Identity Management Requirements in Future Internet

Jenny Torres[1], Ricardo Macedo[2], Michele Nogueira[2], Guy Pujolle[1,3]

[1]Laboratory in Computer Science (LIP6) – University Pierre and Marie Curie
Paris – France

[2]Informatics Department – Federal University of Paraná
Curitiba – Brazil

[3]IT Convergence and Engineering – POSTECH
Korea

{Jenny.Torres,Guy.Pujolle}@lip6.fr, {rmacedo,michele}@inf.ufpr.br

Abstract. *The characteristics of the Future Internet and the emerging technologies result in new requirements, in which user security issues are highlighted. Identity Management requirements are linked to the development of systems able to prevent unauthorized use of digital identities, information overload, and to enhance user privacy. This paper highlights the Identity Management requirements in Future Internet context, based on its characteristics. Security and privacy were identified as key factors since they determine the overall trustworthiness of a system in terms of confidentiality, integrity and availability. Further, we introduce a discussion, in which we present the relationship between the Identity Management requirements and a future Internet scenario.*

1. Introduction

The increasing use of the Internet and the fast advance of new technologies have motivated the development of the Future Internet (FI) [Paul et al. 2011]. FI is supported by a network infrastructure, which increases the dependence on distributed information and decentralized control, requiring strong guarantees of security [Chim et al. 2011, Gomez-Skarmeta et al. 2010, Weber et al. 2010]. The main goal of the network infrastructure, known as Future Network, is to provide service-related functionalities independent of subjacent technologies. This network has as main characteristics the heterogeneity, dynamicity, interdependence and autonomy, increasing security issues and making difficult to protect services and applications.

In FI, Identity Management (IdM) plays a fundamental role. As a FI service, an IdM can assist the network infrastructure by providing information about user's profile, service features and access policies, in order to improve the efficiency of other services and to ensure network operation transparency, such as mobility, routing and others. IdM has attracted attention in recent years as an efficient way to provide trust between entities, protect or mitigate the effects of malicious entities, manage user's identities, identify entities in a system and control their access to resources [Sabena et al. 2010, Sarma and Girao 2009]. Features, such as security, determine the overall trustworthiness of a system in terms of performance, robustness and privacy. In the new paradigm of FI, many security problems are related to the concept of identity, such as the explosion of the number of identities, identity theft and identity impersonation [Van Rooy and Bus 2010, Wan et al. 2010].

The goal of this paper is to identify IdM requirements in FI based on its characteristics. There are many factors driving the adoption of IdM solutions, since their requirements vary depending on the proposal, applications and environment. The paper proceeds as follows. Section 2 provides an overview about the main characteristics of FI. Section 3 describes the core of IdM, which includes main definitions, operations and components. Section 4 presents the requirements for IdM systems in FI. Section 5 presents a discussion on the interaction between the requirements previously defined with a specific scenario. Finally, Section 6 concludes the paper.

2. Future Internet

In this section, we present FI from a service-oriented perspective and less protocol-oriented. For most users, the Internet is defined as a set of services, since they associate it with easy access to information and search engines, video and music availability or entertainment services. Understanding how users employ FI and the relationship between services with underlying communication networks is important to identify the requirements that the network infrastructure must support. Among those requirements, we have the connection of existing networks, survivability, support of multiple types of services, distributed management, cost-effectiveness, and resource accountability [Levin et al. 2009].

Among the advances of FI, shaped by Internet users behavior, we highlight the *personalized services*, which are strongly related to social networks. They digitally represent personal relationships and provide an important reference for identity and confidence issues in the Internet. Further, advances that should assist in defining FI are privacy and anonymity, which are becoming increasingly important for Internet users. On the other hand, as devices on cellular networks had been enabled for the Internet Protocol (IP) and sensors have been added to some networks, the Internet has gone mobile. The role of mobility has been changing over time and now it is considered one of the major features in FI. New challenges are centered on mobile access to networked information objects. FI is mainly related to the delivery of new services that will be provided in a pervasive and ubiquitous way, that is, anywhere, anytime and on any device through a selected communication technology. This is a heterogeneous environment where there are challenges as: security, quality of service (QoS) and costs. FI will integrate services offered by traditional networks and innovative IP services in a single service platform, and this integration should be as transparent as possible to the end user [Salsano et al. 2008].

3. Identity Management

This section overviews fundamentals of IdM, main concepts, operations and actors in IdM systems [Bosworth et al. 2005, ITU-T 2009]. An *entity* can be a person, a network service, a network computing device or a mobile telephone device. They use credentials and have a life cycle separated from any associated identity, identifier or credential life cycle. A *credential* is used to prove an identity to a system. There can be various types of credentials, but all are involved in ensuring a system that an entity truly has the right to use a particular identity. *Identity* is an instrument used by an entity in order to provide information about itself to the system. It is always associated with an entity or generally formed by a unique identifier, which is used to prove ownership of the identity. An *identifier* is a unique index for an identity. It must be unique within any given system, but might be reused across several. The main difference between identifiers and credentials

is the fact that an identifier must necessarily be unique and the credential not. Even being unique, the identifier can be the union of others identifiers not unique.

The four main operations of an IdM system are: identification, authentication, authorization and accounting [Bosworth et al. 2005]. *Identification* is the action of an entity providing an identity to the system through an identifier. The identification tells the system who user is trying to connect, but it offers no proof. To obtain proof of this identity, the system makes the *authentication* process where the connecting entity provides credentials for the claimed identity, known only by it. After authentication, the system can be certain that the entity is the rightful owner of the chosen identity. Each entity will have a set of actions allowed on the system. These permissions are known as privileges and are determined in the *authorization* stage. The system must look up the relevant privileges for the authenticated identity. Therefore there must be a binding of identity to privileges. Finally, *accounting* is a recording of what happened once authorization has been granted. It consists of a set of records, each one linking an established identity to an action.

In a general IdM system, we can identify three entities involved: user, identity provider and service provider [Cao and Yang 2010]. A *User (U)* is an entity that uses a service supplied by a service provider. Users use IdM systems to access services that require certification of their attributes by a third party. This is common in Internet access because users do not trust the security of data transmission. *Identity Provider (IdP)* is an entity that controls user's credentials and provides authentication services. *Service Provider (SP)* is an entity that offers one or more services from being accessed by potential users and uses the IdP services to authenticate a user.

4. Identity Management System Requirements in Future Internet

This section defines the requirements for IdM systems on the context of FI. Poorly designed IdM systems can aggravate existing security problems and create opportunities to extract personal information from users [Dhamija and Dusseault 2008]. We classify the requirements for IdM on the FI context as: *FI characteristics aware* and *IdM characteristics aware*, as illustrated in Figure 1. In the figure, we can see on the left side the requirements aware of FI characteristics and on the right side the requirements aware of IdM characteristics. The combination of these two kinds of requirements results in the requirements for IdM on the FI context.

In Figure 1, *privacy* is an important requirement in terms of law enforcement and user trust. The Internet and all technical communication have to comply with laws and regulations concerning the respective rights and privileges of the user and the provider. As FI involves the transfer of sensitive information between parties, protecting privacy can prevent personal information to be used improperly causing loose of autonomy and freedom. To maintain privacy, it should be possible for users to be anonymous, to use pseudonyms, to choose IdPs that do not link all user transactions at all SPs together and not to keep records of everything the user was doing. To ensure *security*, an IdM system has to be as robust as possible against attacks on the availability, integrity and confidentiality of its services and information. This is particularly important because of the concentrated amount of information about the user it stores and represents. Nevertheless, there are always risks of spying, manipulation and identity theft. Because of the amount of identity information stored and managed by organizations, security is an essential re-

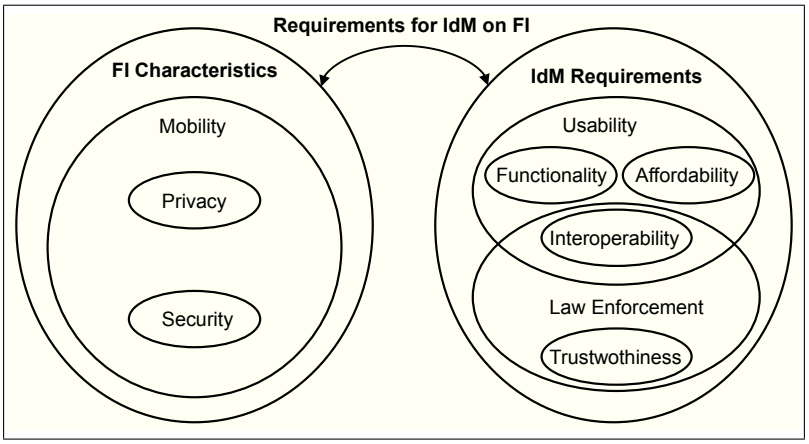

Figure 1. Requirements for IdMs on Future Internet

quirement for the SP. IdM systems require the user and the SP to place a large amount of trust in the IdP. All the identity information is stored at IdPs, and users can do nothing but trust them to preserve their privacy and secure their identity information.

In general, making IdM systems simple and easy to use reduces barriers to adoption. *Usability* refers to the effectiveness, efficiency, and satisfaction with which specified users achieve specified goals in particular environments [Levin et al. 2009]. A lack of usability can have a negative impact on functionality, security and privacy. Although many IdM systems claim to be designed with user in mind, most still have important usability issues [Alpár et al. 2011]. Considering the heterogeneous environment of FI and the complexity that can cause the lack of usability, IdM systems must be easy to use and its operations should be transparent for the user. Among some aspects missing in actual IdM systems there is the location independence, which means to create, manage, and use the identities independently of their current location and current device in use. Any enhancement of usability is more a question of *affordability*. Every technology needs to be affordable to become widely accepted. This applies to all kinds of users but can be rephrased to the question if the IdM system only adds overhead or enhances the functionality or quality of a given transaction. Organizations will look at IdM systems less from a cost but from a cost-effectiveness angle. In other words, the benefits of an IdM system need to outweigh its direct and indirect cost.

Mobility is very important in the growing use of portable devices. In a mobile environment, a user has several devices such as telephones, smart cards or RFID (Radio Frequency ID). As these devices have fixed identifiers, they are essentially providing a mobile identity. The mobility in IdM takes into account location data of users in addition to their personal data. Mobile IdM empowers users to manage their identities to enforce their security and privacy interests. Privacy and the protection against identity theft are important criteria for services that use mobile identities. However, in addition to privacy, also usability is important for the success of mobile IdM. Usability influences the correctness of security mechanisms. In mobile IdM, users must be able to control the disclosure of their identity and also their location.

The main *functionality* of IdM systems is to help the user to manage their identities. An IdM system has to provide the possibility of managing partial identities and

identity data. It is also necessary for IdM systems to have interfaces to the communication partners, especially to digital networks. An IdM system can act as gateway for digital communication. This gateway functionality lets it to manage data exchange with all communication partners. IdM systems incorporate the gateway functionality by definition, because IdM is always a process between the user and another party. Typically, organizations will have to manage members' and associates' identity information, thus different kinds of identities. Functions for controlling this complexity and keeping it up-to-date are part of the main basic requirements of functionality that must be considered when proposing an IdM system.

Trustworthiness is a prerequisite for all transactions, which defines if a user trusts the SP or the system. Even in systems where the user has complete control over hardware, software and data flow, a certain amount of trust is still required because the complexity of the system demands transparency. Therefore, the reputation of software and hardware suppliers and SPs becomes an asset in the market. Although the notion of trust may depend on many factors, it is clear that privacy, security and usability are preconditions for trustworthiness. Also the law enforcement influences the perception of trust. Agencies responsible for control and *law enforcement*, such as police departments or criminal investigative practices are typically interested in collecting as much information as possible for giving evidence and make criminal proceedings easier and more effective. Any IdM system has to take care about the legal requirements for law enforcement of the countries where it should be used. However, these requirements are sometimes contradictory in different countries and even regions within a country, as the result of different cultures and realities.

Interoperability among existing systems is a basic requirement for an IdM system. IdM systems should implement interfaces compatible with international standards. It is possible that certain players will resist compatible interfaces in order to protect their market position. In such a case, the acquisition of critical mass for IdM systems as a product may be more difficult. Trust regulations may be able to regulate conventional trends in the market. Achieving interoperability across different contexts is impossible without a coherent semantic foundation in the culture and society where the IdM systems intend to be used.

5. Discussion

This section discusses how the requirements described in Section 4 can be observed in a realistic context of FI. The scenario is inspired by the Pervasive Healthcare example presented in [Akinyele et al. 2010]. We have chosen a pervasive healthcare context to search solutions that enable continuous monitoring of the health on chronic patients through the use of embedded wireless sensors. With this technology, it is also possible to obtain a larger amount of information about patient's health, including the creation of medications produced according to the specific needs of a person. In this scenario, it is necessary to make a communication between the sensors that will monitor patients and devices for storage of medical information. Therefore, the efforts of non-disclosure of data collected about patient health to unauthorized persons highlight the necessity for data *privacy*. Consider an attacker who removes the information stored about a patient or makes it unavailable. For instance, suppose that he is allergic to penicillin. In this case, this patient can receive a medication based on penicillin and as a result may manifest symptoms of

faints. Thus, the need to ensure that data collected is exactly the same than that stored and to guarantee that it is always available when required show the necessity for *security*. *Usability* requirement is related to security too. Users must understand which security actions are required of them, to not disclose their personal data. While to make the use of data collected feasible for any type of user, it requires *affordability*.

In conjunction with the computerization of healthcare, there is the concept of Electronic Medical Records (EMR) [Benaloh et al. 2009]. The EMR is the on-line *availability* of information about a patient with restrictions access. Since this information may only be disclosed to the patient, your doctor or in an emergency, this information may be disclosed to other doctors. Based on the location of the patient in an emergency procedure could be created to make available information about the patient to the doctor that is closer to employ the requirement for *mobility*. The *functionality* can be achieved by considering the creation of several partial identities in order to use a specific identity for medical information, isolating this information from other identities. The requirement *trustworthiness* can be used by trust between the patient's body sensors and data storage service. Finally, consider two cities *A* and *B* each one has a unique IdM for health monitoring of patients using different technologies. The requirement for *interoperability* exists when a chronic patient travels from city *A* to city B, for example.

6. Conclusions and Future Work

FI asserts that the digital world is becoming more flexible, interconnected and open. Boundaries between enterprises, organizations and government agencies are getting indistinct as people cover multiple roles and are involved in different activities across heterogeneous environments, creating new threats and issues. IdM need has a strategic role achieving this new world and addressing these new issues. A new generation of IdM solutions is needed to provide mechanisms to rapidly adapt and affront changing environments, in business, personal and social contexts.

In this paper, we highlighted the requirements of IdM for FI. IdM plays a key role in enabling personal and business activities along with interactions and transactions in the digital world. Although IdM has strong links with the management of security and privacy, the security component is only a small area, due to there are much more requirements and technologies needed to achieve IdM systems. IdM systems still have challenges today. Among these challenges, there are those related to security, privacy and usability that must be treated in order to become more suitable for FI. Beyond these issues, the IdM systems developed for FI need to be interoperable, since heterogeneous technologies are expected to work together. The network infrastructure needs to achieve these requirements in order to not compromise services. Different IdM systems will have different trust requirements, since there are costs associated with establishing trust.

References

Akinyele, J. A., Lehmann, C. U., Green, M. D., Pagano, M. W., Peterson, Z. N. J., and Rubin, A. D. (2010). Self-protecting electronic medical records using attribute-based encryption. *IACR Cryptology ePrint Archive*, 2010.

Alpár, G., Hoepman, J., and Siljee, J. (2011). The identity crisis security, privacy and usability issues in identity management. *Identity Management on Mobile Devices*, abs/1101.0427.

Benaloh, J., Chase, M., Horvitz, E., and Lauter, K. (2009). Patient controlled encryption: ensuring privacy of electronic medical records. In *Proceedings of the 2009 ACM workshop on Cloud computing security*, CCSW '09, pages 103–114, New York, NY, USA. ACM.

Bosworth, K., Lee, M. G. G., Jaweed, S., and Wright, T. (2005). Entities, identities, identifiers and credentials - what does it all mean? *BT Technology Journal*, 23(4).

Cao, Y. and Yang, L. (2010). A survey of identity management technology. In *Information Theory and Information Security (ICITIS), 2010 IEEE International Conference on*, pages 287–293.

Chim, T., Yiu, S., Hui, L., and Li, V. (2011). SPECS: secure and privacy enhancing communications schemes for VANETs. *Ad Hoc Network*, 9:189 – 203.

Dhamija, R. and Dusseault, L. (2008). The seven flaws of dentity management: usability and security challenges. *IEEE Security and Privacy*, 6:24–29.

Gomez-Skarmeta, A. F., Martinez-Julia, P., Girao, J., and Sarma, A. (2010). Identity based architecture for secure communication in Future Internet. In *The 6th ACM Workshop on Digital Identity Management*, pages 45–48, Chicago, Illinois, USA.

ITU-T (2009). NGN Identity Management framework. Recommendation ITU-T Y.2720. December.

Levin, A., Sutherland, E., and Choe, Y. (2009). The Future Internet. Technical report, International Communication Union - ITU.

Paul, S., Pan, J., and Jain, R. (2011). Architectures for the future networks and the next generation internet: a survey. *Computer Communications*, 34:2–42.

Sabena, F., Dehghantanha, A., and Seddon, A. P. (2010). A review of vulnerabilities in identity management using biometrics. In *International Conference on Future Networks*, pages 42–49.

Salsano, S., Polidoro, A., Mingardi, C., Niccolini, S., and Veltri, L. (2008). Sip-based mobility management in next generation networks. *IEEE Wireless Communications*, 15(2):92–99.

Sarma, A. and Girao, J. (2009). Identities in the Future Internet of Things. *Wireless Personal Communication*, 49:353–363.

Van Rooy, D. and Bus, J. (2010). Trust and privacy in the future internet, a research perspective. *Identity in the Information Society*, 3:397–404. 10.1007/s12394-010-0058-7.

Wan, M., Liu, Y., Zhou, H., and Zhang, H. (2010). A chord-based handoff authentication scheme under id/locator separation architecture. In *Advanced Intelligence and Awarenss Internet (AIAI 2010), 2010 International Conference on*, pages 309–314.

Weber, S., Martucci, L., Ries, S., and Mühlhäuser, M. (2010). Towards trustworthy identity and access management for the Future Internet. In *Trustworthy IoPTS: The 4th International Workshop on Trustworthy Internet of People Things and Services*, Tokyo, Japan.

