IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 3 Issue 12, December 2016
ISSN (Online) 2348 – 7968 | Impact Factor (2015) - 4.332
www.ijiset.com

Digital Identity

Matthew N. O. Sadiku [1], Adebowale E. Shadare [2] and Sarhan M. Musa [3]

[1, 2] Department of Electrical & Computer Engineering, Prairie View A&M University, Prairie View, TX 77446, USA
[3] Department of Engineering Technology, Prairie View A&M University, Prairie View, TX 77446, USA

Abstract

Digital identity is an emerging legal concept as a result of government services and businesses going online. It is responsible for the way government is providing essential information and services and interacting with its citizens. It is increasingly becoming significant from legal and commercial viewpoints as personal, legal, and commercial transactions are performed electronically. This paper presents a brief introduction to digital identity.

Keywords: *digital identity, electronic identity (e-ID), online identity, paper identity*

1. Introduction

Identity is now routinely being used for commercial and legal transactions. Traditional identity documents used in face-to-face environments do not meet the needs of today's societies, which have been transformed from analog to digital. We live in an age where companies track our digital identities (full name, date of birth, gender, online behaviors, etc.) and sell the information to another companies as a form of intellectual property. As individuals, governments, and businesses increasingly transact online, the need to establish digital identity has increased.

A digital identity (DID) or electronic identity (e-ID) is the digital representation of the information on a person, organization or object. It is the computer network equivalent to the real identity of a person or entity. It is information about a person, organization, or device used by computer networks to represent us. This information can be used for many purposes such as proving one's identity. Like real identity, a person's digital identity may include:

- Username
- Passwords
- Date of birth
- Social security
- Online search activities

This information is available in our electronic ID, driving licenses, and passports. The digital identity is the primary means to have access to digital government, employment, social security benefits, health care, and tax filling [1].

2. Identity Management

To secure digital identity, a system management must be in place. This management is important in customizing users, protecting privacy, and complying with regulations. Right now, there is no way of determining a person's identity in the digital world. There is lack of common standard among electronic services: some demand four-digit PINs, while others require usernames and passwords. Today, passwords are no longer efficient to assure security because of password proliferation (the need to remember several passwords). Most of the current laws are old and local and were not designed for computer networks.

New technologies are emerging to help protect digital identities and build trust [2,3]. The smart identity card has been applied for remote transactions. The Public Key Infrastructure (PKI) forms the basis of digital signatures and certificates. PKI is being used by the banking and finance sectors where sensitive information must be handled with strong authentication [4]. The use of smart identity cars, PKI, and biometrics bridges the digital and the physical identity.

All digital identity schemes depend on authentication of identity and verification of identity [5]. The authentication process establishes the user's identity. Verification ensures that the information is reaching the right individual seeking it. The management of digital identity has not reached a level of maturity that would enable full realization of ecommerce [6].

3. Challenges

Some of the challenges faced by digital identity include privacy, security, identity theft, and interoperability.

***Privacy*:** Online privacy (a slight misnomer) can protect most of the personal information constituting a person's digital identity. The digital commerce requires the use of a digital identity to transact. This requirement makes digital identity vulnerable. The damage caused when the identity of the individual is compromised by system malfunction can be harsh and long-lasting.

***Security*:** As personal and commercial transactions are now performed online and across national borders, the issue of security appears urgent. Establishing trust in online security systems is challenging.

***Identity Theft*:** This refers to the act of impersonating identities of others. Digital identity may contain some sensitive information which can be targets of attacks such as identity theft. Cyberspace is an opportunistic place for identity theft. Digital identity becomes a source of anxiety as people online plunder bank accounts, steal identities, or commit fraud [7].

***Interoperability*:** This implies that when a digital identity is issued by one organization, it is recognized by other entities. Some have suggested some form of "electronic passport" or "digital wallet" to create a globally accept identity. Digital identity interoperability is facilitated by a common language to represent all attributes of digital identity (such as Security Assertion Mark-up Language (SAML) from OASIS – Organization for the Advancement of Structured Information Standards) and a transparent standard hierarchy.

4. Conclusion

Digitalization of government services is motivated by the need to reduce costs and increase efficiency. Providing quality information and services to citizens is the goal of digital governments. Digital identity describes the virtual identity of a user in a computer network. It has become the primary means by which a person relates in the digital world. The ability to identify individuals from basic data such as date of birth and sex has never been easier. As digital identity systems become more global and complex, there is a decrease in trust. Ultimately, you should protect your digital identity because no one cares more about the validity of the information than you [8].

References

[1] C. Sullivan, "Digital citizenship and the right to digital identity under international law," *Computer Law & Security Review*, vol. 32, 2016, pp. 474-481.
[2] C. Evans-Pughe, "Engineering Digital Identity," *Engineering & Technology*, pp.16-18 June 2008.
[3] A. Master, "Digital identities can tame the wild, wild web," *Information Systems Security*, vol. 13, no. 6, 2005, pp. 15-22.
[4] J. Eaton, 'Open, Sesame?' – the problems of digital identity and secure access to information in the Internet era: issues for information industry," *Business Information Review*, vol. 16, no. 4, Dec. 1999, pp. 184-191.
[5] C. Sullivan, "Digital identity, privacy and the right to identity in the United States of America," *Computer Law & Security Review*, vol. 29, 2013, pp. 348-358.
[6] A. M. Al-khouri, "Digital identity: transforming GCC economies," *Innovation: Management, Policy & Practice*, vol. 16, no. 2, 2014, pp. 184-194.
[7] I. Bourass et al., "Towards a new model of management and securing digital identities," *Proceedings of the Fifth Conference on Next Generation Networks and Services*, May 2014, pp. 308-312.
[8] P. Simmonds, "The digital identity issue," *Network Security*, August 2015, pp. 8-13.

About the Authors

Matthew N.O. Sadiku is a professor at Prairie View A&M University, Texas. He is the author of several books and papers. He is a fellow of IEEE.

Adebowale E. Shadare is a doctoral student at Prairie View A&M University, Texas. He is the author of several papers.

Sarhan M. Musa is a professor in the Department of Engineering Technology at Prairie View A&M University, Texas. He has been the director of Prairie View Networking Academy, Texas, since 2004. He is an LTD Spring and Boeing Welliver Fellow.