P. J. Šafárik University in Košice
Faculty of Science

THESIS ASSIGNMENT

Name and Surname: Jakub Ďuraš
Study programme: Applied Informatics (Single degree study, bachelor I. deg., external form)
Field of Study: 9.2.9. applied informatics
Type of Thesis: Bachelor thesis
Language of Thesis: English
Secondary language: Slovak

Title: Open digital signature software

Title SK: Otvorený softvér na elektronické podpisovanie

Aims:
1. Explore the principles and global legal status of digital signatures.
2. Review current digital signature software.
3. Propose and develop open-source, cross-platform, and user-friendly software compliant with eIDAS Regulation (Regulation No 910/2014) for digital document signing.

References:
1. Christof Paar and Jan Pelzl: Understanding Cryptography - A Textbook for Students and Practitioners, Springer, 2009, ISBN 978-3-642-04100-6
2. Stephen Mason: Electronic Signatures in Law - Fourth Edition, Humanities Digital Library, 2016, ISBN 978-1-911507-01-7, http://humanities-digital-library.org/index.php/hdl/catalog/view/electronicsignatures/1/86-1
3. Mike Rosulek: The Joy of Cryptography, School of Electrical Engineering & Computer Science, Corvallis, Oregon, USA, 2019, http://web.engr.oregonstate.edu/rosulekm/crypto/crypto.pdf

Annotation: With the recent changes in the legal status of digital signatures in many parts of the world, there is a need for easily accessible solutions intended as an alternative to handwritten signatures. This may be more necessary than ever since digital communication is the preferred way of communication. This bachelor thesis aims to explore the principles and legal status of digital signatures, review current digital signature software, and explore possible obstacles the open-source community is facing to develop such specialized applications. We propose an open-source, cross-platform, and user-friendly software compliant with the eIDAS Regulation (Regulation No 910/2014). Our application should allow ordinary users to quickly sign and verify signatures of different types of documents and therefore easily use them in everyday life.

Keywords: digital signature, digital seal, qualified, open-source, XAdES, PAdES, CAdES, desktop software

Supervisor: RNDr. Viliam Kačala
Rektorát, dekanát : Dek. PF UPJŠ - Dean's office
Electronic version available: unlimited

Approved: Prof. RNDr. Viliam Geffert, DrSc.

riaditeľ ústavu