Wireless Pers Commun (2009) 49:353–363
DOI 10.1007/s11277-009-9697-0

Identities in the Future Internet of Things

Amardeo C. Sarma · João Girão

Published online: 31 March 2009

Abstract There are two problem areas of the current Internet to be solved in Future Internet scenarios—security and putting the user back in control despite the move to the Internet of things. With this in mind, we address problems associated with the diversifying of the Internet towards an Internet of things, and with increased ways to be reachable, whether the user wants it or not, in the digital world. The paper presents two approaches to cope with the problem: The Identinet and a concept designated by the digital shadow. The paper presents an architecture based on these concepts.

Keywords Identity · Virtual identity · Digital identity · Digital shadow · Identinet · Security · Privacy · Future Internet · Internet of things

1 Introduction

The current discussions on the Future Internet indicate a crisis of the capabilities of the current Internet and the attached world-wide services and applications. The problems concern, on the one hand, the loss of security and privacy in communications and services, with personal data becoming available and unwanted communication becoming rampant. Even various security mechanisms that are available, such as pop-ups warnings about certificate mismatches, are ignored by a user unable to understand the implications. On the other hand, the proliferation of service offerings and options now completely overwhelm the normal customer, who has severe problems managing access to services and the underlying infrastructure.

The overall problem is further aggravated by the diversification of the Internet, with new end systems and networks coming into play, of which wireless sensor networks and vehicular systems are just examples. The user is thus confronted with a wide range of methods

A. C. Sarma (✉) · J. Girão
NEC Laboratories Europe, Kurfürstenanlage 36, 69115 Heidelberg, Germany
e-mail: sarma@nw.neclab.eu

J. Girão
e-mail: girao@nw.neclab.eu

and devices with which to access the digital world, and it can no longer be assumed that a single, independent access per device will suffice, nor that the user will actually own all these devices.

The EU projects Daidalos [1] and SWIFT [2] have begun to address this problem, and several solutions have been presented. The same may be said of other projects, such as PRIME and PrimeLife, who were more directly focused on privacy and security concerns.

In defining how a digital identity relates to entities (or objects, real or imagined), the paper adopts the approach that data, including attributes within a digital identity, designates constructs referring to entities. Examples of constructs are age, identifiers, and in general concepts, propositions and claims about an entity. The sum of all constructs form the identity of the entity. The data of a digital identity thus *denotes* these entities and *designates* an identity, which in many cases are of persons. This is an adaptation of Bunge [3] in *Sense and Reference*, which was conceived of primarily in the context of science but we believe can be adapted to this context (Fig. 1).

This paper presents two major directions to handle the ensuing problems. One is the move towards an *Identinet*, where identities are at the end point of all communications. These identities may represent entities of all kinds including persons, devices and software. The other is to introduce the *digital shadow* of entities in the digital world. The digital shadow designates the concept of entities using services, nodes, equipment and the infrastructure in a specific context, which can help users to attach to possibly multiple entry points into the physical Internet without losing a consistent view on that data.

The paper is organized as follows. Section 2 introduces related work. Section 3 illustrates the interests of various stakeholders to consider in a future architecture to allow balances and trade-offs of such interests. Sections 4 and 5 then presents the two major directions this paper proposes—the *Identinet* and the *Digital Shadow*. Section 6 is on how the Internet of things is affected. Section 7 then presents the SWIFT architecture followed by conclusions in Sect. 8.

2 Related Work

The Daidalos project was one of the first to address identity management with a strong focus on network and service infrastructures. One of these results was the virtual identity concept [4,5] and its application to such infrastructures, where the virtual identity denotes an entity in a specific role or usage context, not the entity in its entirety. However, they have not addressed the problem of how the wide range of entities can be organized in establishing a particular use or session.

Available schemes, such Microsoft Passport [6] or Microsoft Cardspace [7], OpenID [8], or Liberty Alliance [9] approaches focus more on general Web 2.0 types of approaches without addressing explicitly how identity management copes with entities using the infrastructure or an Internet of things. However, new activities in the future may move in this direction as well.

The European project Privacy and Identity Management for Europe (PRIME) [10] has addressed privacy issues on controlling data scattered through different networks, but have not specifically addressed the organization of data in the network related to both the entities concerned and their relation with affected (used) elements of the infrastructure. The follow-up project PrimeLife has looked into infrastructure issues related specifically to trusted content [11]. Interoperability, privacy and mobility in the FIDIS project [12] also relate to parts of the problem addressed in this paper.

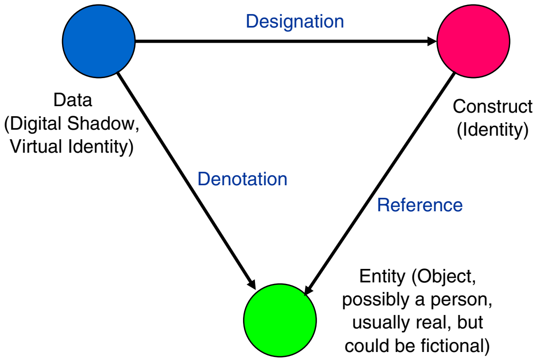


Fig. 1 Base assumptions on the approach

The ITU Internet Report 2006 digital.life [13] has shown the path that digital identities may take in an environment including Second Life. In parallel, the ITU-T Focus Group on identity management has developed use cases and requirements during 2007 for next generation networks (NGN) with scenarios that need to be extended in the context of the Internet of things [14]. These have now been taken up and further developed in ongoing work of the ITU-T Study Groups 13 and 17. Specific problems relate to mobility in an identity enabled infrastructure are dealt with by Matos et al. [15]. There are many requirements related to privacy and data protection formulated by official and particular EU sources that need to be taken into consideration for any future architecture [16–18]. Finally, 3G America has produced a white paper on the status of standardization reflecting the current state-of-the-art [19]. These directions and standards form the baseline for the further development of Identity schemes in the Future Internet of things.

3 Internet Stakeholder Interests

A future-proof solution must take into consideration the interests of relevant stakeholders (Fig. 2) from the first stages when a future architecture is designed. On the one hand, we target an optimized trade-off between three groups:

- *Users*, perhaps represented by devices or software: Their interest is mainly focused on utilization of services and the infrastructure and the properties associated with such use.
- *Providers* of services and the infrastructure: Their primary target is business, and thus ultimately to run profitable enterprises.
- *Society* including the legal framework: Their target is to protect the society at large and prevent illegal activities.

These interests may collide with each other, and so trade-offs will be required to ensure a smooth operation of the Internet. Also, the above roles are often not exclusive, with a single person perhaps in multiple interest roles. In the last years, the interest of all the above stakeholders has been compromised by a group of *attackers*. They seek to gain, either financially or otherwise by exploiting holes in the overall system. They utilize the system to their own benefit and at the cost of one of the above. Again, the roles here too may overlap (Fig. 2).

A key aspect for an architecture will be to cater for things the stakeholders do *not* want. These are negative requirements, such as a user not wanting to be reachable for some reason or another. This is a generalization of the spam problem, which now threatens other communication channels than email. Any new architecture must guarantee user controlled reachability. The user similarly would like to restrict or control what others know about him or her. At the same time, a provider may want to or legally be required to know some things about a user, such as the user's identity or at least some attributes, such as age or nationality. The provider may also want some information to better serve the user, or for advertising.

Finally, there are also requirements to counter some of the side-effects of increasing ubiquity and complexity of systems. Regaining control implies that the user should be able to initiate a specific "use" or session within the digital world, which requires a controlled set-up of end entities, such as users wishing to start a communication, via the ports of the digital world into the infrastructure, followed by a controlled collaboration of equipment or nodes in the infrastructure to enable such a session. Examples on entry ports for a user would be a terminal or a screen. Regaining control is one of the key points that the presented architecture will address, which includes representing not only the communicating entities, but also the interim nodes by identities.

Though some of the other problems, such as on reachability and privacy, are not directly addressed in this paper, the intention to mention them here is to ensure that the proposed architecture conceptually enables methods to solve them. An example is providing some means of identifying the end-points of a communication, and providing means to store the interests of the stakeholders securely in the digital world. These schemes must resolve not only reachability, but also the interests of the stakeholders in a dynamic environment.

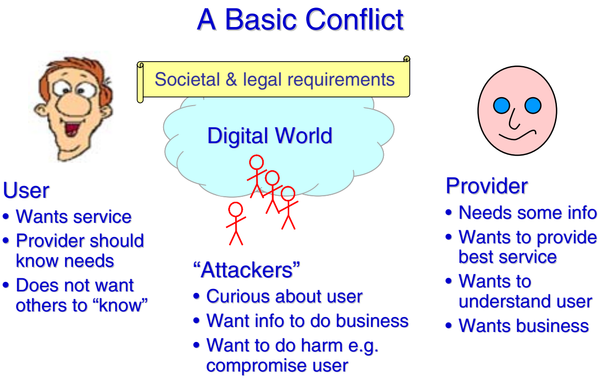
4 Identinet

The EU project Daidalos [1] was the first to address the issue of bringing identity management to the network, for which it first addressed identity and privacy across layers. This direction is being continued under the EU ICT FP7 project SWIFT [2], the work of which is reflected here. Both projects have addressed and are addressing a vertical approach to identity management, as well as how to leverage Identity technologies as an enabling technology for convergence.

SWIFT is now taking this to the next step towards making identities part and parcel of the Internet and future infrastructures. This is based on most actual needs of communications. Users want to communicate with each other, use a service, utilize some software, convey some information or steer some device. Today's communication end-points are instead the device or more specifically an interface such as those denoted by an IP address. The proposal makes it part of the solution that multi-homing, the aggregation of multiple interfaces for routing, becomes multi-homing to the user via possibly different devices, all of which may be associated to the same person in a service session. The general scheme is illustrated in Fig. 3, which makes the Future Internet of things an *Identinet*. Here, each end point, whether a person, a service, some software or a sensor cloud will be represented by an identity, that is again designated in its digital from as data, such as by a virtual identity [4]. Some devices now considered end points become interim nodes in the communication, each of which is also represented by an identity.

Since an entity that is represented by an identity is not confined to a specific class, such as persons, identity technology becomes a convergence technology potentially able to bridge service categories even into the physical world as will be illustrated in the next section. By allowing users to reason intuitively about a specific session or usage and the involved end

Fig. 2 Stakeholders


A Basic Conflict
Societal & legal requirements
Digital World
User
• Wants service
• Provider should know needs
• Does not want others to "know"
"Attackers"
• Curious about user
• Want info to do business
• Want to do harm e.g. compromise user
Provider
• Needs some info
• Wants to provide best service
• Wants to understand user
• Wants business

points, such an infrastructure becomes much easier to handle in the future "global village" that includes technically less savvy parts of the population.

This approach also has a further huge potential benefit. By having identities as the end-points, it becomes much easier to ensure (wanted) reachability to the end point independent of the device being used, such as a phone or laptop of a user, while providing the basis for filtering and prioritizing incoming communication requests that are linked to an identity, even if in pseudonymous form. The possibility to identify possibly misbehaving interim nodes is an additional benefit. By scoping the information required for routing between the devices of the user, the architecture provides privacy, both for the location of the user and the type of devices in the communication. The Identinet has thus the potential to bring back some of the lost security and privacy into world-wide communications by being able to identify, in a controlled and privacy-enabled manner, each end-point and intermediate node of a communication.

5 Digital Shadow

One entity's influence, denoted by its virtual identity, is not restricted to the one service it consumes. It could be said that such a presence occupies many network nodes and service support functions in the overall architecture. We have termed this data and its associated functions the digital shadow. The digital shadow thus represents the entity's uses and sessions, and contains the required information and the endpoint devices in the communication and service provisioning. The digital shadow is thus the projection of a virtual identity onto the logical nodes that compose the architecture, and denotes the logical end points and used interim nodes, as depicted in Fig. 1. Access to and manipulation of the digital shadow is tightly controlled and restricted to the entity itself and authorized providers that know the virtual identity and the context of its use. Even so, authorized providers may be further restricted to the sessions in which they are directly involved.

A virtual identity is a sub-set of the digital information about a user [4]. A user may have more than one virtual identity to represent the different personas and aspects of its service usage. More than a question of personalization, this mechanism should ensure the user's privacy across the aspects of its personality. A virtual identity may contain data relevant to many services and networks, including subscriptions, identifiers, service preferences, etc. While its logical understanding is that the information may be available from any point in the architecture, the information itself can be distributed and limited to access by only some

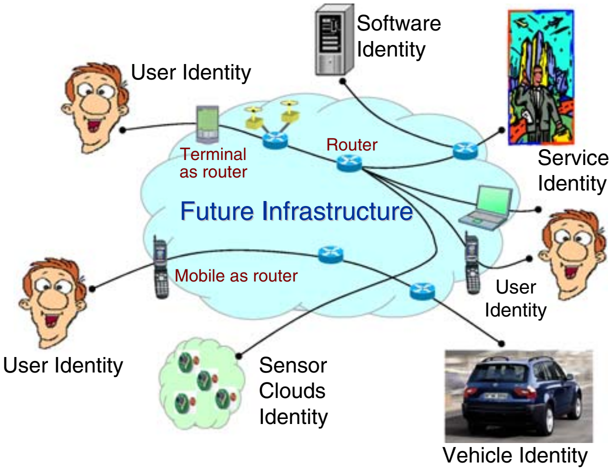


Fig. 3 Identinet as the end-point of communications

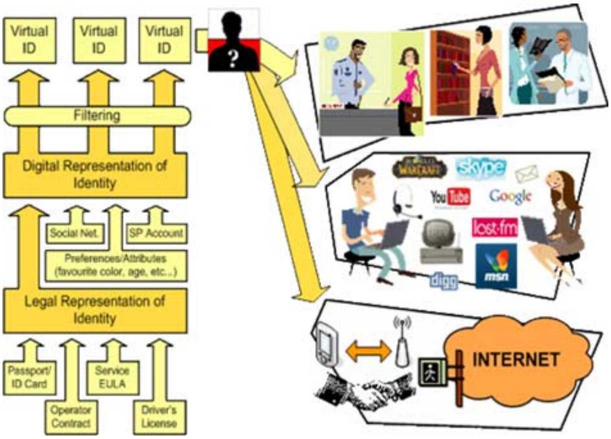


Fig. 4 The virtual digital world for a user

entities. As described in Fig. 4, the virtual identity can then be used in a transparent way to gain access to the network, services and even perform operations in the “real world”.

The digital shadow allows the user to excerpt its influence over multiple devices simultaneously by associating its virtual identity with those devices. In a similar manner, the user’s influence goes beyond owned devices, since it affects routers, proxies, servers, etc. This information can all be harnessed, for the user’s benefit, and provided to cross-domain and cross-layer operations. One example is that low level queuing information from a user’s flow in a router is provided to a higher level routing function to provide a better service to that particular user.

By scoping the information in a digital shadow, we limit its influence across domains. While some information is only valuable within the boundaries of a device, other is valuable across domains. General policies of the services, legal and user should reflect the privacy level of the operation and whether it is successful or not. The scoping of the information also

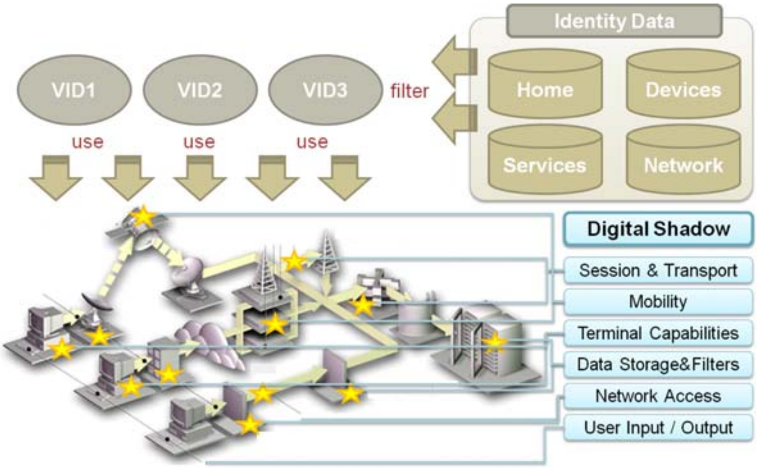


Fig. 5 Virtual identity model

means that a piece of data may be different depending on scope (or context). The difference may be caused by the source or access control on the data.

In the model depicted in Fig. 5, we see the relation between the virtual identity of the user and its counterpart, the digital shadow. The direct differentiation is that the virtual identity pertains to information about the user and the digital shadow its sessions and influence in the architecture.

6 Impact on the Internet of Things

The Internet of things describes a world where humans are surrounded by machines that communicate with each other and can allow people to interact with the digital world. To succeed in this vision, it is not only the people who need an understanding of this multi-device environment, but also the network needs a representation of "who" the user is. SWIFT provides a solution to this problem by considering the virtual identity as the endpoint of communication, independent of the device. The direct impact of this concept is that, in a world where humans are surrounded by machines, it is the user's virtual identity and digital shadow that is understood as consistent endpoint information; allowing users to interact with several devices, seamlessly, under one name.

Users project their virtual identity onto devices in the Internet of things by an authentication process, a temporary feeble association or a long term relation. The authentication process will allow a user to employ the services any device, public or not, as if it were its own.

A temporary volatile type of association is also required for usability purposes. It is often not possible to perform a strong authentication because of the nature of the device or the context in which it is being used. This type of association, while not as secure and strong as the first, will still allow the user to perform some non-critical operations on that device.

We also envision a long term kind of association. This type of relation should be used when the user is the owner of the device and the device is of everyday use. We can think of

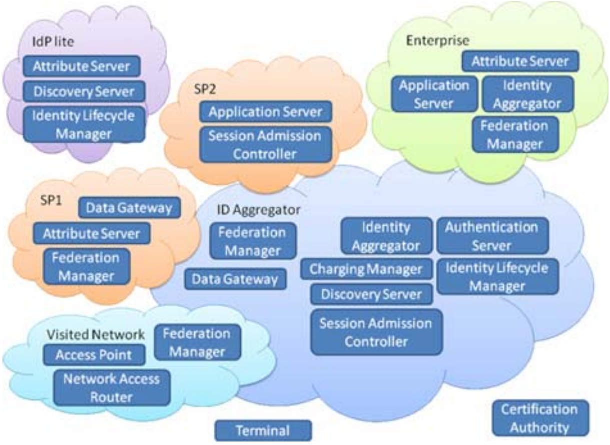


Fig. 6 Identity management deployment

a watch or phone, which, while not requiring constant authentication, is recognized by other devices as part of the user's digital shadow.

The problem of scope reappears, since identification is a product of the task the user wants to perform. While the user may want to identify its car for some service, it does not need to identify every communication-capable component in the car. In a similar manner, for a sensor network, it is many times the collective result which the user needs and not the individual sensor. These problems are addressed in how a digital shadow comes to influence the devices. One may look at a sensor network as a logical device and not as a collection of individual sensors.

7 The SWIFT Architecture

In building an architecture that can sustain the previously introduced concepts, we have to consider the distributed nature of data, the scope under which the data can be retrieved and the access control layer which defines data dissemination. As such, the architecture is constructed around the identity management functions and hierarchical in its nature. Different domains can exchange information about a virtual identity and its digital shadow.

Fig. 6 represents a deployment of SWIFT functions, for which we identify a number of involved nodes and network elements:

- *Terminal*: the device which has direct contact to the user.
- *Access Point*: logical entry point of the terminal in the network.
- *Network Access Router*: higher level functions of network access.
- *Session Admission Controller*: generalized name for session control functions.
- *Authentication Server*: provides user virtual identity recognition.
- *Attribute Server*: virtual identity attribute storage and management server.
- *Identity Aggregator*: identity aggregation functions for hierarchical deployment.
- *Discovery Server*: identity and service information directory and search functions.
- *Federation Manager*: cross domain information exchange negotiation functions.
- *Data Gateway*: cross domain information exchange and transformation functions.
- *Certification Authority*: root of trust.
- *Identity Lifecycle Manager*: identity information management.

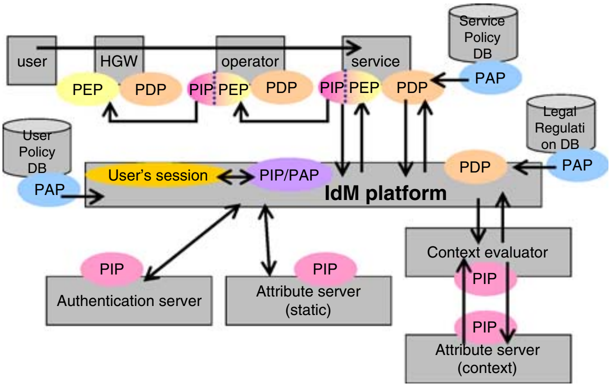


Fig. 7 Access control architecture

- *Charging Manager*: accounting, charging and billing functions.
- *Application Server*: service provisioning.

Together with the general architecture, we focus on the access control framework which will ensure the properties of scope and privacy towards its users. Figure 7 depicts the relations between those elements.

The SWIFT architecture is hierarchical and requires an access control infrastructure that copes with that property. Due to the scope of the information, a decision over a certain action can usually not be carried out in one place, since either the full policy is not known or the information required to make the decision is not fully present. At the same time, the policy for a decision might also be stored in a different location. By mixing these requirements, we propose an Access Control framework connected to the identity management platform.

Policy decision points (PDPs) and policy enforcement points (PEPs) are cascaded to allow a policy evaluation to occur distributed across domains. A policy administration point (PAP) is part of the attribute resolution functions on a virtual identity. This allows a PDP to simply use the same interfaces as a service to obtain a policy it requires. All elements are potential policy information points (PIPs) which source the information required for a decision from any point in the architecture.

8 Conclusions

We observe increasing requirements on ease of use of networks and services while maintaining privacy, and a proliferating number of "endpoints" including sensor clouds and of new networks types, such as vehicular networks. To solve the ensuing problems, this paper has proposed using identities, more precisely virtual identities, as representations of entities of all kinds as the end points of communication. It also proposes using digital shadows that represent projections of the entities involved in a communication use or in sessions. These new approaches will be validated within the EU ICT project SWIFT. The handling of the privacy of data in the network and the infrastructure will be one of the vital issues to solve, as the temporary collection of session data is a potential asset that can be exploited. Future work will need to ensure that privacy needs of users and governmental requirements on handling data are met. The increased ease of use and improved flexibility to support new services and means of access in a dynamic and collaborative environment must be matched with an increased support for privacy protection if the solution is to be accepted.

Acknowledgements This work has been partially sponsored by the EU-funded projects Daidalos and SWIFT. The authors thank and acknowledge a lot of the people involved in both projects who have contributed considerably to the work described here in various discussions.

References

1. Designing Advanced Network Interfaces for the Delivery and Administration of Location Independent, Optimised Personal Services (DAIDALOS). http://www.ist-daidalos.org.
2. Secure Widespread Identities for Federated Telecommunications (SWIFT). http://www.ist-swift.org/.
3. Bunge, M. On reference in relation to denotation and designation in "Sense and Reference". *Treatise on basic philosophy*, (Vol. 1, Semantics I, pp. 33–82).
4. Sarma, A., Matos, A., Girao, J., & Aguiar, R. L. (2008). Virtual identity framework for telecom infrastructures, *Wireless Personal Communications 45*(4), 521–543.
5. Aguiar, R. L., Sarma, A., Bijwaard, D., Marchetti, L., Pacyna, P., & Pascotto, R. (2007). Pervasiveness in a competitive multi-operator environment: The Daidalos project. *IEEE Communications Magazine, 45*(10), 22–26.
6. Microsoft Passport, Microsoft Developer Network (MSDN). http://msdn.microsoft.com/archive/en-us/passport25/start_full.asp.
7. Microsoft Cardspace, Microsoft Developer Network (MSDN). http://msdn.microsoft.com/CardSpace.
8. OpenID, OpenID Specifications, The OpenID Foundation. http://openid.net/developers/specs/.
9. Liberty Alliance, Liberty Alliance ID-WSF 2.0 Specifications. http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_ff_1_2_specifications.
10. Leenes, R., Schallerböck, J., & Hansen, M. (2008). Privacy enhancing identity management. del_CHT_D15.1.h_wp15. http://www.prime-project.eu.org/.
11. Spitz, S., Hinz, W., & Bergfeld, M.-M. (2008). Infrastructure for trusted content. http://www.primelife.eu/deliverables.
12. Future of Identity in the Information Society (FIDIS). http://www.fidis.net.
13. ITU, digital.life, Chapter 4. http://www.itu.int/osg/spu/publications/digitalife/.
14. ITU-T Focus Group on Identity Management. http://www.itu.int/ITU-T/studygroups/com17/fgidm/.
15. Matos, A., Sargento, S., & Aguiar, R. L. (2007). Embedding identity in mobile environments. In *The second international workshop on mobility in the evolving Internet architecture*, Kyoto, Japan.
16. European Community: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. (1995).
17. Article 29 Data Protection Working Party. Privacy on the Internet: An integrated EU approach to on-line data protection, 5063/00/EN, WP 37. (2000).
18. European Community: Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications) (2002).
19. 3G Americas, Identity Management—Overview of Standards and Technologies for Mobile and Fixed Internet. (2009). http://new.3gamericas.org/.

Author Biographies

Amardeo C. Sarma received his Bachelor of Technology degree from the Indian Institute of Technology, Delhi, in 1977 and his Master's degree (Diplom-Ingenieur) from the Technical University of Darmstadt in 1980, both in electrical engineering. He was at Deutsche Telekom and predecessor from 1981 to 1995, where he participated in several internal and international projects dealing with signalling, protocols, ATM, middleware and specification techniques. In 1995, he joined EURESCOM GmbH in Heidelberg as Project Supervisor, where he supervised international projects in the area of software technologies, middleware, ATM and IP. In April 2001, he joined NEC Laboratories Europe in Heidelberg, where he is currently responsible as senior manager for the areas identity management, security for restricted devices and car-to-car communication. He was chairman of ITU-T Study Group 10 from 1996 to 2001 and then co-chairman of the combined Study Group 17 on "Data Networks and Telecommunication Software" until 2004. He is ACM member, IEEE senior member and Steering Board member of the WWRF (Wireless World Research Forum). He is currently technical project manager of the European ICT "SWIFT" project within the 7th Framework Programme of the EU.

João Girão received his diploma from the University of Aveiro, Portugal, in 2003. Since 2003, he has been a member of the Ubiquitous Secure Communication group at NEC Laboratories Europe, in Heidelberg, where he currently occupies a senior researcher position and is responsible for technical coordination for the identity management area. From 2004 and on, he has been pursuing, in parallel, a PhD with the University of Bochum in the area of security for wireless sensor networks. In the past he has worked in security topics related to mobility and ad hoc networks, while his current focus is on applying identity management concepts to both services and the network. He is a member of both the IEEE and ACM.