P. J. Safarik University

Faculty of Science

OPEN ELECTRONIC SIGNATURE SOFTWARE

BACHELOR'S THESIS

Field of Study:	**Applied Informatics**
Institute:	**Institute of Computer Science**
Tutor:	**RNDr. Viliam Kačala**

Košice 2020

Jakub Ďuraš

Acknowledgments

Thanks to the Planet!

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

Abstrakt

Abstrakt v SK jazyku bude pridaný neskôr ako voľný preklad z EN verzie (pozri ďalšiu stranu). Predíde sa tak zbytočnej práci keďže EN abstrakt sa môže časom meniť.

Kľúčové slová: *elektronický podpis, elektronická pečať, kvalifikovaný, open-source, XAdES, PAdES, CAdES, počítačový softvér*

Abstract

With the recent changes in the legal status of electronic 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 electronic communication is the preferred way of communication. This bachelor thesis aims to explore the principles and legal status of electronic signatures, review current electronic 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: *electronic signature, electronic seal, qualified, open-source, XAdES, PAdES, CAdES, desktop software*

Contents

List of Figures

List of Tables

Introduction

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Integer lacinia, nulla porta varius tempus, lacus metus blandit lorem, a rutrum justo wisi id sapien. Integer risus libero, feugiat eleifend, ornare ac, volutpat nec, sem. In facilisis, quam eu elementum aliquet, lorem quam euismod dui, aliquet laoreet purus ipsum ac quam.

Chapter 1

Background and theory

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Integer lacinia, nulla porta varius tempus, lacus metus blandit lorem, a rutrum justo wisi id sapien. Integer risus libero, feugiat eleifend, ornare ac, volutpat nec, sem. In facilisis, quam eu elementum aliquet, lorem quam euismod dui, aliquet laoreet purus ipsum ac quam.

1.1 Legal

-

1.2 Cryptography

-

1.3 Software engineering

-

Chapter 2

Problem setting

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Integer lacinia, nulla porta varius tempus, lacus metus blandit lorem, a rutrum justo wisi id sapien. Integer risus libero, feugiat eleifend, ornare ac, volutpat nec, sem. In facilisis, quam eu elementum aliquet, lorem quam euismod dui, aliquet laoreet purus ipsum ac quam.

Chapter 3

Analysis

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Integer lacinia, nulla porta varius tempus, lacus metus blandit lorem, a rutrum justo wisi id sapien. Integer risus libero, feugiat eleifend, ornare ac, volutpat nec, sem. In facilisis, quam eu elementum aliquet, lorem quam euismod dui, aliquet laoreet purus ipsum ac quam.

Chapter 4

Implementation

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Integer lacinia, nulla porta varius tempus, lacus metus blandit lorem, a rutrum justo wisi id sapien. Integer risus libero, feugiat eleifend, ornare ac, volutpat nec, sem. In facilisis, quam eu elementum aliquet, lorem quam euismod dui, aliquet laoreet purus ipsum ac quam.

Chapter 5

Results

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Integer lacinia, nulla porta varius tempus, lacus metus blandit lorem, a rutrum justo wisi id sapien. Integer risus libero, feugiat eleifend, ornare ac, volutpat nec, sem. In facilisis, quam eu elementum aliquet, lorem quam euismod dui, aliquet laoreet purus ipsum ac quam.

Donec dolor arcu, posuere at, vehicula vitae, accumsan ut, lacus. Nulla tristique eros eu diam. Vivamus nec tortor vel ligula elementum lacinia. Curabitur euismod eros adipiscing ipsum. Donec sed quam at felis suscipit egestas. Morbi faucibus libero sit amet libero. Nullam laoreet ipsum eu eros. Donec in diam. Ut facilisis eros vel leo. Nunc vitae mauris. Donec leo erat, luctus porttitor, laoreet eget, facilisis non, erat. Integer nec elit.

Conclusion

Ut lobortis semper risus, non condimentum dui convallis ut. Nulla eget volutpat tellus. Vestibulum lobortis tincidunt massa eu rhoncus. Suspendisse luctus eu dui non vehicula. Vivamus elementum auctor felis, placerat maximus magna lobortis ut. Donec placerat sem a mi sagittis blandit. Maecenas pellentesque laoreet mauris, dictum viverra ante sodales sed. Nullam non ligula quis ante ultricies finibus non quis ex. Ut tempor vitae ipsum sed imperdiet. Fusce aliquam nisl sit amet nunc tempor convallis. Vivamus vehicula magna sit amet purus commodo, et tincidunt purus accumsan. Nulla velit dolor, lacinia nec scelerisque a, euismod a sapien.

Bibliography

[1] Beck, G., 2007. *Zakázaná rétorika: 30 manipulatívních technik.* Preklad Pomikálová, M.. Praha: Grada Publishing. ISBN 978-80-247-1743-2.

[2] Vojčík, P., 2010. *Občianske právo hmotné II.* 3. prep. a dopl. vyd. Košice: UPJŠ v Košiciach. ISBN 978-80-7097-817-7.

[3] Šoltés, M. a Radoňák, J., 2013. *Základné princípy laparoskopickej chirurgie.* Košice: UPJŠ v Košiciach. ISBN 978-80-8152-074-7.

[4] Guzanin, Š., Sabovčík, R. a Kačmár, P., 2004. *Selected Chapters of Plastic and Reconstructive Surgery: vysokoškolské učebné texty.* Košice: Univerzita Pavla Jozefa Šafárika v Košiciach, Lekárska fakulta. ISBN 80-7097-557-1.

[5] Nagyová, I. et al. 2009. *Measuring health and quality of life in the chronically ill.* Košice: Equilibria. ISBN 978-80-892-8446-7.

[6] Speight, J. G., 2005. *Lange's Handbook of Chemistry* [online]. London: McGraw-Hill. [cit. 2009.06.10.] ISBN 978-1-60119-261-5. Dostupné na: `http://www.knovel.com/web/portal/basic_search/display?_EXT_KNOVEL_DISPLAY_bookid=1347&_EXT_KNOVEL_DISPLAY_fromSearch=true&_EXT_KNOVEL_DISPLAY_searchType=basic`

[7] Bačkor, M. a Mihaličová, S., zost., 2013. *Zborník príspevkov z konferencie 11. dni doktorandov experimentálnej biológie rastlín a 13. konferencie experimentálnej biológie rastlín* [online]. Košice: Univerzita Pavla Jozefa Šafárika v Košiciach, Prírodovedecká fakulta [cit. 2009-06-10]. ISBN 9788081520327. Dostupné na: `http://www.upjs.sk/public/media/5596/PF-Zbornik-prispevkov-konferencie-11-dni-doktorandov.pdf`

[8] *Thaiszia: Journal of Botany.* Košice: P.J.Safarik University, Botanic Garden, 1990– . ISSN 1210-0420.

[9] *Ikaros: elektronický časopis o informační bezpečnosti* [online], 2002. [Praha]: Ikaros. 1997– [cit. 2002-03-08]. Dostupné na: `http://www.ikaros.cz/`. ISSN 1212-5075.

[10] *CHIP: magazín informačních technologií*, 2013. Praha: Burda Praha, roč. 23, říjen. ISSN 1210-0684.

[11] Sabol, J., 2000. Jazyk ako ľudské posolstvo: (namiesto doslovu). In: *O jazyku a štýle kriticky aj prakticky*. Prešov: Náuka, s. 149–159. ISBN 809676022X.

[12] Tóthová, E. a kol., 2013. A rare t(9,22,16)(q34,q11,q24) translocation in chronic myeloid leukemia for which imatinib mesylate was effective: a case report. In: *XXVII. Olomoucké hematologické dny s mezinárodní účastí, 12.–14.5.2013, Olomouc: sborník abstrakt*. Olomouc: Univerzita Palackého v Olomouci, s. 75–76. ISBN 9788024434803.

[13] Beňačka, J. et al., 2009. A better cosine approximate solution to pendulum equation. In: *International Journal of Mathematical Education in Science and Technology*. Vol. 40, no. 2, p. 206–215. ISSN 0020-739X.

[14] Dubayová, T. et al., 2010. The impact of the intensity of fear on patient's delay regarding health care seeking behavior: a systematic review vyhľadaní zdravotníckej starostlivosti. In: *International Journal of Public Health*. Vol. 55, no. 5, p. 459–468. ISSN 1661-8556.

[15] Steinerová, J., 2000. Princípy formovania vzdelania v informačnej vede. In: *Pedagogická revue*. Roč. 2, č. 3, s. 8–16. ISSN 1335-1982.

[16] Hoggan, D., 2002. Challenges, Strategies, and Tools for Research Scientists. In: *Electronic Journal of Academic and Special Librarianship* [online]. Vol. 3, no. 3 [cit. 2013-01-10]. ISSN 1525-321X. Dostupné na: `http://southernlibrarianship.icaap.org/content/v03n03/Hoggan_d01.htm`

[17] Srbecká, Gabriela, 2010. Rozvoj kompetencí studentů ve vzdělávání. In: *Inflow: information journal* [online]. Roč. 3, č. 7 [cit. 2013-08-06]. ISSN 1802-9736. Dostupné na: `http://www.inflow.cz/rozvoj-kompetenci-studentu-ve-vzdelavani`

[18] Zemánek, P., 2001. The machines for "green works" in vineyards and their economical evaluation. In: *9th International Conference: proceedings. Vol. 2. Fruit*

Growing and viticulture [CD-ROM]. Lednice: Mendel University of Agriculture and Forestry, p. 262–268. ISBN 80-7157-524-0.

[19] MIKULÁŠIKOVÁ, M., 1999. *Didaktické pomôcky pre praktickú výučbu na hodinách výtvarnej výchovy pre 2. stupeň základných škôl*: diplomová práca. Nitra: UKF.

[20] URDZÍK, P., 2007. *Predikcia intrauterinnej rastovej retardácie a preeklampsie pomocou biochemických a ultrazvukových markerov*: dizertačná práca. Košice: UPJŠ v Košiciach.

[21] BAUMGARTNER, J. a kol., 1998. *Ochrana a udržiavanie genofondu zvierat, šľachtenie zvierat*: výskumná správa. Nitra: VÚŽV.

[22] STN ISO 690: 2012. *Informácie a dokumentácia. Návod na tvorbu bibliografických odkazov na informačné pramene a ich citovanie.*

[23] VKÚ, 2003. *Košice: mapa okolia.* [1:15000]. 3. vyd. Harmanec: VKÚ. ISBN 80-8042-223-0.

[24] *Zákon č.131/2002 Zb. o vysokých školách a o zmene a doplnení niektorých zákonov.*

[25] *Zákon č. 313/2001 o verejnej službe.*