A trustworthy and privacy-enhancing registration process for social network services

Ana Ballester[1], David Campos[1], Francisco Jordan[2], Jorge Palacio[1], Helena Pujol[2]

[1] Distributed Multimedia Applications Group, Universitat Politècnica de Catalunya
[2] Safelayer Secure Communications, S.A.
{anab, dcampos, jpalacio}@ac.upc.edu
{jordan, helena.pujol}@safelayer.com

Abstract. The increasing popularity of social network services (SNS), being used by millions of people everyday, has arisen some security and privacy issues. While users must be free to choose which amount of personal information they provide, SNS providers should get more involved to guarantee that their services are correctly exploited. This leads us to propose a more secure but still privacy-enhancing solution for registration processes, that involves the use of digital certificates —which are a reliable source of personal information—, as well as information cards —which hold privacy properties. Safelayer applications PKI Trust Center and Interidy Identity Provider implement this proposal.

Keywords: digital certificate, information card, privacy, social network service, tagging, trust

1 Introduction

Online Social Network Services (SNS) have revolutionized the way we communicate and cooperate with others. Most users seem to be willing to publish their personal data, agenda and even thoughts, but they are seldom aware of the potential risks they may be exposed to, when they make this kind of information available indiscriminately or when they get in touch with unfamiliar people. Obviously, this is critical when children and young people are involved.

Concerned about this sociological challenge, the European Commission has actively contributed to develop the Safer Social Networking Principles for the EU [1], together with 20 SNS providers and a number of NGOs, which propose good practice recommendations to enhance the safety of children and young people using these services.

Although access control and transparency, as well as education, are essential to improve security in the Information Society, it is also important to improve the trustworthiness of registration processes. For example, most SNS are targeted at users 14 and over, but there are also other SNS that only accept users aged 13 to 17, like Teen Second Life. Besides, there are SNS that are targeted at a professional audience, whereas others belong to a single organization. Therefore, some mechanisms should

be established to ensure that registered users hold some particular attributes, while they still should have the chance of registering with privacy, for instance, using a pseudonym.

1.1 Providing trustworthy attributes

SNS providers usually delegate the trustworthiness of the information collected during the registration process to the user. This is achieved by including an explicit clause in the terms of service, which the user must declare to have read and accept in order to register. However, SNS providers, authorities and even users should not rely on such a weak trust mechanism when their very privacy and security may be exposed.

Digital certificates are a trustworthy source of personal data. They involve a Certification Authority, which is a trusted third party which guarantees that the personal attributes stated by the certificate are true and correspond to the certificate's holder. The legal document that describes how a Certificate Authority manages the life-cycle of the certificates it issues is known as Certification Practice Statement, and follows the RFC 3647 [2]. Consequently, not all digital certificates are equally reliable, as each Certification Authority is ruled by its own procedures. In particular, many Certification Authorities require the physical presence of the future certificate holder at one point of the certificate issuance process, while others don't. This kind of requirements, as well as the cryptographic characteristics of the associated keys, determines the level of trust that can be put in a Certification Authority.

1.2 Ensuring privacy

Digital certificates represent a huge source of reliable data. In the particular case of Spain, more than 14 million citizen e-ID cards [3] have already been issued. However, digital certificates identify users unequivocally, and therefore they are not suitable for applications that require a higher level of privacy during the user registration process, like SNS. So, in order to get benefit from this already deployed infrastructure, we could think of a mechanism that complemented it by providing more privacy.

This may be achieved with information cards [4], which can be seen as an electronic version of conventional cards in our wallets. Information cards involve the user in the personal data disclosure process, allowing him to decide which particular personal attributes (name, age, nationality, etc.) he wants to reveal to the service provider, in this case, the SNS.

2 Signing up with trustworthiness as well as privacy

By combining the trust infrastructure of digital certificates and the privacy-enhancing properties of information cards, a more reliable and confidential authentication mechanism can be implemented.

Safelayer's PKI Trust Center compiles and displays Certification Practice Statements information in a user-friendly way, and compliments it with contributions from Certification Authorities administrators and users, in a Web 2.0 style. The technology underneath is based on ontologies and Semantic Web standards like OWL and RDF, which make information machine readable and processable. By the use of data mining techniques a trust rating is automatically inferred for each Certification Authority.

In addition, Safelayer's Interidy Identity Provider is set to issue information cards with personal attributes that are imported from digital certificates. The criterion that determines if the imported personal data is trustworthy enough is the trust rating provided by PKI Trust Center.

So, a user should fulfill two steps in order to register in a social network application with privacy. First, the user should generate an information card from one of his personal certificates using Interidy Identity Provider. This card would contain a set of verified claims. Afterwards, the user could complete the registration process by presenting this information card to the social network registration service

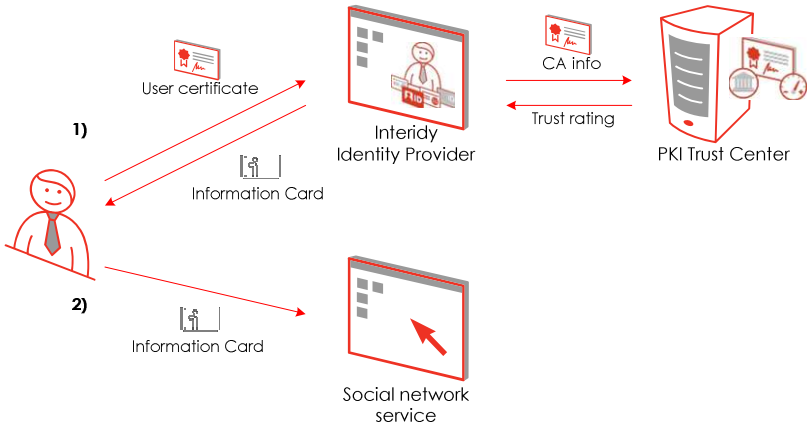

Fig. 1. First, the user generates an information card from a digital certificate, and afterward, the user completes the registration process at the social network application.

With this solution, as the user is able to reveal only a minimum subset of required personal attributes (for example, being over 14), his privacy is preserved and he is entitled to use pseudonyms all through the registration process.

3 Conclusion

Two main requirements should be ensured during the registration process of a user in a social network online service. On the one hand, a user should be able to register with enough privacy guarantees, even with a pseudonym in case he didn't want to

disclose his real name. On the other hand, the service provider should be able to validate that its users fulfill certain criteria, being one of the most critical, the fact that they all belong to a particular age range. Therefore, a third party is needed to act as a Certification Authority that will bind authentic identity attributes to end entities, but a privacy-respecting authentication mechanism is desirable so that users are required to disclose the minimum set of identity attributes.

This solution may be achieved by combining the functionalities of Interidy Identity Provider and PKI Trust Center applications, which are available at Safelayer Sandbox website [5].

Acknowledgments. This research has been supported by Safelayer Secure Communications and the Centre for the Development of Industrial Technology (CDTI) of Spain, within the framework of the Segur@ project, reference CENIT-2007 2004 of the CENIT Program (part of the INGENIO 2010 initiative) [6].

References

1. "The Safer Social Networking Principles for the EU", Europe's Information Society Thematic Portal, Safer Social Networking Activity, 2009, http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf
2. S. Chokhani, W. Ford, R. Sabett, C. Merrill, S. Wu, "RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", Internet Engineering Task Force, 2003
3. Portal oficial sobre el DNI electrónico, http://www.dnielectronico.es/
4. Information Cards, http://informationcard.net/
5. "Proyecto SEGUR@ - Seguridad y Confianza en la Sociedad de la Información", http://www.cenitsegura.com
6. Safelayer Sandbox, http://sandbox.safelayer.com