Open electronic signature software

Author: Jakub Ďuraš

Tutor: RNDr. Viliam Kačala

1.

PROBLEM AND MOTIVATION

SIGNATURE USABILITY

PROBLEM

Handwritten signatures still the norm.

Electronic communication often impossible.

MOTIVATION

Recent changes in the legal status around the world (e.g. eIDAS).

No friendly open-source app specifically for “Advanced electronic signatures”.

Stephen Mason: Electronic Signatures in Law - Fourth Edition, Humanities Digital Library, 2016, ISBN 978-1-911507-01-7, humanities-digital-library.org

SIGNATURE SECURITY

PROBLEM

Handwritten signatures have to be verified, otherwise they don't uniquely link or identify.

Content or date and time can be changed after signing.

MOTIVATION

Cryptography can practically guarantee all of that.

We can trust the third party - Slovak eID - MV SR.

Christof Paar and Jan Pelzl: Understanding Cryptography - A Textbook for Students and Practitioners, Springer, 2009, ISBN 978-3-642-04100-6

2.

OBJECTIVES

General objectives

1. Explore the principles and global legal status of electronic signatures (compilation, result is website, infographics).
2. Review current electronic signature software (comparing UX and output).
3. Propose and develop open-source, cross-platform, and user-friendly software compliant with eIDAS Regulation (Regulation No 910⁄2014) for electronic document signing (software engineering).

3.

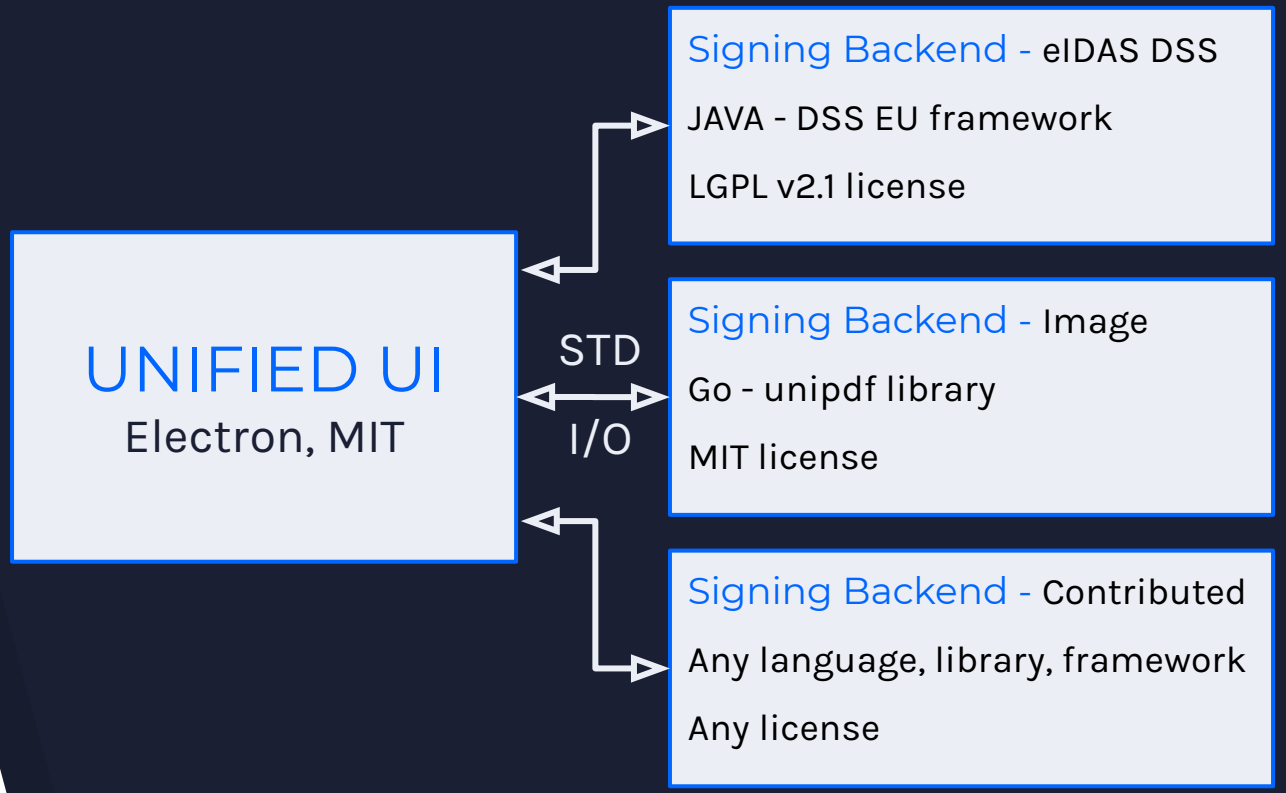
PROGRESS

DEMO

Current state

- Repositories with the software set up (incl. CI).
- Software requirements - Requirements.
- Architecture with Backend specification.
- Working Proof of Concept - Octosign and naive DSS backend (only PAdES on Windows).
- Exploration and discussion around the legal implications when using the certificates on the EU ID cards and bundled PKCS#11 DLLs.

APP ARCHITECTURE



Plan for the current term

- Complete most important UI parts.
- DSS backend should work on all 3 platforms with any PKCS#11 shared library and any file format.
- Document testing, development process, release process.
- Create simple website with downloads and info about the SK eID in 2 languages.

Thank you for your attention

https://github.com/durasj/octosign
https://thesis.science.upjs.sk/~jduras