2 Editorial: Serbian Publication InfoReview joins UPENET, the Network of CEPIS Societies Journals and Magazines
2 From the Chief Editor’s Desk
New Deputy Chief Editor of UPGRADE

3 Presentation: Identify Yourself but Don’t Reveal Your Identity — Javier Lopez-Muñoz, Miguel Soriano-Ibañez, and Fabio Martinelli

6 Digital Identity and Identity Management Technologies — Isaac Agudo-Ruiz

13 SWIFT — Advanced Services for Identity Management — Alejandro Pérez-Méndez, Elena-Maria Torrogllosa-Garcia, Gabriel López-Millán, Antonio F. Gómez-Skarmeta, Joao Girao, and Mario Lischka

21 A Privacy Preserving Attribute Aggregation Model for Federated Identity Management Systems — George Inman and David Chadwick

27 Anonymity in the Service of Attackers — Guillermo Suarez de Tangil-Rotaiche, Esther Palomar-Gonzalez, Arturo Ribagorda-Garnacho, and Benjamin Ramos-Alvarez

32 The Importance of Context-Dependent Privacy Requirements and Perceptions to the Design of Privacy-Aware Systems — Aggeliki Tsouhou, Costas Lambrinoudakis, Spyros Kokolakis, and Stefanis Gravalis

38 Privacy… Three Agents Protection — Gemma Dèler-Castro

44 Enforcing Private Policy via Security-by-Contract — Gabriele Costa and Ilaria Matteucci

53 How Do we Measure Privacy? — David Rebollo-Monedero and Jordi Forcós

59 Privacy and Anonymity Management in Electronic Voting — Jordi Puiggalí-Alpezz and Sandra Gausch-Castelló

66 Digital Identity and Privacy in some New-Generation Information and Communication Technologies — Agustí Solanas, Josep Domingo-Ferrer, and Jordi Castellá-Roca

72 Authentication and Privacy in Vehicular Networks — José-Maria de Fuentes García-Romero de Tejada, Ana-Isabel González-Tablas Ferreras, and Arturo Ribagorda-Garnacho

79 From ITNOW (BCS, United Kingdom)
ICT in Education
Enthusing Students — Bella Daniels
81 From InfoReview (JISA, Serbia)
Information Society
“Knowledge Society” is a European Educational Imperative that Should not Circumvent Serbia — Marina Petrovic

CEPIS NEWS

84 Selected CEPIS News — Fiona Fanning
86 Privacy-Consistent Banking Acquisition — CEPIS Legal and Security Special Interest Network

* This monograph will be also published in Spanish (full version printed; summary, abstracts, and some articles online) by Novática, journal of the Spanish CEPIS society ATI (Asociación de Técnicos de Informática) at <http://www.ati.es/novatica/>.

UPGRADE is the European Journal for the Informatics Professional, published bimonthly at <http://www.upgrade-cepis.org/>

Publisher

UPGRADE monographs are also published in Spanish (full version printed; summary, abstracts and some articles online) by Novática

UPGRADE was created in October 2000 by CEPIS and was first published by Novática and INFORMATIK/INFORMATIQUE, bimonthly journal of SVI/FSI (Swiss Federation of Professional Informatics Societies, <http://www.svifi.ch>)

UPGRADE is the anchor point for UPENET (UPGRADE European NETwork), the network of CEPIS member societies’ publications, that currently includes the following ones:

- InfoReview, magazine from the Serbian CEPIS society JISA
- Informatika, journal from the Slovenian CEPIS society SDI
- Informatik-Spektrum, journal published by Springer Verlag on behalf of the CEPIS societies GI, Germany; and SI, Switzerland
- ITNOW, magazine published by Oxford University Press on behalf of the British CEPIS society BCS
- Mondo Digitale, digital journal from the Italian CEPIS society AICA
- Novática, journal from the Spanish CEPIS society ATI
- OCG Journal, journal from the Austrian CEPIS society OCG
- Přirofornik, journal from the Croatian CEPIS society CCS
- Tólvumál, journal from the Icelandic CEPIS society ISIP

Editorial Team
Chief Editor: Llorenç Pagés-Casas
Deputy Chief Editor: Rafael Fernández Calvo
Associate Editor: Fiona Fanning

Editorial Board
Prof. Vasile Baltas, CEPIS President
Prof. Wolfgat Studny, CEPIS Former President
Hans A. Frederik, CEPIS Vice President
Prof. Nello Scarabottolo, CEPIS Honorary Treasurer
Fernando Piera Gómez and Llorenç Pagés-Casas, ATI (Spain)
François Louis Nicolet, SI (Switzerland)
Roberto Carneil, ALSI – Tecnoteca (Italy)

UPENET Advisory Board
Dubravka Dulak (Inforeview, Serbia)
Matjaž Gams (Informatika, Slovenia)
Hermann Engesser (Informatik-Spektrum, Germany and Switzerland)
Brian Runciman (ITNOW, United Kingdom)
Franco Filippazzi (Mondo Digitale, Italy)
Llorenç Pagés-Casas (Novática, Spain)
Vesel Rikal (OCG Journal, Austria)
Panicos Mavroudis (Přiroforník, Cyprus)
Thorvarður Kari Ólafsson (Tólvumál, Iceland)
Rafael Fernández Calvo (Coordination)

English Language Editors: Mike Andersson, David Cash, Arthur Cook, Tracey Darch, Laura Davies, Nick Dunn, Rodney Fennimore, Hilary Green, Roger Harris, Jim Holder, Pat Moody.

Cover page designed by Concha Arias-Pérez “Indissociable Identity” © CEPIS 2010
Layout Design: François Louis Nicolet

Composition: Jorge Llobera-Gil de Ramalles

Editorial correspondence: Llorenç Pagés-Casas <pages@ati.es>
Advertising correspondence: <novatica@ati.es>

UPGRADE Newslsl list available at <http://www.upgrade-cepis.org/pages/editinfo.html#newslsl>
Copyright © Novática 2010 (for the monograph) © CEPIS 2010 (for the sections UPENET and CEPIS News)
All rights reserved under otherwise stated. Abstracting is permitted with credit to the source. For copying, reprint, or republication permission, contact the Editorial Team

The opinions expressed by the authors are their exclusive responsibility

ISSN 1684-5285

Monograph of next issue (April 2010)

“Information Technology inTourism Industry”

(The full schedule of UPGRADE is available at our website)
Identity and Privacy Management

SWIFT – Advanced Services for Identity Management

Alejandro Pérez-Méndez, Elena-Maria Torroglosa-García, Gabriel López-Millán, Antonio F. Gómez-Skarmeta, Joao Girao, and Mario Lischka

Traditional solutions for identity management, based on the end user authentication, usually by means of credentials such as username and password, have significantly improved in recent years with the incorporation of SSO (Single Sign-On) mechanisms and the concept of identity federations. However, both providers and end users are demanding additional services not yet available in current solutions. These additional advanced services such as anonymity, authorization based on end user attributes, and cross-layer SSO, would improve the usability and security of these systems. The SWIFT (Secure Widespread Identities for Federated Telecommunications) project aims to offer an identity management framework in which all these advanced topics can work together.

Keywords: Identity Management, Privacy, SSO, SWIFT, Virtual Identity.

1 Introduction

Identity management is an aspect of Internet service provision that causes concern to network and security administrators of organizations willing to provide services over the Internet [1]. From the point of view of both organizations and end users, management of user accounts is of paramount importance both to protect service providers against malicious users, and to protect users against providers that want to obtain information about user profiles, behaviour patterns, site visited sites, etc [2].

The increasing importance of new services on the Internet, mainly due to the increasing popularity of social networks [3], results in users having to manage a many accounts associated to those services and which contain information about their own identity. This situation leads to bad management of these accounts by end users and, therefore, to security risks [4].

On the contrary, service providers have traditionally based end user access to services on end user information, linked to end user identity, which is used for authentication

Authors

Alejandro Pérez-Méndez is a researcher in the Department of Information and Communications Engineering of the Universidad de Murcia, Spain. His research interests include network security and identity management. He received his MSc in Computer Science from the same university. He is currently involved in the IST-SWIFT research project. <alex@um.es>

Elena-María Torroglosa-García is a researcher in the Department of Information and Communications Engineering of the University of Murcia, Spain. Her research interests focus on identity management, privacy and security. She is currently involved in the IST-SWIFT research project. <emtg@um.es>

Gabriel López-Millán is an assistant professor in the Department of Information and Communications Engineering of the University of Murcia, Spain. His research interests include network security, AAA, PKI, and IPv6. He received his MSc and PhD in Computer Science from the same university. <gabilm@um.es>

Antonio F. Gómez-Skarmeta received his MSc degree in Computer Science from the University of Granada and his BSc (Hons.) and PhD degrees in Computer Science from the University of Murcia, Spain. Since 2009 he has been Full Professor at the same department and university. He has worked on various national and international research projects, including Euro6IX, 6Power, Positif, Seinit, Deserec, Enable and Daidalos.

His main interest is in the integration of security services at different layers such as networking, management and web services. He is associate editor of the IEEE SMC-Part B and reviewer of several international journals. He has published over 90 international papers and has been a member of several program committees. <skarmeta@um.es>

Joao Girao received his diploma in Computer and Telematics from the Universidade de Aveiro, Portugal, in 2003. In 2003 he joined the Ubiquitous Secure Computing group at NEC Laboratories Europe, in Heidelberg, Germany, where he is responsible for the technical coordination of the Identity Management area. He has been involved in several standards activities such as the ITU-T, ETSI, IETF and Liberty Alliance. He has published widely, in particular in the areas of Identity Management and Wireless Sensor Network security. <joao.girao@nw.netlab.eu>

Mario Lischka received his Diploma (1999) and PhD (2006) in Computer Science from the University of Dortmund, Germany, focusing on distributed role based access control. He joined NEC Laboratories Europe in 2006 working on Identity Management and authorization. He is currently developing a distributed access control framework in the EU FP7 SWIFT project. In addition he is involved in standardization activities in Liberty Alliance and Open Mobile Alliance. <mario.lischka@nw.netlab.eu>
purposes. Nowadays, more and more providers are requesting solutions to incorporate additional end user information in order to decide whether an end user is allowed or not to access the service, that is, not just making use of login and password, but using additional attributes (such as organization, role, age, etc.) thus incorporating a complete authorization process.

It is also important to note that service providers are forming identity federations, [1] in order to facilitate user access to different services by means of Single Sign-On (SSO) mechanisms [5]. These identity federations try to partially mitigate the problem of the existence of multiple user accounts, but they rarely offer solutions for the management of authorization, privacy nor anonymous access to services [1].

The SWIFT project (Secure Widespread Identities for Federated Telecommunications) [6] defines an identity management framework that aims to provide a solution to all these advanced aspects requested by end users and by service providers. SWIFT aims to allow users to group all their accounts into virtual identities. Moreover, it allows users to access the services in an anonymous way, thus avoiding traceability by third-parties.

Starting from this identity federation scenario, it is desired, moreover, to introduce SSO management not only at the service layer such as web services, but also in those scenarios where network access requires a previous authentication step. That is, to perform a single authentication process both for network access and to allow SSO access to the upper layer services.

In order to describe these characteristics, this paper is structured as follows. Section 2 offers an overview of how SWIFT incorporates this set of advanced identity management aspects. In Section 3, components of the architecture are briefly described, while Section 4 depicts a use case illustrating the basic behaviour of the different entities. Section 5 gives an overview of related work, before we conclude with an outlook on future work in Section 6.

2 Advanced Identity Management Aspects in SWIFT

The following section provides a high-level overview of the most important advanced identity management aspects covered by SWIFT.

2.1 Identity Aggregation

Nowadays, typical Internet users have many accounts with different service providers (e.g. electronic bank, email, social networks, blogs, etc.). Associated with each of these accounts are both authentication credentials and some amount of personal information related to the user (e.g. name, address, hobbies, work place…). This exposes a series of drawbacks for the user, like having to remember the credentials associated to each one of them, the difficulty of controlling privacy (e.g. revoking access to my phone number in all the accounts) and the tedious need to complete registration forms usually with the very same data.

SWIFT allows users to create virtual identities that link or aggregate authentication credentials and attributes coming from different providers [7], as shown in Figure 1. These providers can play different roles: Authentication Providers utilizing Authentication Statements asserting to other entities that a particular user has been authenticated properly, or Attribute Providers, storing and managing the various pieces of information on a particular identity. A single provider could play both roles if required.
Virtual identities are created and managed on special identity providers called Identity Aggregators, which act as an intermediary entity between Service Providers and the end user information stored on the different identity providers. For each new virtual identity there exists a VID (virtual identifier), that identifies univocally such an identity within the context of an Identity Aggregator (e.g. alice@aggregator.org).

The description of the management of these virtual identities is out of the scope of this paper. A detailed description can be found in [8].

Figure 1 shows an example where the user has defined a virtual identity using his credentials from one of his accounts at Identity Provider A (that will act as Authentication Provider). Besides, the end user has also aggregated some attributes from his accounts at Identity Providers A, B and C (that will play the role of Attribute Providers).

Virtual identities allow solving the drawbacks mentioned above, since it is not required to remember so many of credentials (only the aggregated ones) and service providers can obtain data dynamically from the virtual identity (this way avoiding the problems of redundancy and privacy).

2.2 Identity-based Access Control

In an identity management system, the point of view of end users regarding release of information releasing is the opposite to that of service providers. While the former prefer to reveal the minimum amount of information as possible, when they access a service, service providers seek to obtain as much information as possible about users in order to, on the one hand, provide the service and, on the other hand, to obtain a greater knowledge about the profile of their users. Therefore, a good identity management system must find a compromise to cover the requirements of both end users and service providers.

Thus, a service provider needs to know some identity information of the users to be able to decide whether the service will be provided or not. This process of gathering information and deciding about the access to a service is called Access Control [9][7].

In SWIFT, access control is based on the virtual identity of the user. When a user desires to access a service he presents an Initiation Statement or an SSO Token (if SSO is desired) [8]. However, the Service Provider requires information asserting that she is a valid and identified user in the system. Thus, it contacts with the Identity Aggregator and forwards the received information from the end user. Once the Identity Aggregator has determined the identity of the user, it provides the Service Provider with the Authentication Statement, which makes sure that the user has been authenticated by the Identity Aggregator.

In addition to the verification of the user’s identity, the service provider may require an additional authorization process to verify that the end user satisfies certain requirements before providing her with the service (for example, to be over 18 years old, to have certain nationality or to have a positive balance on a banking account). Thus, the service provider must contact with the Identity Aggregator and request the end user attributes. The amount of user’s information that will be available for the service provider will depend on the attributes that were aggregated by the end user to that virtual identity and the Attribute Release Policies that were defined by her. As the environment is highly distributed, policies have been introduced to specify the user’s intentions [10].

Summarizing, access control is performed in the service providers based on the authentication statements issued by the Identity Aggregator, as well as on the end user attributes, obtained from the Attribute Providers through the Identity Aggregator.

2.3 Cross-layer SSO

One of the main objectives of SWIFT is to provide a Single Sign On (SSO) mechanism [5][11]. This mechanism should work across different network layers, in such a way that allows reusing the authentication performed at one layer to authenticate at a different one. This means that if an end user is authenticated during the access to the network using one of his virtual identities (for example by means of EAP-MD5, EAP-TLS, or PEAP etc. [12] the authentica-
tion material obtained during the process will allow her to access later on to services at the application layer (for example, web services) without repeating the authentication process again.

Figure 2 shows an example where a SWIFT end user is firstly authenticated to access the network, and then he makes use of the defined SSO mechanisms to access a web service. A complete authentication process is performed for the network access, by means of some network level authentication protocol (for example, EAP). As a result of this authentication, the user obtains a SSO Statement generated by the Identity Aggregator. With this statement the user is able to generate the specific SSO Token used to access the web service. The service provider will request the validation of the token to the Identity Aggregator before providing any service to the user.

This provides an added value to end users, but with the drawback of not being transparent for them, as happens with the traditional methods. The management of SSO tokens and statements is described in [8].

2.4 Privacy Management

User privacy management is one of the pillars of the SWIFT architecture. The objective is to provide the end user with the required mechanisms and procedures to control the amount of personal information that is revealed to the different entities in the system. In SWIFT, end user privacy is taken into account from the moment virtual identities are created. Along with the creation process (called enrolment), an end user does not reveal the actual identifiers he has in the different involved providers. A pseudonym (identifier that is created by an entity to refer another entity) is established instead between those providers and the Identity Aggregator. This way, it is impossible for the Identity Aggregator to determine whether the same user has created more than one virtual identity.

As described in Section 2.1, each virtual identity has a unique identifier called VID. This VID, therefore, must be presented by the end user on each access to a protected service, with the purpose of being identified by his Identity Aggregator. In order to protect user privacy, and since this information must go through the service provider, the VID is protected in such a way that only the Identity Aggregator is able to know all details. This way, service providers are not able, on the one hand, of recognizing the identity of the end user (anonymity) and, on the other hand, of relating different accesses of the same user to the same service (unlinkability) [7].

Besides protecting their identity, SWIFT allows end users to control what kind of information can be revealed and to whom. As indicated before, when an end user accesses to the different available services, her intention is to reveal as minimum amount of information as possible (Section 2.2). For this reason, SWIFT makes use of advanced attribute release policies that are established by the end user at the Identity Aggregator, which becomes into the trust point of the framework. These policies are expressed using the XACML language [13] or a newly introduced version of distributed XACML [10].

2.5 Virtual Terminal

Currently, an end user has more than one device or terminal. Sometimes the use of certain digital identities is limited to be bound to some specific devices due to, for example, processing capacity restrictions, security constraints, etc., conditioning this way the flexibility and usability of the system. With the aim of mitigating this problem, the concept of virtual terminal has been defined within SWIFT [14], which tries to make identities usable among all the user’s devices.

The use of virtual terminals allows, for example, reducing the number of authentication processes that must be
performed among the devices, enabling the use of authentication capabilities of a device into another one (for example the use of a SIM card [15] to authenticate a web video streaming session) and moving application sessions among devices in a single way for end users and service providers.

In the virtual device architecture [14], one of the devices assumes the role of master device. Its responsibilities are to coordinate the inclusion and removing of devices, as well as the announcement of capabilities and the selection of the most indicated device to perform an operation. Figure 3 shows the basic architecture for the virtual terminal, where the different functional blocks that compose a device are depicted. Each of these functional blocks is in charge of a specific task: credential manager, identity manager and device coordinator.

Therefore, this architecture allows providing transparency in using and managing a group of devices as if they were a single device, sharing identity information and session control.

2.6 Mobility

Identity management mechanisms provided by SWIFT, specially the SSO one, allow management of the terminal mobility [16] to be simplified. This way, when a terminal moves from one network to another, it can perform a faster authentication, involving a lower number of messages and computational overhead, by making use of the material obtained from the first authentication.

Besides optimizing the network authentication process, the possibility of joining identity management with mobility management improves the access and availability of dynamic user information (for example the current location of the user or his preferences for certain services based on the current connection capabilities).

An example of mobility would be when Bob connects to the network with his PDA using his home cable connection, and then he decides to move to his car where he wants to keep connected to the network (in this case using a UMTS connection), and to maintain the active session alive.

SWIFT defines a framework that allows managing of end user mobility based on the use of authentication tokens and the mediation of the Identity Aggregator.

3 Components of the SWIFT Architecture

While Section 2 has described a series of important aspects within the SWIFT functionality, this section focuses on the description of the main components of the framework that performs the functionality described in this docu-
Identity and Privacy Management

4 Use Cases

In this section we present a high level vision of two of the use cases that have been defined for SWIFT and that are exhaustively in [8] and [17]. They depict the SWIFT identity management capabilities, specifically the use of virtual identities, attribute aggregation and the cross-layer SSO authentication.

4.1 Authentication and Authorization for Network Access

In this use case, Alice (EU) desires to access the network using one of her virtual identities. As shown in Figure 4, Alice initiates the process presenting an Initiation Statement to the network provider (NP), including information about the VID (step 1). As described before in this document, this information is protected to avoid anyone except the IdAgg to recognize the EU. That statement is forwarded from the NP to the IdAgg, which identifies that it refers to Alice’s virtual identity (alice@idagg.com) and determines the AuthNP that will be in charge of her authentication (step 2 and 3). Once Alice has been authenticated (by means of some network authentication mechanisms) (4), the AuthNP sends an artifact to the end user (step 5), enabling to retrieve a SSO Statement at a later point of time (step 14 and 15). Additionally the AuthNP provides an Authentication Statement to the IdAgg, where it is certified that Alice has been successfully authenticated (6). Following the same rationale, the IdAgg generates an Authentication Statement for the NP (7) where, besides of asserting Alice’s authenticity, a pseudonym is provided. This way the SP only needs to trust in the statement issued by the IdAgg, knowing nothing about the AuthNP that actually performed the authentication.

Once the authentication has been performed, the NP can request end user attributes to complete the process of authorization, prior to provide the service to Alice. In the first instance, the NP makes use of the pseudonym obtained in the previous step to request the attribute age from the IdAgg (8). The IdAgg determines which virtual identity is behind the indicated pseudonym, whether the requested attribute
is available or not (i.e. it was aggregated by the end user and the privacy policies allow it to be provided to the NP). If so, the IdAgg contacts with the AttP and requests the attribute (9). The AttP provides the attribute to the IdAgg (10), then does the same for the NP (11). In the same way, the NP only trusts the IdAgg for providing attributes.

Once the NP has obtained the users attribute age it can verify, by means of the corresponding access control policies (12), that she can be provided with the service (13) since she is over 18 years old. During this process the NP never knows the users actual identity, preserving her anonymity.

4.2 SSO Authentication for Web Access

In this use case an end user, Alice (EU), desires to access a web service, making use of one of her virtual identities and the SWIFT SSO mechanisms. As a previous step, Alice generates a SSO Token based on the SSO Statement received along the network access authentication and the SP that she wants to access. This token is protected in such a way that only the IdAgg is able to read it. As show in Figure 5, Alice starts the exchange of messages by sending this SSO Token to the SP (1). After that, the SP forwards the token to the IdAgg in order to validate its authenticity (2). Then the IdAgg determines the virtual identity of Alice (in this case, alice@idagg.com) and verifies that the SSO Statement used for its generation correspond with the one generated for the last Alice’s authentication. Once the IdAgg has validated the SSO Token, it generates and provides an Authentication Statement (3) to the SP. At this point the SP can perform the authorization process as described in the previous section (4) and provide the service to Alice (5).

As for the previous use case, the web access is performed in an anonymous way to the SP, which trusts the IdAgg for the identity management processing (authentication and attribute provisioning). Besides, the attribute retrieval is common for all the use cases, being the pillar of the authorization process.

5 Related Work

Currently we can find some related work with some of the specific aspects embraced by SWIFT, though none of them provides a complete and integrated functionality.

One of them is Idemix [18], that proposes an identity management solution where it is possible the aggregation of identities and the advanced privacy management. On the other hand, regarding the cross-layer SSO mechanisms, there are some proposals for its integration with IMS networks [19]. Finally, regarding the network authentication and access control policies, projects like DAMe [20] have presented their proposals and advances in the field.

6 Conclusions

This paper presents a high-level vision of a framework offering solutions for advanced identity management aspects to both service providers and to users. The potential to aggregate end user accounts thus simplifying their management, or end users performing anonymous access to services which guarantee that they are valid, authenticated and authorized, offers great possibilities for both users and services. For instance, offering customized services depending on the end user attributes. For those organizations that require an authenticated network access (universities, research centres, companies etc.), the association between the network authentication process and the access to higher-level services increases the usability of these solutions.

These concepts are being developed within the SWIFT project and offer a base framework for further work in other identity management aspects, including advanced access control mechanisms, identity delegation, service-bound accounting etc. As an immediate next step, a formal security analysis is being performed over the current framework proposal.

Acknowledgments

This work was partially funded by SWIFT (FP7, Grant Number 215832). The authors also thank the Funding Program for Research Groups of Excellence (04552/GERM/06) established by Fundación Séneca, Region of Murcia, Spain.

References

Identity and Privacy Management


[15] 3GPP TS 42.017. Subscriber Identity Modules (SIM); Functional characteristics.


