Introducing Infocards in NGN to enable user-centric identity management

Davide Proserpio, Fabio Sanvido, Patricia Arias Cabarcos, Rosa Sánchez Guerrero, Florina Almenárez-Mendoza,
Daniel Díaz-Sánchez and Andres Marín-López
Dept. Telematic Engineering, Carlos III University of Madrid
Avda. Universidad 30, 28911 Leganes (Madrid), Spain
http://pervasive.gast.it.uc3m.es
{dproserp, fsanvido, ariasp, rmsguerr, florina, dds, amarin}@it.uc3m.es

***Abstract*—With the rapid evolution of networks and the widespread penetration of mobile devices with increasing capabilities, that have already become a commodity, we are getting a step closer to ubiquity. Thus, we are moving a great part of our lives from the physical world to the online world, i.e. social interactions, business transactions, relations with government administrations, etc. However, while identity verification is easy to handle in the real world, there are many unsolved challenges when dealing with digital identity management, especially due to the lack of user awareness when it comes to privacy. Thus, with the aim to enhance the navigation experience and security in multiservice and multiprovider environments the user must be empowered to control how her attributes are shared and disclosed between different domains. With these goals on mind, we leverage the benefits of the Infocard technology and introduce this user-centric paradigm into the emerging NGN architectures. This paper proposes a way to combine the gains of a SAML federation between service and identity providers with the easiness for the final user of the Inforcard System using the well known architectural schema of IP Multimedia Subsystem.**

I. Introduction

IP Multimedia Subsystem (IMS) is a set of specifications that describes the Next Generation Networking (NGN) architecture to deploy IP based telephony and multimedia services. IMS defines an architectural framework for the convergence of voice, video and data using the session initiation protocol (SIP) [1] over an internet protocol (IP) based infrastructure. Besides, IMS is a solution to achieve multimedia and communication applications over SIP in a transparent way. IMS changes the way to access service by creating an application-oriented horizontal solution. Due to this fact together with the use of IP and SIP protocols, many operators have accepted IMS as the future network architecture. In a scenario where many operators interact and deploy new value added services we have to be able to provide them in a secure fashion among different network domains and independently of the network access. Furthermore we have to be able to protect the user interests and manage her identity as described in the 'Identity Laws' defined by Kim Cameron [2]. Apart from this, the user should be able to manage her own credentials and decide when to use them.

Many solutions based on the concept of Identity Federation have been proposed in the last year to handle these issues. Among them the emerging technology of information card tries to overcome the limitations of the actual identity management system and gives the users more control over their own information. This system has some limitations: no possibility of roaming without exporting *infoCards* to the new device and the user can only create and select an *infoCard* with credentials belonging to only one identity provider when in many cases this is insufficient. Besides, there are no implementation to integrate the information card paradigm into NGN architectures. To ride over these problems, in this article we propose the use of an identity management system (IdM) based on *infoCards* along with an NGN architecture to enable an user centric identity framework in an interdomain scenario. Our solution allows users to create an information card to gain access to a service using "multi-Idp credentials" by means of introducing an *IdP Proxy* in the current IMS architecture. At the same time, we overcome the problem of *InfoCards* roaming using an *InfoCards Storage System* and an *Identity Selector* both placed in the Home Domain. To deploy this architecture we use the language of assertions and infrastructure defined by OASIS: SAML (Security Assertion Markup Language) [3], an XML-based standard for expressing attributes and to request or retrieve assertions or references to assertions (*artifacts*) in an identity management framework. To transport SAML messages we adopt the solution defined in [4], where a new binding over SIP is defined to transport SAML messages.

The remainder of this document is organised as follows. In Section II we give a brief overview of the background technologies that lay the foundations of our work, and we also present some related research in the field. Then, the main limitations regarding Identity Management in NGN are identified in Section III. In order to outclass these challenges, we present a novel infoCard-based solution in Section IV, whose implementation details are provided in Section V. Finally, the main conclusions and future works are explained in Section VI.

II. Background technologies and related Work

A. Background technologies

1) IMS: IP Multimedia Subsystem is a standard to define New Generation Network (NGN) architecture focused on the

Work partially funded by the Madrid regional community project eMadrid under grant No. S2009/TIC-1650.

978-1-4244-5638-3/10/$26.00 ©2010 IEEE

convergence of the mobile and fixed networks. It is based on a common control plane using the Session Initiation Protocol (SIP) over internet protocol (IP) and it defines a framework to provision access to services in a transparent and easy way. One of the core elements of the control layer of IMS is the called Call Session Control Function (CSCF) Server. IMS defines three CSCF: a Proxy-CSCF, a SIP proxy in charge of redirecting the messages to the correct Home Domain of the User Equipment (UE). A Serving-CSCF in charge of authenticating the users and providing service to them. An Interrogating-CSCF, in charge of locating the S-CSCF in the Home Domain. Another important element is the Home Subscriber Server (HSS) that stores the user profile of each end user. This profile can include user's IP address, telephone records, buddy list and so on. On the top of the IMS architecture there is the service layer. IMS allows service providers to define and offer multimedia services through the called Application Servers that provide an interface against the control layer using the SIP protocol. IMS Authentication and Key Agreement (AKA) [5] is based on a challenge-response authentication mechanism. This implies the exchange of four messages between the end user and the IMS Home Domain after the user has obtained access to the network. This mechanism provides mutual authentication between the UE, using the ISIM (IMS Service Identity Module), and the home network using symmetric cryptography.

2) Information Cards: InfoCards [6] are an identity technology that allows users to select among their multiple identities to identify themeselves to a service. Also, users can manage in an easy, visual way their different electronic identities. Windows CardSpace [7], Higgins project [8], Open Source Identity Selector [9] or Bandit [10] are Identity Selector implementations used nowadays.

Regarding user-centric approaches, *infoCards* are like business cards which let users decide what information will be disclosed during an interaction, keeping personal data under control and they also let Relying Parties to get the information they need directly from the users. The Identity Selector Interoperability Profile specifies two types of *infoCards*: Personal or Self-Issued (claims about the user itself, e.g. phone number, e-mail address, web address); and also Managed Information Cards, issued by Identity Providers. The latter can be auditing, non-auditing, or auditing-optional to accommodate the needs of different business models. Furthermore, *InfoCards* support several data formats and authentication methods such as XML, SAML, and OpenID. InfoCard-based identity management systems typically use Web Services Security protocols (WS-*) and SOAP. WS-Trust [11] is the protocol used to obtain and exchange security tokens. Moreover, the integrity of the tokens is preserved using an XML-Signature as part of the WS-Security [12] protocol.

3) SAML: defines an XML based framework that allows to express assertions about an identity, including attributes, authorization and/or authentication information of a subject with the aim to facilitate relations between different security domains and their relationships with users. This specification defines four key elements: *Assertions*, which carry statements about a Principal as asserted by an IdP and can be related to authentication, attribute or authorization; *Protocols*, which describe the sequence of request-response messages for the exchange of *Assertions*; *Bindings*, which define how SAML *Assertions* and request-response protocol messages can be exchanged between entities using underlying communication protocols (such as HTTP, SOAP, Diameter or SIP); and *Profiles*, which define the specific sequence of messages and the *Bindings* required in each case to complete each of the use cases defined in the standard. Variations of the same profile can be obtained for each combination of use case and *Binding*.

On the other hand, we briefly introduce the main entities which can appear in a SAML-based identity federation management system, as well as the different roles they can play:

- *Service Provider (Relying Party, SP)*, entity which makes decisions based on the information that is provided by a third party about a particular subject, it is who provides a service.
- *Identity Provider(Asserting Party, IdP)*, entity which is responsible for issuing, maintaining and managing identity information about users in a federation. The IdP has the authentication infrastructure and implements the functionality to carry out storage of credentials, deleting and retrieving them from the user. In addition, IdPs issue SAML assertions which can be used by SPs when deciding on an *End User*.
- *End Users*, who are the subject of the assertions. They interact (usually via an user agent, typically a web browser), with SPs.

Note that currently SAML is the only open standard and is tightly coupled to other identity federation specifications and implementations, like the Liberty Alliance Identity Federation Framework [13], WS-Federation [14] or Shibboleth [15]. Moreover, SAML is highly flexible, which allows all its components can be extended.

B. Related Work

In [16], the authors propose a single SAML-based scheme to achieve Single Sign On (SSO) in NGN when accessing third party services or web services. This work suppose to store user credential like accounting information in the service provider network after the authentication phase and service delivery. Another idea, introduced in [17], bridges network access with authentication in the the application level in order to provide a form of unified SSO using information Card. While the first work is very general, the later is focused in linking two well known existing federations: Eduroam and EduGAIN. However, there are important drawbacks to be tackled, namely the need for the end user to be aware of her personal information exchanges.

Our vision is closer to that presented in the DAIDALOS project [18], which introduces the concept of Virtual Identity (VID) as a way to obtain a privacy enabled service authorization. Thus, they put the user in control to create and manage different identities or avatars, deciding how her attributes are disclosed when navigating between services. Although their approach allows user-centric identity management and focuses on preserving privacy, the derivate architecture becomes significantly complex, as it implies non trivial modifications in almost every existing component in the NGN model. Furthermore, this project is not directly targeting the limitations of the present IMS model. Here, we aim to address the main limitations regarding identity management in NGN defining a user centric framework to allow user to access services but with minor architectural changes in existing entities.

III. Identity Management Challenges in NGN

The IMS framework focuses its efforts in deploying a common plane to allow simple access to different types of service: SIP services, web services and third-party services. Although it includes the possibility to use non SIP services in its specification [19], there is no a detailed implementation of how to gain access to them. Problems like security and privacy of user information in an inter-domain scenario or how to manage identity among different operators are to be addressed in order to allow users to access services in a secure fashion. Additionally, users are often required to memorise user/password pairs in order to access all the services they want. This fact represents a minor inconvenience if users only access a few services, but with the rapid increase of web services the traditional approach to identity management is already having serious negative effects on the user experience. Besides this, the increase of new technologies have accustomed users to a new degree of "user experience". Users are able to share or subscribe to a service according to their needs and preferences. Furthermore, new mobile devices with increased capabilities allow users to access services everywhere, giving complete freedom to the end user. IMS today is not able to give the same degree of experience to the users. New paradigms are to be defined in order to make IMS the future network for accessing multiple domain services in a user centric, dynamic and secure way. Finally, the IMS registration procedure involves at least two authentication processes: the first with the access network and a second one with the IMS Home Domain. This number can increase quickly when a user tries to access third-party domain services, constituing another important limitation to be tackled.

IV. InfoCard management protocol in an inter-domain environment

In this section we describe our proposal that defines an architecture for IMS that overcomes the limitations of current frameworks. The proposed protocol defines an user centric environment to distribute user credentials in a secure fashion in order to gain access to web services or third-party services. To manage user's credentials, we have defined a modified *infoCard* system that allows users to choose what attributes to disclose to the SP, but without storing any card. This is thanks to the **Personal Identity Management System** (PIMS) defined along with the user's Home Domain. This entity implements an Idp Proxy, a card storage system and an identity selector. In this way, if the user wants to change her device, she can do it without exporting any *infoCard*. Furthermore, our architecture provides a framework to create an *infoCard* using trusted credentials from different IdPs. Moreover, although the user information, once the card has been created, is stored in the Home Domain for further uses, the credentials issued by other IdPs are not disclosed to the Home Domain since they are encrypted. Figure 1 depicts the flow message of the proposed protocol.

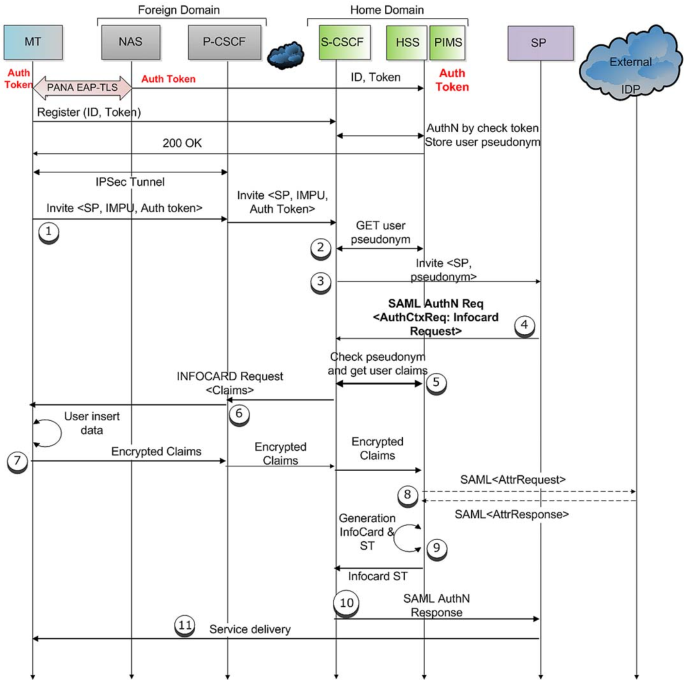

Fig. 1. New infoCard creation using heterogeneous domain's credentials

A. Assumptions

We suppose that there are federation relations among SP, Home Domain, the external IdP and MT. Within the federation, SP, Home Domain and IdP trust each other. Trust is established using X.509 certificates. Thus, the establishment of trust relationships is managed with formal contracts specifying policies surrounding these relationships. SP and IdP Proxy use the certificates of the external IdP published in the federation in order to verify the digital signature on its messages and accept the authentication assertions. Information cards are created dynamically by combining attributes that either the IdP Proxy or the external IdP send along with assertions. Furthermore, the SP has to be *InfoCard* enabled.

B. Protocol definition

First the Mobile Terminal (MT) has to gain access to the network and successfully register with the IMS core network as explained in [20]. In this way, we can obtain an authentication token that relates both the IMS registration and access network authentication. Once the user is authenticated, the HSS communicates with the Personal Identity Management

System (PIMS) in order to create and store in the PIMS an user pseudonym associated with the authentication token, so a valid authentication context will be created at the IdP when the IMS registration succeeds. Pseudonyms are aliases for a user and can be used as a handle by SPs to retrieve identity information about a user from the IdP.

In step 1 the MT sends a SIP INVITE message that carries the URI of the SP, the IMPU and the authentication token to the P-CSCF of the foreign network that is in charge of forwarding the message to the S-CSCF of the home network. The S-CSCF asks the PIMS for the pseudonym of the user over the Cx interface (step 2). It creates a new INVITE with the retrieved field and sends it to the correct Service Provider (step 3). The SP receives the message and creates a digitally signed SIP-SAML Proxy Authentication Request message, that includes the user pseudonym, asking for an *infoCard* to permit access to the service (step 4) and specifying the authentication context requirements (`<RequestedAuthnContext>`) for the authentication statement returned in *SIP-SAML Authentication Response* (step 10). As it was mentioned in section II-A3, SAML components can be extended. So we propose an authentication context extension (*InfoCard SAML Authentication Context Extension*) that allows users to use Information Cards as authentication method. The message is forwarded to the S-CSCF. In step 5 the S-CSCF, over the Cx interface, sends a message to the PIMS asking for an infoCard that matches the service request. The PIMS verifies the user pseudonyms and the signature and, if they are correct, it looks for the card. If there is no appropriate *infoCard*, the S-CSCF sends the request to the P-CSCF, that forwards the message to the MT(step 6). In step 7 the user creates a SIP message including the attributes needed for the service. The SP credentials are encrypted using the public key of SP's certificate. In this way the attributes are not disclosed to the Home Domain. If claims from other IdPs are needed, the user selects which Idp to use in order to get the requested information and adds the IdP identificator (IdPID) to the message. The message is forwarded to the home network. In step 8 the PIMS parses the message and if there is an IdPID, it creates a SAML Attribute Request and sends it to the corresponding IdP. Note that through the mechanism of Single Sign On, as the user is already authenticated to the Home Domain IdP after the IMS registration, the IdP Proxy (acting as a SP) can ask the external IdP for user's attributes without providing any additional information. The Idp creates a SAML Attribute Response including the attributes encrypted and sends it back to the PIMS. In step 9 the PIMS creates and stores the *infoCard* using all the received attributes. It generates a Security Token (ST) and sends it to the S-CSCF. In step 10 the S-CSCF creates a SIP-SAML Authentication Response including the ST and forwards it to the SP. If the SP successfully checks the *infoCard*, the requested service is returned to the user (step 11).

Notice that at step 5, if an *infoCard* was retrieved from the PIMS, the S-CSCF sends it to the MT in order to confirm its validity. The user through an interface is able to see the selected Information Card and in this way she can confirm or not the usage of the card. Once the MT sends the confirmation to the S-CSCF, it sends the *infoCard* to the SP. Then, it checks the claims and delivers the service to the user.

C. Security Analysis

The main objectives of the proposed protocol are to create, transport and securely store user attributes and credentials to be used in an *InfoCard* environment. We assume as initial condition that each involved entity shares a public X.509 certificate, so everyone is able to encrypt a message with the receiver's public key if needed. The MT and the Home Network share between each other a long term shared secret used during the authentication phase. This assumption is commonly employed in the regular IMS registration protocol. Besides, as explained in IV-A, the SAML components in the architecture are federated with each other. Therefore, when a MT performs an IMS registration with the home network, it is performing indeed a Single Sign On with the federation. In step 3 the PIMS signs the fields of the INVITE message with its private key in order to provide integrity to the message. At the same time it initiates SP authentication by including a challenge (*CH1*) encrypted with the SP's public key. The challenge has to include the same timestamp value present in the signature of the INVITE message in order to prevent replay attacks. The INVITE message is then composed and forwarded to the SP by the S-CSCF using an user pseudonym in order not to disclose to the SP the real user identity. The SP answers in step 4 in the same way with a signed message that includes the challenge received from the S-CSCF (*CH1*) and a new challenge value (*CH2*), encrypted with the public key of the Home Network, that will be used to authenticate the S-CSCF. When the home network receives the message it can securely authenticate the SP by matching the previously sent *CH1* with the value received from the SP. The SP will be able to securely authenticate the home network at step 10. Here the S-CSCF sends a SAML authentication response message that includes the *InfoCard* security token generated by the PIMS and the *CH2* value previously received from the SP, thus the SP can authenticate the home network as well as the user.

V. Implementation issues and Use-case example

In order to test the proposed protocol we have to define the IMS-SAML infrastructure. Regarding IMS a complete architecture has been deployed by means of using the open source implementation provided by Fraunhofer Institute (FOKUS) [21]. An infocard enabled SP has been implemented using Sailfin Application Server [22], a robust and scalable SIP servlet technology and OpenSSO [23] that provides a module which implements a full infocard protocol using Java Library Openinfocard. In order to extend the HSS capabilities we use digitalME, an open source set of components that enable users and applications to interact with Infocard-compatible web sites and services, to deploy an identity selector and an infocard storage. Moreover another instance of OpenSSO is used to define a Security Token Service. For deploying the IdP, we are using Authentic which is an IdP implementation based on the lasso library [24] and also supports SAML 2.0 messages. Thus, we are currently working in order to integrate the new software components that will allow the proposed infocard-based protocol to operate.

A. Use-Case Example

In this section, we present a scenario in which the infrastructure proposed in this article could prove useful and furthermore, improve user experience when she performs a transaction similar to the one explained below. The main actors in this scenario are: the Mobile Operator (Home Domain), which has agreements with the Travel Agency (SP) and the Bank (external IdP). We can reasonably suppose that a **Secure Electronic Transaction** (SET) [25] system is deployed by the IMS and SAML architectures. The federation between the Bank, Home Domain and Travel Agency (TA) accomplishes with the SET requirement that parties involved in the transaction can verify the validity of the counterpart certificates. The user agrees with the TA upon the details of the transaction such as the purchase amount. This aspect is out of the scope of the protocols and can even take place over an unsafe connection. Once the details are defined, SET Initiation request/response messages can be sent in the step 3 of Fig.1, exchanging user's local ID, a random challenge (as already included in the proposal), the TA and Bank certificate and an *infoCard* request. The user fills up the required fields of the *infoCard* (or confirms them) and sends it back to the Operator. The *Order Information*, refreshed to match current payment in case of reusing an existing *infoCard*, and the *Payment Instruction* are carried encrypted with the TA public key and the Bank public key respectively. Moreover a double signature including both encrypted parts is generated to guarantee integrity of the message. The Operator checks the validity of the user *Payment Instruction* with the Bank and, unless it fails, sends the *infoCard* security token to the TA. At this point the TA can decrypt and verify user's *Order Information* data and use *Payment Instruction* data to terminate the payment with the Bank. In this kind of operations none of the involved parts knows all the information of the transaction. Actually, the Operator knows the user is buying from the TA but ignores the *Order Information* and *Payment Instruction* , the TA knows only the *Order Information* and the Bank knows only user's *Payment Instruction*. Furthermore, straightness of SAML federation conditions and the extra degree of security that our proposal brings by the validations on steps 5 and 8 can overcome some well known weaknesses of SET protocol [26], that focuses on the registration of the involved entities with a common Certification Authority and allows an attacker to personify either the SP or the gateway/bank used for the payment.

VI. Conclusions and Future Work

In this article we have introduced the concept of *infoCard* in the IMS NGN. We have defined a protocol to overcome the limitations of the current identity management systems based on this technology. With the introduction of a Personal Identity Management System (PIMS), we have designed an user centric scenario to allow users to securely use their credentials in order to gain access to a service. Moreover, we allow the creation of *infoCards* using claims from different Identity Providers and we also give users the freedom to change device without having to export their Information Cards (*infoCard* roaming). Finally, we have described some implementation details of the proposal that we are currently facing and we have also presented an use case where our proposal can be used. We have deployed both IMS and SAML infrastructures based on opensource technologies and we are currently working in the PIMS functionality. As future work we aim to develop and test the performance of the proposed identity protocol.

References

[1] J. Rosenberg, H. Schulzrinne, G: Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler: "Sip: Session initiation protocol". Technical Report RFC3261, IETF (2002)

[2] K. Cameron. *The laws of identity*, http://www.identityblog.com/?p=352

[3] OASIS.: Security Assertion Markup Language (SAML) V.2.0. Technical Overview. http://www.saml.xml.org

[4] H. Tschofenig, J. Hodges, J. Peterson, J. Polk, D. Sicker. SIP SAML Profile and Binding, draft-ietf-sip-saml-07.txt. March 2010.

[5] 3GPP: Technical specification group services and system aspects. Access security for IP-based services. TS 33.203 V8.3.0, Jun 2008.

[6] Information Cards.: Information Cards Foundation, 2009. Available at: http://informationcard.net/

[7] Microsoft Windows CardSpace. Available at: http://msdn.microsoft.com/en-us/library/aa480189.aspx

[8] Higgings.: Higgins Open Source Identity Framework. Available at http://eclipse.org/higgins/, March 2010.

[9] OSIS: Open Source Identity Systems. Open Source Identity Systems Wiki. Available at: http://osis.idcommons.net/, March 2010.

[10] Novell, The Bandit project. Available at: http://www.bandit-project.org/, March 2010.

[11] A. Nadalin, M. Goodner, M. Gudgin, A. Barbir, and H. Granqvist: *WS-Trust 1.3*. OASIS Standard. March 2007.

[12] A. Nadalin, C. Kaler, R. Monzillo and P. Hallam-Baker (eds.): *Web Services Security: SOAP Message Security 1.1 (WS-Security 2004)*. OASIS Standard Specification. February 2006.

[13] LA.: *Liberty ID-FF Protocols and Schema Specification.* Available at: http://www.projectliberty.org

[14] WS-Federation.: *Web Services Federation Language version 1.1.* December, 2006.

[15] Internet2.: Shibboleth Architecture. http://shibboleth.internet2.edu

[16] J.-Ch. Grgoire and S. Islam: *"An SSO-Enabled Architecture for Beyond the IMS Domain Services"*. In: 6th International Workshop on Next Generation Networking Middleware. Italy, 2009

[17] E. Hoz, A. Garcia, I. Marsa-Maestre, M.A Lopez-Carmona, and B. Alarcos: *An infocard-based proposal for unified SSO*. In: Ninth Annual International Symposium on Applications and the Internet. July, 2009.

[18] Z. Chen: *A Privacy Enabled Service Authorization Based on a User-centric Virtual Identity Management System.* In: Second International Conference on Communications and Networking. China, 2007.

[19] 3GPP: *Technical specification group services and system aspects.* IP Multimedia Subsystem (IMS), Stage 2. TS 23.28 V8.5.0, Jun 2008.

[20] D. Díaz, D. Proserpio, A. Marín, F. Almenárez and P. Weik*"A general IMS registration protocol for wireless networks interworking"*. In: Wireless Mobile Networking Conference (WMNC), 2009.

[21] Open IMS Core: http://www.openimscore.org/

[22] Project SailFin: http://wiki.glassfish.java.net/Wiki.jsp?page=SailFin

[23] OpenSSO: https://opensso.dev.java.net/

[24] Lasso, Liberty Alliance Single Sign-On: http://lasso.entrouvert.org/

[25] Mastercard/Visa: *SET Secure Electronic Transaction Specification*. Books 1-3, May 1997.

[26] S. Brlek, S. Hamadou and J. Mullins: *"Some Remarks on the Certificates Registration of the Electronic Commerce Protocol SET"*. In: International Conference on Internet and Web Applications and Services/Advanced International Conference. Feb, 2006