

# Core Structure Elements Architectures to Facilitate Construction and Secure Interconnection of Mobile Services Frameworks and Advanced IAM Systems

Athanasios Karantjias and Nineta Polemi

University of Pireaus, Informatics Department  
80 Karaoli & Dimitriou Str,  
185 34 Pireaus, Greece  
karant@unipi.gr, dpolemi@unipi.gr

**Abstract.** The impressive penetration rates of *electronic and mobile* networks provide the unique opportunity to organizations to provide advanced e/m-services, accelerating their entrance in the digital society, and strengthening their fundamental structure. *Service Oriented Architectures (SOAs)* is an acknowledged promising technology to overcome the complexity inherent to the communication among multiple e-business actors across organizational domains. Nevertheless, the need for more privacy-aware transactions raises specific challenges that SOAs need to address, including the problems of managing identities and ensuring privacy in the e/m-environment. This article presents a targeted, user-centric scalable and federated *Identity Management System (IAM)*, called *SecIdAM*, and a mobile framework for building privacy-aware, interoperable, and secure mobile applications with respect to the way that the trust relationship among the involved entities, users and SOAs, is established. Finally, it analyzes a user-transparent m-process for obtaining an authentication and authorization token, issued from the *SecIdAM* as integrated in the IST European programme SWEB for the public sector.

**Keywords:** e/m-Federation, Identity and Access Management, Privacy, Security, Cryptography.

## 1 Introduction

Until now, XML technologies and *Web Services (WSs)* have been considered as the most appropriate approach for achieving interoperability, facilitating the communication among multiple e/m-business actors, across organizational domains. However, till recently these solutions faced many problems due to:

- The impediments to the delivery of bundled, context-sensitive services to end-users couldn't satisfy the desire of *Service Providers (SPs)* to develop and deliver user-centric, strong and secure identity services 1.
- The increasing regulatory compliance and audit requirements 2, which force SPs to consider a higher assurance level for user identity in e/m-provision of services, imposing the implementation of proprietary *Identity and Access*

*Management (IAM)* mechanisms with questionable levels of usability, manageability, and scalability.

- The fact that the mobile aspect is partially covered in these solutions.

*Service Oriented Architectures (SOAs)* encompass services that essentially implement business processes involving various actors. A major concern of these actors is related with the accomplishment of secure interactions. The satisfaction of the main dimensions of security (authentication, confidentiality, integrity, and non-reputation) has always been a vital issue when integrating large-scale enterprise solutions. The adoption of world-wide accepted standards such as XML Cryptography, *Public Key Infrastructure (PKI)* and *WS-Security (WS-S)* already provide viable solutions to create secure e/m-environments 3.

However, the need for privacy aware transactions raises specific problems that SOAs need to solve including the management of users' identities both in the electronic environment and the mobile one. The common practice is the adoption of privacy policies 45 as a means to imprint the capabilities and requirements of the entities participating in a SOA enterprise system. Nevertheless, privacy policies do not constitute a full identity handling solution on their own, since they do not implement or guarantee all the required identity management processes. Even if the research and industry communities have identified several identity management solutions that implement complete e-identity handling frameworks 46 nowadays a SOA designer has to identify the appropriate e/m framework that better suites the needs of his system, without introducing additional complexity to the design or leaving out important aspects of privacy management.

This article proposes a targeted, user-centric and federated IAM system, called *SecIdAM*, and a mobile development framework for building advanced m-services, with respect to the way that the trust relationship among the involved entities, users and SOA enterprise systems, is established enabling the user to e/m-access advanced business services. The proposed system *SecIdAM* has been implemented in the IST European programme SWEB 7. The rest of the paper is organized as follows: Section 2 presents existing IAM-solutions, models, and related work performed. Section 3 presents the *SecIdAM* and Section 4 presents an advanced mobile framework for building synchronous, privacy-aware m-applications. Section 5 presents the usage scenario, while Section 6 contains acknowledgements and Section 7 draws conclusions.

## 2 Existing Implementations and Related Work

Several solutions for managing and controlling end-user's access, permissions, and allowed actions to e-resources are already proposed by many projects and initiatives. According to their results, three main types of IAM-solutions were proposed. The first refers to account management and implements an *Authentication, Authorization, and Accounting (AAA)* infrastructure. Representative designs of this type are the *Liberty Alliance (LA)* 48 and the *WS-Federation* 69. LA creates a set of specifications (*ID-FF*, *ID-WSF*, and *ID-SIS*) for identity federation in network environments, ensuring interoperability, supporting advanced privacy, and promoting the adoption of its guidelines and best practices. *WS-Federation*, on the other hand, is a component of the *WS-Security* model, defines mechanisms for enabling different security domains

to federate by allowing and brokering trust of identities, attributes, and authentication between the WSs implemented.

The second type refers to user data profiling process, such as the detailed log files or data warehouses, which support personalised services and analyse user's behaviour. Finally, the third type is based on solutions for user-controlled, context-dependent role and pseudonym management.

Other projects and research initiatives 1011 propose and implement system architectures that reconcile privacy and accountability of users' e-interactions, distinguishing mainly two IAM-solutions:

- The *enterprise IAM-solutions*, in which data-control is exercised by the enterprise instead of the individual user.
- The *user-centric IAM-solutions*, in which the administration and control of identity information is placed directly into the hands of individuals, allowing users themselves to have full control of their personal information and preferences.

All these attempts aim to cover all possible cases, and therefore remain in a generic level. The facts that privacy and identity management, at the time that many of these solutions were deployed, were very innovative assets when building advanced e/m-enterprise systems, and the primitive status of core WSs standards, led to ineffective and rather closed IAM solutions 12.

In addition these solutions provide automated systems to SPs for managing identities, authentication and authorization, whereas do not adopt the user perspective, who needs to simplify his entrance in a large scale enterprise framework. Last but not least, the fact that the mobile aspect is partially covered imposes the replacement of these solutions with more synchronous ones.

### 3 Federated Identity Management System

Privacy in massively inter-connected environments and its social acceptance from end-users requires totally novel approaches to identity and privacy management 13, through trustworthy interfaces, taking into account multiple requirements such as anonymity, pseudonymity, linkability / unlinkability 14, and data protection regulations 1516 in place.

Our approach recognizes the need for broader e/m-business solutions, in which the notion of federation is expanded, and the relationship of each user with the overall framework is established, guaranteed and monitored by a trusted third entity. The user-centric *SecIdAM*, the architecture of which is depicted in Figure 1, undertakes the management of the partial identities and pseudonyms of all kind of users, as well as for the provision of proper asserted claims for accessing business services deployed in SOA oriented enterprise systems.

The *SecIdAM* consists of four different and district tiers, the *Interaction Tier*, the *Main Enterprise Tier*, the *Secondary Enterprise Tier*, and the *Middleware* one.

The *Interaction Tier* undertakes the establishment of communication with all external entities such as the e/m-users, and the enterprise systems of the SPs. This communication is based on WSs, processed from the *Web Service Manager*. The quality

of protection through message integrity, message confidentiality, and single message authentication, is provided through the use of WS-S mechanisms, the implementation and validation of which are undertaken from the *Message Security Manager*.

The *Main Enterprise Tier* implements the core authorization mechanisms. The *Service Handling* component handles all service calls into the enterprise and assigns specific events to other internal handlers and components. The XACML-based *Policy Enforcement 5* module specifies and enforces fine-grained, system-readable privacy policies, used to control access to WSSs, digital objects and services, enclosing users' preferences and *SecIdAM's* requirements.

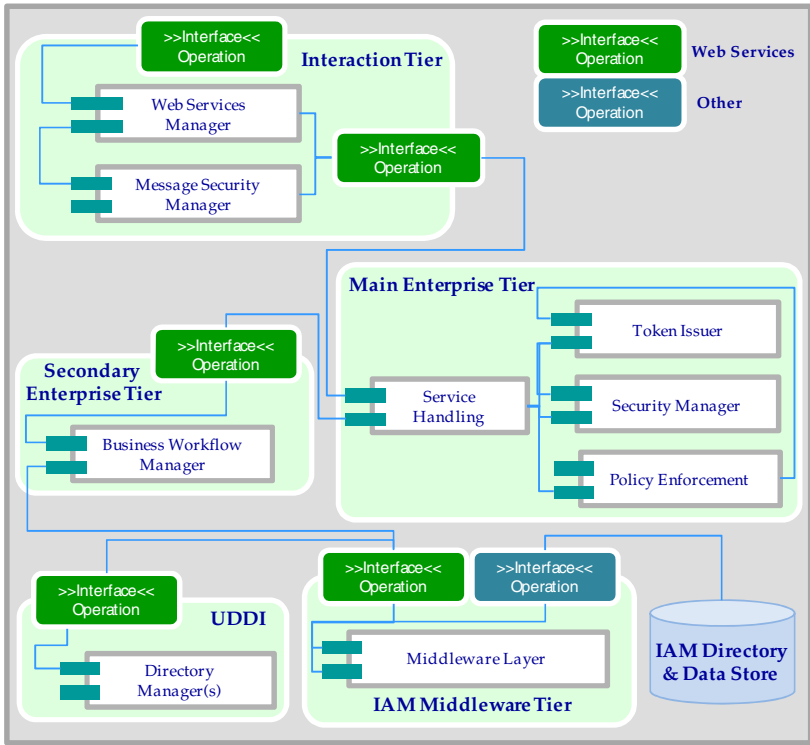


Fig. 1. Architectural overview of SecIdAM

Therefore, within this component an initial policy matching of the SPs' requirements with the users' preferences and capabilities and vice versa is achieved. The *Security Manager* module handles all security cryptographic credentials provided from a PKI, while it implements all the advanced security mechanisms on the *SecIdAM* such as the creation/validation of XML digital signatures and XML encryption and decryption.

The *Token Issuer* module issues XML-based security tokens, integrating the WS-Trust standard 21, providing authorization, and advanced auditing mechanisms. To maximize interoperability with clients and systems from multiple vendors, the *SecIdAM*

supports the WS-Federation and SAML 2.0 protocols 17. For higher administrative efficiency, it automates federation trust configuration and management, using the harmonized federation metadata format 18. This automation enables the *SecIdAM* and SPs to publish their federation metadata in a standard format, which can be exchanged between potential partners. Consequently, using a single specification that can support both passive web application and active WS requestors is a key advantage for effectively using this system in multiple and heterogeneous environments.

The *Secondary Enterprise Tier* manages the choreography of the core IAM system's services, implementing their business logic, defining and mixing human based actions, and creating business rules based on workflow data, through the use of *Business Process Management Notation (BPMN)* systems. It actually places a significant emphasis on all processes within the secondary enterprise tier of the system, both in terms of streamlining process logic to improve efficiency, and also to establish processes that are adaptable and extensible so that they can be augmented in response to business change 19. Our primary goal was to establish a highly agile automation environment, fully capable of adapting to change, which is realized by abstracting the business process logic into its own tier.

The *Middleware Tier* integrates all required interoperable mechanisms through the integration of an *Enterprise Service Bus - ESB* framework 20. This tier is actually a light weight messaging layer that uses disparate technologies, transports and protocols. Specifically this tier undertakes to communicate with a UDDI server or any other directory server, or even a single database server, which provides a set of services supporting the description and discovery of all businesses, and SPs, as well as the predefined policies, agreed between the *SecIdAM* and each SP separately. An optimum federated IAM system must give the capability to adopt and manage data structures from multiple and heterogeneous environments while not changing the implemented services. Therefore, the middleware tier operates as a transformation layer for every possible data that have to be inserted or exported from the *SecIdAM*.

## 4 Privacy-Aware Mobile Framework

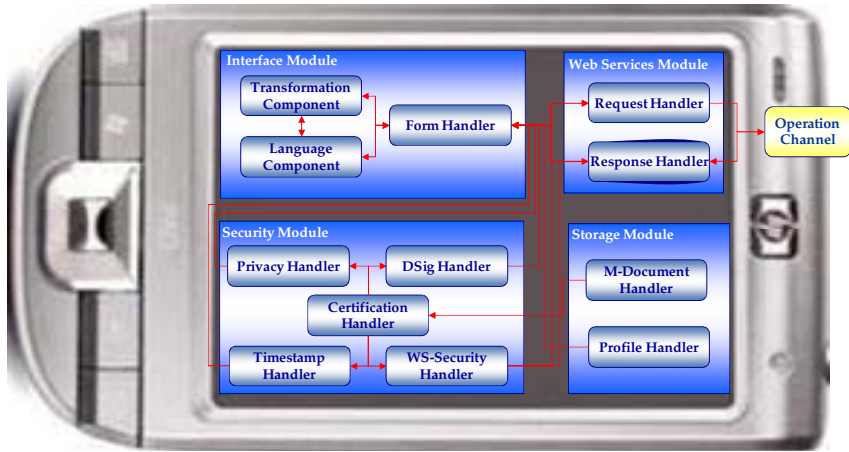
A shrinking workforce, combined with the need to deliver higher levels of service to key constituents is contributing to a requirement for federal organizations workers to use wireless networks and devices to perform mission-critical business functions at anytime, anywhere. A set of fundamental design principles, strategies and guidelines has to be clearly specified, addressed, built, and maintained in order catch common goals and benefits. The goals behind these principles are tied directly to some of the most strategic objectives of service-oriented computing:

- Allow for service logic to be repeatedly leveraged over time so as to achieve an increasingly high return on the initial investment of delivering the m-service.
- Increase business agility by enabling the rapid fulfillment of future business automation requirements through wide-scale m-service composition.
- Successfully address advanced m-privacy and m-security mechanisms.

Rather than embedding functionality that should be deployed across every specific m-service, the distributed m-architecture, depicted in Figure 2, offers secure, interoperable,

extensible and reusable WSs interfaces to application developers in order to easily expand the m-functionality and build upon it.

Our main focus, when designing and implementing this innovative mobile framework in SWEB project for the public sector, was to integrate essential functions that can be easily reused, configured and customized for every m-service offered through four core modules.



**Fig. 2.** Mobile Client Tier Architecture

The *Web Services Module* implements all formulation and handling mechanisms of the transmitted messages to external communicating entities through the *Request Handler*. It actually encloses all clusters of data into WSs, integrating as well the reception and extraction of the main body mechanisms, though the *Response Handler*, on every other end of communication.

The *Interface Module* implements the transition between m-forms, through the *Form Manager* during the process of user interaction, the selection and automated adjustment of language and character set on these forms through the *Language Manager*, and the transformation of the given data into a format compliant with the adopted XML schemas through the *Transformation Manager*.

The *Security Module* integrates strong security mechanisms on the mobile device, providing essential interfaces for achieving multilayer security (transmission, processing and storage). It creates and verifies XML digital signatures on the m-documents through the use of the *XML Security Manager*, which are automatically structured from the *Form Manager*, as well as the hash values of the signed m-documents and requests for valid timestamps (if needed) through the *Timestamp Manager*. All SOAP messages are digitally signed and encrypted from the *WS-Security Manager* using strong cryptographic credentials which are stored and handled by the *Certificate Manager*. Furthermore, it creates the appropriate requests for obtaining valid authorization tokens from the *SecIdAM* through the *Privacy Handler*, receives and handles them by automatically embedding them into messages to be sent to SOA oriented platforms.

Finally, the *Storage Module* stores and handles the created and received m-documents, through the use of the *m-Document Manager*, and the various profiles of users on the mobile device, activating the *Profile Manager*. Depending on each authenticated user on the application, many required fields (ex. name, surname, V.A.T. number, etc), are automatically filled on the m-forms.

The logic encapsulated in this m-framework by each service is associated with a context that is sufficiently generic and agnostic to all usage scenarios, so as to be considered reusable.

## 5 Usage Scenario of *SecIdAM*

There are several prerequisites for using the *SecIdAM* in a large scale framework for both end-users and SPs that operate one or more SOA oriented enterprise systems. First of all, the SP has to communicate with it and register all the e/m-services provided from its systems. This procedure requires the names of the services and the policies for e/m-accessing them as well as to build the profile of the SP. Consequently, each SP must define the roles for all kind of end-users, (e.g. “simple user”, “admin”, “employee”, etc) for each service and the required information provided from the end-user for obtaining these roles.

Moreover, the SP has to specify the exact URL in which the WSs for each business e/m-service listen. This URL is kept in the UDDI registry, with the name of the service and the WSDL description of the corresponding WS. The *SecIdAM* handles only information, which is required for assigning authorization roles to end-users. The UDDI registry undertakes the better organization of a large-scale enterprise framework, managing e-records for each e/m-service that the core IAM system doesn't need to be aware of. In addition all WSDL descriptions of the integrated WSs are stored in this registry.

On the other hand, each end-user has to create one or multiple profiles, providing his/her preferences that concern the information he/she wants to disclose in his/her transactions. Optionally, the user may provide a subset or all the required information, creating multiple profiles, which correspond to different roles. Specific authentication information and a pseudonym are bound to each of the above profiles. In addition to these, the user has to be registered at the PKI in order to obtain the required cryptographic credentials. These credentials have to be successfully installed in the mobile device, in which the mobile application operates.

The satisfaction of these prerequisites makes the user able to access the e/m-services offered from the SOA oriented enterprise platforms, following the sequence of steps depicted in Figure 3. These steps are totally transparent to the end-user, who doesn't need to be aware of all the advanced security mechanisms that run on every m-transaction.

The mobile application receives a request from the user, who has already specified the profile he/she wishes to use, to proceed with the authorization process. It creates a Request Security Token Request 22, embedding the preferred profile, the e/m-service that the user wishes to access and the name of the SP where this service is available. This request is embedded in a SOAP message and the application applies WS-S features on the message, ensuring that this request can only be processed from the *SecIdAM*.

The latter receives the request, and performs decryption on the message and validation on the XML digital signature. This process requires the communication with the PKI, which performs validation on the cryptographic credentials used. Under a successful validation the user is authenticated.

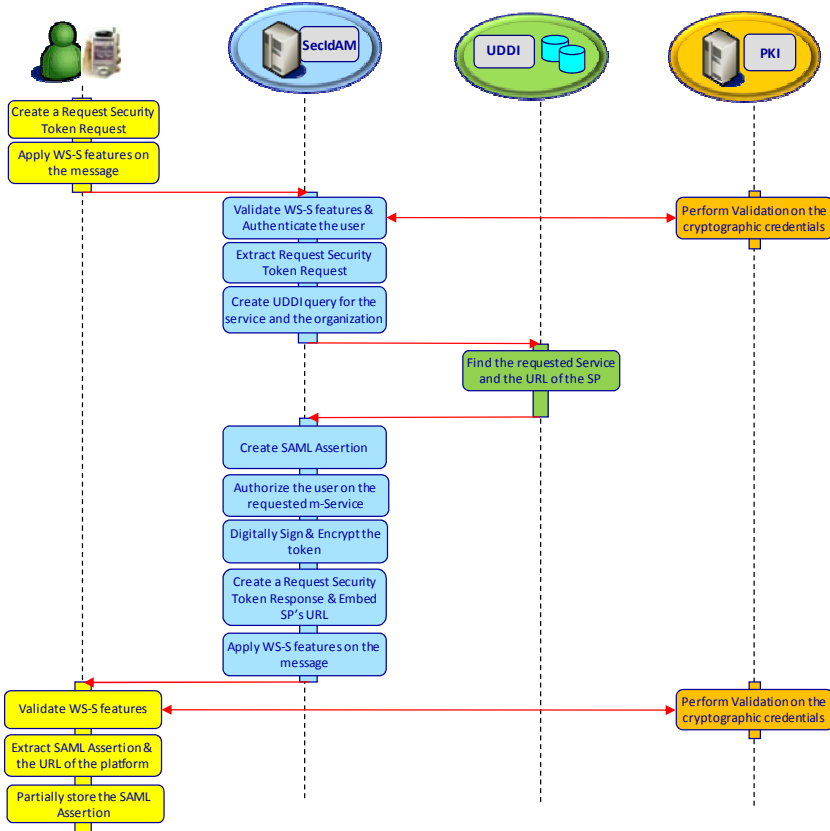


Fig. 3. Usage Scenario for obtaining a valid m-token from SecIdAM

The *SecIdAM* extracts the actual request and retrieves the name of the requested m-service, and the name of the SP. It then structures a query and submits it to the UDDI registry in order to get the appropriate record of the requested service on the given SP. Upon successful retrieval of this record, the UDDI returns the appropriate URL, in which the mobile application has to communicate and request the actual m-service, to the *SecIdAM*.

It receives the results and authorizes the user according the preferred profile, selected from the user, and the policies specified from the SP. After successful authorization, the *SecIdAM* creates a SAML assertion. This assertion has a specific validity period, which is actually specified from the SP, embeds the role of the end-user and a new pseudonym for him/her, ensuring his/her anonymity. The role assigned to the



user results from the information that he/she intends to release, and has been defined during the profile creation.

The *SecIdAM* digitally signs the assertion with its private key and encrypts it with the public key of the SP. Consequently, only this organization will be able to decrypt and further process this SAML assertion, which is required for the accomplishment of the authorization process on its SOA oriented enterprise system.

The next step requires the creation of *Request Security Token Request 22* in which the URL is embedded. The *SecIdAM* structures a SOAP message which includes the above response, applies WS-S features on it, and responds to the m-application.

The latter receives this SOAP message, performs decryption on it and validation on the digital signature. As previously this procedure requires communication with the PKI in order to ensure the validity of the credentials used. Under successful validation the mobile application extracts the encrypted SAML assertion and partially stores it in the mobile device, in order to embed it on the headers of the actual m-service request that will be submitted on the SOA platform. It also extracts the required URL in which the platform that provides the actual m-service operates.

## 6 Conclusions

Advanced SOAs are considered the most promising way to achieve complex communication among multiple e/m-business actors across organizational domain. However, the lack of strong security and privacy mechanisms, and the adoption of inefficient, insecure, and expensive enterprise identity management systems necessitate a large-scale innovation, across organizational boundaries and between public and private institutions, in which privacy and identity management will not be treated as generic problems.

Essentially, this paper intends to provide practical and comprehensive coverage of a synchronous enterprise, user-centric and federated IAM system, and a mobile development framework for building advanced privacy aware m-applications that can be implemented on a modular basis, designed and implemented in the IST European programme SWEB 7. These solutions encompass fundamental design principles such as interoperability, scalability & extensibility, privacy, security, and reusability, in order for large-scale frameworks to successfully solve problems arising from identity management, ensuring privacy awareness for each managed identity.

## Acknowledgements

The authors would like to thank the E.C. for its support in funding the SWEB project [7], and all the project partners.

## References

1. Bertino, E., Martino, L.D.: A Service-oriented Approach to Security - Concepts and Issues. In: Eighth International Symposium on Autonomous Decentralized Systems, ISADS 2007, Sedona USA, pp. 7–16 (2007)
2. Peyton, L., Doshi, C., Seguin, P.: An audit trail service to enhance privacy compliance in federated identity management. In: Proceedings of the 2007 conference of the center for advanced studies on Collaborative research, CASCON 2007, pp. 175–187. ACM, Ontario (2007)

3. Kaliontzoglou, A., Sklavos, P., Karantjias, T., Polemi, D.: A secure e-Government platform architecture for small to medium sized public organizations. *Electronic Commerce Research & Applications* 4(2), 174–186 (2005)
4. Liberty Alliance. Liberty ID-WSF Web Services Framework Overview, version 2.0 specifications, <http://www.projectliberty.org>
5. Papastergiou, S., Karantjias, A., Polemi, D.: A Federated Privacy-Enhancing Identity Management System (FPE-IMS). In: *Proceedings of the 18<sup>th</sup> Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, Athens (2007)
6. Lockhart, H., et al.: *Web Services Federation Language (WS-Federation). Version 1.1* (December 2007)
7. SWEB IST project, Secure, interoperable, cross border m-services contributing towards a trustful European cooperation with the non-EU member Western Balkan countries, Sixth Framework Programme, IST-2006-2.6.5, <http://www.sweb-project.org>
8. Liberty Alliance Project, Liberty Alliance & WS-Federation: A Comparative Overview (2003), <http://www.projectliberty.org/resources%20/whitepapers/>
9. Goodner, M., et al.: *Understanding WS-Federation, version 1.0* (2007)
10. PRIME Project, Privacy and Identity Management for Europe, European R&D Integrated Project under the FP6/IST Programme (2005), <http://www.prime-project.eu.org>
11. Meints, M., et al.: *D3.1: Structured Overview on Prototypes and Concepts of Identity Management Systems* (2005), [http://www.fidis.net/fileadmin/fidis/deliverables%20/fidis-wp3-del3.1.overview\\_on\\_ims.final.pdf](http://www.fidis.net/fileadmin/fidis/deliverables%20/fidis-wp3-del3.1.overview_on_ims.final.pdf)
12. Rieger, S., Neumair, B.: Towards usable and reasonable Identity Management in heterogeneous IT infrastructures. In: *10<sup>th</sup> IFIP/IEEE International Symposium on Integrated Network Management – IM 2007*, Munich, pp. 560–574 (2007)
13. Corradini, F., et al.: The e-Government digital credentials. *International Journal of Electronic Governance (IJEG)* 1(1), 17–37 (2007), <http://www.inderscience.com/filter.php?aid=14341>
14. Haddad, W.: Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology. Network Working Group, IETF Trust (2008)
15. Directive, Directive 97/66/EC of the European Parliament and of the Council of 15th December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector. *Official Journal L L 024, 0001– 0008* (1997)
16. Directive, Directive 01/45/EC of the European Parliament and the Council of Ministers on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. *Official Journal L 008, 0001– 0022* (2001)
17. SAML, Security Assertion Markup Language v.2.0 – Technical Overview. Working Draft 1.0 (2006), <http://www.oasis-open.org>
18. OASIS WSFED Technical Committee, *Web Services Federation Language Version 1.2*, OASIS, Working Draft (2008)
19. Pasley, J.: How BPEL and SOA Are Changing Web Services Development. *IEEE Internet Computing* 9(3), 60–67 (2005)
20. Mule Technical Committee, “Mule 2.0”, Release Candidate 2 (2008), <http://mule.mulesource.org>
21. OASIS Web Service Secure Exchange Technical Committee, *OASIS WS-Trust 1.3*, OASIS Standard (2007)
22. SWEB consortium, *D4.1: SWEB platform development report*, European Commission, Belgium (2008)