Open electronic signature software

Author: Jakub Ďuraš

Tutor: RNDr. Viliam Kačala

SIGNATURE USABILITY & SECURITY

PROBLEM

Handwritten signatures still the norm despite issues with:

- electronic communication
- forgery
- ability to change content, date & time

MOTIVATION

- Changes in the legal status around the world (e.g. eIDAS).
- Possibilities of cryptography.

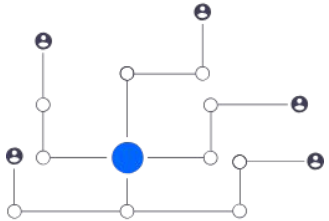
GENERAL OBJECTIVES

1. Explore the principles and global legal status of electronic signatures.
2. Propose and develop open-source, cross-platform, and user-friendly platform for electronic document signing.
3. Provide information and way to create signatures compliant with eIDAS Regulation (Regulation No 910⁄2014).

DIFFERENT TYPES

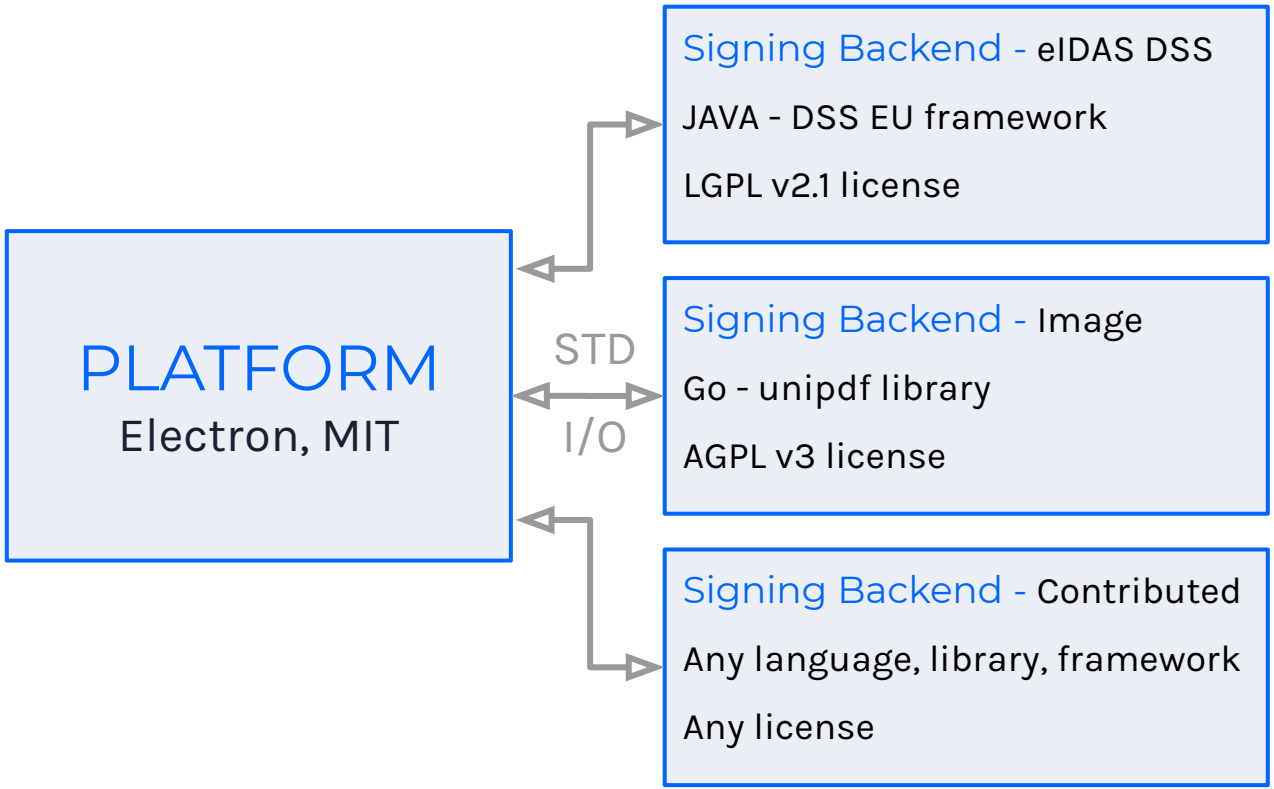
IMAGE

STANDARDIZED
PUB-KEY & CERTIFICATE



EXPERIMENTAL

SOFTWARE


PLATFORM
Electron, MIT
STD
I/O
Signing Backend - eIDAS DSS
JAVA - DSS EU framework
LGPL v2.1 license
Signing Backend - Image
Go - unipdf library
AGPL v3 license
Signing Backend - Contributed
Any language, library, framework
Any license

ENGINEERING FOR OPEN SOURCE

Backend specification

Jakub Ďuraš edited this page on Jan 8 · 11 revisions

Octosign can use different signing backends that are dynamically lo
in any language and with any directory structure and architecture. T

- Config file `backend.yml` in the root directory with information
- Use of plaintext communication protocol using the standard st
  standard output (STDOUT), and standard error (STDERR).
- Mandatory end-to-end tests.

Config file

Each backend provides a necessary amount of information for the a
description, or the executable that should be called. Here is an exam

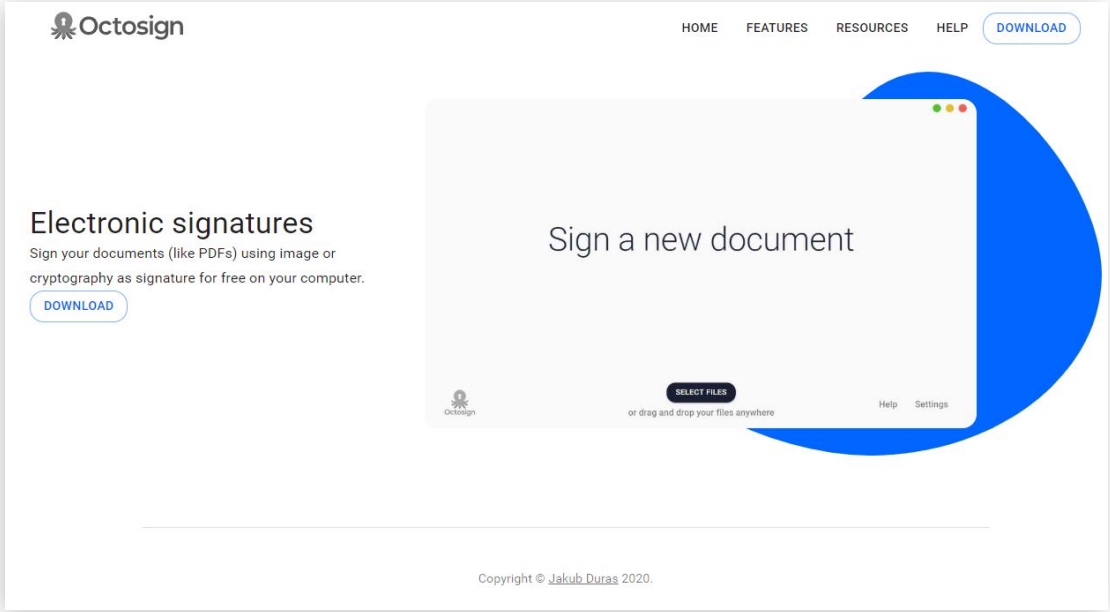
```yaml
name: Electronic signature
description: Advanced electronic signature usable on PDF and
repository: https://github.com/durasj/octosign-dss
version: 1.0-SNAPSHOT
author: Jakub Ďuraš <jakub@duras.me>
license: MIT
exec: ./jdk/bin/java.exe -jar ./sign.jar
build: bash -e ./dist.sh
```

```cpp
#include <iostream>
#include <cstring>
#include <regex>
#include <errno.h>

int main(int argc, char** argv) {
    if (argc < 2) {
        std::cerr << "One of the operations required
        return 1;
    }

    if (strcmp(argv[1], "meta") == 0) {
        std::cout << "OK";
    } else if (strcmp(argv[1], "sign") == 0) {
        std::string new_name = std::regex_replace(arg
        if (rename(argv[2], new_name.c_str()) == -1)
            std::cerr << "Error: " << strerror(errno)
            return 1;
        }
    } else if (strcmp(argv[1], "verify") == 0) {
        bool contains = std::regex_match(argv[2], st
        printf(contains ? "SIGNED" : "UNSIGNED");
    }
    return 0;
}
```

INFORMATION AND COMMUNITY




potvrdenie-objednavky.pdf
SELECT FILES

Thank you for your attention

www.octosign.com

thesis.science.upjs.sk/~jduras