Asigurarea Calitatii - Quality Assurance, ISSN 1224-5410
Vol. XXIV, Issue 93, January-March 2018
Pages 22-27

SSL Digital Certificates Analysis

Gabriel PETRICĂ, Sabina-Daniela AXINTE,
Ioan C. BACIVAROV
EUROQUALROM, Facultatea de Electronică, Telecomunicații și Tehnologia Informației,
Universitatea POLITEHNICA din București, România
gabriel.petrica@upb.ro

Abstract
The explosive development of Internet services has led to the appearance of security threats regarding transmitted or stored data privacy. A powerful solution for the authentication of Web servers is the SSL digital certificates, a collection of data through a recognized Certificate Authority attests an entity's identity on the Internet and confirms its public key, used to encrypt communications between the client (Web browser) and that server providing a certain Web service. This paper discusses the concepts of digital signature and digital certificate, making an incursion in the field of SSL digital certificates for Web servers.

Keywords: digital signature, digital certificate, SSL digital certificate, Certificate Authority, public key encryption

References:

[1] Joshua Davies, "Implementing SSL/TLS Using Cryptography and PKI", Wiley, 2011, ISBN 978-0470920411.
[2] Ioan-Cosmin Mihai, Gabriel Petrică, Costel Ciuchi, Laurențiu Giurea, "Provocări și strategii de securitate cibernetică", Editura Sitech, Craiova, 2015, ISBN 978-606-11-4951-3.
[3] Microsoft TechNet Library, https://technet.microsoft.com (accesat la 21 aprilie 2017).
[4] Public Key Infrastructure, https://en.wikipedia.org/wiki/Public_key_infrastructure (accesat la 15 aprilie 2017).
[5] Stephen A. Thomas, "SSL&TLS Essentials: Securing the Web", Wiley, 2010, ISBN 978-0471383543.
[6] Registrul furnizorilor de servicii de certificare, Ministerul Comunicațiilor și Societății Informaționale, http://www.mcsi.ro/Minister/Domenii-deactivitate- ale-MCSI/Tehnologia-Informatiei/Servicii-electronice/Semnatura-electronica/Registrul-furnizorilo-de-servicii-de-certificare-P (accesat la 2 aprilie 2017).
[7] Legea nr. 455 din 18 iulie 2001 privind semnătura electronică, Monitorul Oficial nr. 429 din 31 iulie 2001, http://www.cdep.ro/pls/legis/legis_pck.htp_ act_text?idt=28985 (accesat la 10 august 2017).
[8] Advanced security settings, Google Chrome Help, https://support.google.com/chrome/answer/95572?hl=en (accesat la 3 mai 2017).