Proceedings of the 15th International Conference on Quality and Dependability
Sinaia, Romania, September 14th-16th, 2016
ISSN 1842-3566
Pages 225-232

Using Digital Signature to Ensure Information Security

Gabriel PETRICĂ, Ioan C. BACIVAROV
Laboratorul EUROQUALROM, Facultatea de Electronică, Telecomunicaţii şi Tehnologia Informaţiei, Universitatea POLITEHNICA din Bucureşti, România
gabriel.petrica@upb.ro, bacivaro@euroqual.pub.ro

Abstract
The digital signature is an encrypted mark of authentication, embedded in documents and emails or used in Internet communications, which ensures the integrity and security of data transmitted. Using the digital signature brings additional benefits: the identity of the signer can be verified, ensure product authenticity and transmitted data encryption. The high degree of security conferred by digital signatures is ensured by the use of encryption with public key and hash functions (which determines whether or not the information has been changed). This paper shows how to use digital signatures and certificates to ensure authentication and encryption of information (from simple text to complex documents).

Keywords: digital signature, digital certificate, hash function, Public Key Infrastructure, encryption

References:

[1] H.G. nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică, Monitorul Oficial, Partea I, nr. 296 din 23.05.2013.
[2] Regulamentul (UE) nr. 910/2014 al Parlamentului European şi al Consiliului din 23 iulie 2014 privind identificarea electronică şi serviciile de încredere pentru tranzacţiile electronice pe piaţa internă şi de abrogare a Directivei 1999/93/CE, http://eur-lex.europa.eu/legalcontent/ RO/TXT/?uri= CELEX%3A32014R0910
[3] Digital Signature Standard (DSS), FIPS PUB 186-4, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, http://nvlpubs.nist.gov/nistpubs/FIPS/NIST. FIPS.186-4.pdf
[4] Registrul furnizorilor de servicii de certificare, Ministerul Comunicaţiilor şi Societăţii Informaţionale, http:// www.mcsi.ro/Minister/Domenii-de-activitate-ale-MCSI/ Tehnologia-Informatiei/Servicii-electronice/Semnaturaelectronica/ Registrul-furnizorilo-de-servicii-de-certificare-P
[5] Ioan-Cosmin Mihai, Gabriel Petrică, Costel Ciuchi, Laurenţiu Giurea: "Provocări şi strategii de securitate cibernetică", Editura Sitech, Craiova, 2015, 230 pag., ISBN 978-606-11-4951-3.
[6] J. Habraken: "Office 2013 In Depth", Que Publishing, 2013.
[7] Microsoft TechNet Library, https://technet.microsoft.com
[8] Lisa Bucki, J. Walkenbach, M. Alexander, R. Kusleika, and F. Wempen: "Microsoft Office 2013 Bible: The Comprehensive Tutorial Resource", John Wiley & Sons, 2013.
[9] About certificate signatures in Adobe Acrobat, Acrobat Help, https://helpx.adobe.com/acrobat.html

Proceedings of the 15th International Conference on Quality and Dependability
Sinaia, Romania, September 14th-16th, 2016
ISSN 1842-3566
Pages 225-232
[10] X.509 standard, ITU, https://www.itu.int/rec/T-REC-X.509
[11] Public Key Infrastructure, https://en.wikipedia.org/wiki/ Public_key_infrastructure