and many cards to benefit different services. On the other, in term of identity federation it is part of community making advantages of related benefits.

Enjoy My UniCam card obtained good results during the testing phase, delivering over 330 cards in the first 9 months. The waiting time between the request and the final delivery has been about 15 days, that is a nice result considering the processing. In the next future, UniCam is going to activate several more services such as paying photocopies, coffees or snacks at the vending machines and about public transport service aiming to build up a smart campus.

## References

1. Hansen, M.: Me, Myself and I! Manage your IDs safely (2007)
2. Clauß, S., Köhntopp, M.: Identity management and its support of multilateral security. *Computer Networks* (2001)
3. Bour, I.: Electronic Identities in Europe - Overview of eID solutions connecting Citizens to Public Authorities. Technical report, Transaction Security (2013)
4. NIST: Security requirements for cryptographic modules. Technical report, National Institute of Standards and Technology (2001)
5. Eve Maler, D.R.: The Venn of Identity: Options and Issues in Federated Identity Management. Technical report, European Commission (2010)
6. Gaedke, M., Meinecke, J., Nussbaumer, M.: A modeling approach to federated identity and access management. In: WWW 2005 Special Interest Tracks and Posters of the 14th International Conference on World Wide Web (2005)
7. Carota, S., Corradini, F., Falcioni, D., Maggiulli, M.L., Marcantoni, F., Piangerelli, R., Polzonetti, A., Re, B., Sergiacomi, A.: FedCohesion: Federated Identity Management in the Marche Region. In: Kő, A., Leitner, C., Leitold, H., Prosser, A. (eds.) EDEM 2012 and EGOVIS 2012. LNCS, vol. 7452, pp. 112–124. Springer, Heidelberg (2012)
8. Morgan, R., Cantor, S., Carmody, S., Hoehn, W., Klingenstein, K.: Federated Security: The Shibboleth Approach. Technical report, EDUCAUSE Quarterly (2004)
9. Baldoni, R.: Federated Identity Management Systems in e-Government: the Case of Italy (2012)