



netidee

PROJEKTE

open-pdf-sign

Endbericht | Call 16 | Projekt ID 5822

Lizenz CC-BY-SA

Inhalt

1	Einleitung.....	3
2	Projektbeschreibung.....	3
3	Verlauf der Arbeitspakete.....	5
	Arbeitspaket 1 - <i>Projekt start</i>	5
	Arbeitspaket 2 - <i>Research</i>	5
	Arbeitspaket 3 - <i>Implementierung</i>	6
	Arbeitspaket 4 - <i>Dokumentation und Marketing</i>	7
	Arbeitspaket 5 - <i>Projektabschluss</i>	8
4	Liste Projektergebnisse.....	9
5	Verwertung der Projektergebnisse in der Praxis.....	12
6	Öffentlichkeitsarbeit/ Vernetzung.....	12
7	Eigene Projektwebsite.....	12
8	Geplante Aktivitäten nach netidee-Projektende.....	12
9	Anregungen für Weiterentwicklungen durch Dritte.....	13

1 Einleitung

Elektronische Signaturen von PDFs sind eine großartige Möglichkeit, um die Echtheit und Unverändertheit von Dokumenten zu gewährleisten. Leider gibt es nur wenige benutzerfreundliche Tools unter einer vergleichsweise freien Lizenz, die solche Signaturen serverseitig erstellen können. PDFs zu signieren sollte heutzutage sehr einfach sein, aber leider ist es selbst für erfahrene Informatiker schwierig, PDFs mit Open-Source-Software zu erstellen und zu signieren.

Das Signieren von PDFs erfordert immer noch viel manuelle Arbeit und kostet viel Zeit. Deshalb haben wir, das Projektteam bestehend aus Thomas Schreiber und Philipp Omenitsch, es uns zum Ziel gesetzt, eine Open-Source-Lösung zu entwickeln. Dank der Unterstützung von Netidee konnten wir diese Idee in die Realität umsetzen: Open-pdf-sign ist eine Open-Source-Bibliothek und Lösung zum sicheren Signieren von PDFs.

2 Projektbeschreibung

Das Ziel des Projektes

Thomas Schreiber beschäftigt sich mit PDF-Erstellung für FlexLex und arbeitet bei der RTR am RTR-Netztest. Philipp Omenitsch ist seit vielen Jahren Entwickler und CTO bei Stresscoach, Netzbeweis und Sequel. Gemeinsam haben wir Open-pdf-sign entwickelt. Das Ziel des Projektes ist es ein Open Source Softwarepaket mit einer geeigneten Lizenz zu erstellen, das es Entwicklern mit nur einem CLI Aufruf erlaubt PDF automatisch digital zu signieren.

Die von der Apache-Foundation entwickelte "PDFBox"-Library unterstützt auch digitale Signaturen. Unsere Software setzt auf dieser Softwarelösung auf, abstrahiert die Komplexität und ermöglicht es innerhalb von wenigen Minuten das erste PDF zu signieren.

Zielgruppe 1: Organisationen

Es gibt sehr viele Unternehmen in Österreich die PDFs erstellen. Sei es zur Bestätigung von Dienstleistungen oder beim Erstellen von digitalen Rechnungen im PDF-Format. Insofern haben indirekt fast alle Organisationen in Europa Bedarf, eine digitale Signatur zu erstellen.

Zielgruppe 2: Open Source Community

Entwickler, die mit modernen Webtechnologien Anwendungen entwickeln, die selbst entweder Open Source sind (auch unter permissiven Lizenzen wie MIT / APL) oder nicht veröffentlicht werden sollen.

Überblick über das Projektergebnis

Durch unsere Entscheidung, am Webserver anzusetzen und dessen Erreichbarkeit durch SSL hatten wir bereits alle Teile, die wir für eine Signatur benötigten: Die zu signierenden PDFs, Informationen zur Domain, auf der diese zum Download bereitgestellt werden, und die Schlüsselpaare, um eine Signatur durchführen zu können.

Aufgrund ihrer Marktanteile haben wir uns für den Webserver NGINX mit 34 % Marktanteil entschieden. (Quelle für die Marktanteile:

<https://news.netcraft.com/archives/2022/08/26/august-2022-web-server-survey.html>)

Damit können wir mit open-pdf-sign somit über ein Drittel des Internetverkehrs abdecken. Das ermöglicht es uns, einen großen Teil aller PDFs im Internet zu signieren. Für weitere Server und weniger verbreitete Systeme steht dann ohnehin unser dokumentierter Quellcode zur Verfügung, der es interessierten Entwicklern und der Community ermöglicht, open-pdf-sign auch auf solchen Servern zu unterstützen.

Unser Vorbild für die Vorgangsweise hier war <https://letsencrypt.org/>, die mit ihrem einfachen Installer den komplizierten Prozess, ein Zertifikat zu bekommen, um eine Website mit SSL abzusichern, revolutioniert haben. Sowohl Installer als auch die Ausstellung von Zertifikaten sind bei LetsEncrypt nicht nur sehr einfach, sondern insbesondere auch kostenlos.

Das ist auch der Grund, warum sich unser Subprojekt, der <https://github.com/open-pdf-sign/open-pdf-sign-configurator> sehr stark an das LetsEncrypt-Pendant "Certbot" anlehnen sollte. Zum Glück ist Certbot auch Open Source und mit MIT-Lizenz versehen. Dies hat es uns erlaubt, auf die Vorarbeit dieses Projekts aufzubauen, anstatt beispielsweise eigene Parser programmieren zu müssen.

Durch das Format von NGINX, die sehr wenigen Tools und die schlechte Dokumentation wurde die Implementierung leider um einiges verzögert. Schlussendlich haben wir es aber dennoch geschafft und haben nun das anfangs gesetzte Ziel erreicht: Dem zur Verfügung stellen einer Lösung, die das Signieren von PDFs so einfach gestaltet, dass einem schlichtweg die Ausreden fehlen.

3 Verlauf der Arbeitspakete

Arbeitspaket 1 - Projekt start

- o) Vertragsprüfung, unterschreiben und an netidee senden
- o) Projektplanung auf Basis excel-Vorlage und an berichte@netidee.at senden
- o) Projektwebsite Inhalt überprüft /erster Blog erstellt; Projektteam ergänzt (optional)
- o) Förderabrufformular für Förderrate 1 an berichte@netidee.at

Das Paket wurde abgeschlossen

Arbeitspaket 2 - Research

Wir haben uns mit den verschiedenen Standards für PDF-Signatur (PAdES-B/T/LT/LTA) und verschiedenen Bibliotheken beschäftigt. Viel Zeit wurde dann dafür verwendet, eine passende Bibliothek im passenden Standard auszuwählen.

Die Probleme dabei haben wir im Blog-Artikel <https://www.netidee.at/open-pdf-sign/standards-standards-standards-und-ein-prototyp> beschrieben.

Ähnlich komplex wie die Signaturstandards sind auch die Standards für Schlüsselaufbewahrung. Hier haben wir Zeit dafür aufgewendet, zu recherchieren und zu testen, welche Formate in der Praxis verwendet werden (PKCS7/PKCS12/etc)

Im Bereich der Lösung für die Konfiguration von Webservern, ist es uns gelungen einen Weg zu finden, dies umzusetzen und auch mit der Implementierung zu beginnen. Wir haben uns hier sehr stark an “certbot” von LetsEncrypt orientiert.

Besondere Erfolge/ Probleme

Komplexität der verschiedenen Signaturarten und Formate für Keys.

Gab es große Abweichungen zum Plan? Warum?

Der Research hat mehr Zeit in Anspruch genommen als gedacht.

Arbeitspaket 3 - Implementierung

Kurzbeschreibung der Haupttätigkeiten

- Implementierung des Command line Tools
- Implementierung des Konfigurators für Webserver (Nginx support)
- NPM Modul

Erkenntnisse zur Vorgangsweise

Wie sich im AP 2 bestätigt hat, haben wir beschlossen die Implementierung mit Hilfe von PDFbox umzusetzen. Zusätzlich sind wir auch noch auf eine Open Source Bibliothek der EU (“DSS”) gestoßen, die uns die Implementierung verschiedener Zertifikate erleichtert. Für die Implementierung der verschiedenen Schlüsselformate verwenden wir “bouncy castle”.

Kurzbeschreibung der erreichten Ergebnisse

Prinzipiell haben wir beschlossen unsere Lösung in zwei Teile zu splitten. Zum einen haben wir das CLI tool, das für sich alleine stehen können soll, das als Input PDF und Schlüssel nimmt und eine signiertes PDF zurückgibt („open-pdf-sign“).

Der Zweite Teil besteht aus einem Konfigurationsassistenten („open-pdf-sign-configurator“), deres für Nutzer so einfach wie möglich macht, alle PDFs auf einem Webserver zu signieren.

Das NPM Modul enkapsuliert das Command Line Tool und wurde auf NPM veröffentlicht

Besondere Erfolge/ Probleme

Die Vielzahl an verschiedenen Signaturformaten war nicht nur herausfordernd zu verstehen, sondern war es auch nicht einfach, diese zu implementieren.

Wir haben Feedback vom "certbot" Team einholen können.

Wir haben sehr viel dabei gelernt, einerseits weil unser Projekt mehrere Programmiersprachen verwendet, andererseits aber auch weil wir versucht haben unsere Software wirklich für verschiedene Systeme verwendbar zu machen.

Gab es große Abweichungen zum Plan? Warum?

Wir wären im Juni 2022 gerne schon weiter fortgeschritten gewesen mit der Implementierung des CLI Tools um PDFs auf Webservern zu implementieren. Hier gab es Verzögerungen aufgrund von beruflichen Tätigkeiten. Es ist nicht einfach die verschiedenen beruflichen Tätigkeiten unter einen Hut zu bringen, wir haben uns hier ein wenig verschätzt.

Besonders der Konfigurator hat sich als nicht so einfaches Problem herausgestellt. Zwar gibt es mit "certbot" ein Vorbild, an das wir uns stark angelehnt haben, jedoch ist hier die Implementierung sehr kompliziert, weil Nginx zum Beispiel ein eigenes Format für Konfigurationsdateien verwendet. Außerdem ist das Testen nicht trivial, da wir, um wirklich gut Testen zu können, Server benötigen, die Nginx installiert haben und aktuell PDFs schon ausliefern. Dies sind meist Produktivserver, und auf denen unsere Software zu testen ist nicht sehr gut. Darum haben wir zuerst virtuelle Testserver kreieren müssen mit Docker, was allerdings wieder zu eigenen Problemen geführt hat, da docker kein systemd (der Unix-Dienst, der unseren Service ausführt) unterstützt.

Arbeitspaket 4 – *Dokumentation und Marketing*

Kurzbeschreibung der Haupttätigkeiten

- Dokumentation
- Website
- Vermarktung

Erkenntnisse zur Vorgangsweise

Für das Erstellen der Logos und Designs haben wir mit externen Designern zusammengearbeitet.

Es ist nicht so einfach die richtige Dokumentation für die richtige Zielgruppe zu gestalten. Wir sprechen zwar eine ähnliche Zielgruppe als Anwender an, weil unser Projekt auch für Entwickler bzw. Serveradministratoren zur Verwendung gedacht ist.

Wir haben uns ein wenig mehr von unserer Veröffentlichung auf Producthunt erwartet. Vermutlich ist die Audienz dort aber nicht so technisch wie wir gedacht haben, da unser Produkt doch sehr auf eine Nische abzielt. Zusätzlich haben wir unser Produkt auf Social Media-Plattformen wie LinkedIn und Twitter beworben, wo wir tausende Personen erreichen konnten.

Kurzbeschreibung der erreichten Ergebnisse

Die Dokumentation erfolgt wie üblich bei ähnlichen Projekten auf der Projektwebsite und auch auf Github.

Die Website ist uns sehr gut gelungen und wir sind sehr stolz darauf, sie ist zwar kurz, beinhaltet aber alle wichtigen Punkte unserer Meinung nach und ist sehr übersichtlich und auch anschaulich.

Wir haben unsere Software auf der Plattform "Producthunt" vorgestellt. Wir wurden von Thomas Schranz auf der Website geteilt und haben dort 83 Stimmen erhalten. Bis dato wurde das open-pdf-sign repository 32 mal gecloned und mehr als 60 Entwickler haben uns auf Github besucht. Wir haben aktuell 17 Sterne auf Github erhalten, unser gesetztes Ziel von 20 wurde somit knapp nicht erreicht, wir sind aber ziemlich sicher, dass wir im Laufe der Zeit noch einige Sterne dazuerhalten werden.

Weiters wurden unsere Beiträge auf LinkedIn und Twitter zum Launch mehr als 5000 mal gesehen.

Wir konnten auch mit 2 Entwicklern direkt sprechen, die überlegen "open-pdf-sign" selbst in ihrem Projekt zu verwenden. Das hat uns natürlich am Meisten gefreut.

Wir glauben, dass über Zeit noch einige Leute mehr unser Projekt finden werden und sind gespannt wie viele Leute open-pdf-sign verwenden werden.

Gab es große Abweichungen zum Plan? Warum?

Bezüglich der Vermarktung haben wir ein wenig zu spät damit begonnen wirklich aktiv zu werben für unsere Pakete. Das hat zum einen damit zu tun, dass es erst Sinn macht, wenn zumindest ein Minimalprodukt steht. Bei uns sind jedoch mehrere Projekte miteinander verkettet. Dennoch hätten wir, sobald die CLI fertig war, diese sofort bewerben sollen und später noch den Konfigurator.

Arbeitspaket 5 – Projektabschluss

Kurzbeschreibung der Haupttätigkeiten

netidee Call 16 Endbericht Projekt-ID 5822

- o) Projektverlauf im Projektendbericht, Zusammenfassung und Endabrechnung dokumentieren
 - o) Endbericht, Zusammenfassung, Endabrechnung samt gescannter Originalbelege an berichte@netidee.at übermitteln
 - o) Förderratenabrufformular für die dritte Förderrate ausfüllen und an berichte@netidee.at übermitteln
 - o) Endbericht, Zusammenfassung, Anwender_innen-Dokumentation und Entwickler_innen-Dokumentation auf die Projektwebsite hochladen
 - o) Abschließenden Blogbeitrag verfassen
- Das Paket wurde abgeschlossen

4 Liste Projektergebnisse

1	Projektzwischenbericht	CC-BY-SA	https://www.netidee.at/open-pdf-sign
2	Projektendbericht	CC-BY-SA	https://www.netidee.at/open-pdf-sign
3	Entwickler_innen-DOKUMENTATION des Projektergebnisses für andere Entwickler_innen ("Dritte"), die das Projektergebnis nach Projektende nutzen/weiterentwickeln wollen Für Entwickler_innen (Systemkonzept, ggf.	CC-BY-SA	https://www.netidee.at/open-pdf-sign

	Grobspezifikationen): a. WAS IST ES b. FÜR WEN IST ES /WEM HILFT ES WODURCH c. WIE FUNKTIONIERT ES (für Entwickler_innen: Übersicht und detailliertes Systemkonzept, SW- Struktur)		
4	Anwender_innen- DOKUMENTATION des Projektergebnisses für Anwender_innen, die das Projektergebnis nach Projektende nutzen wollen Für Anwender_innen ("Bedienungsanleitung") : a. WAS IST ES b. FÜR WEN IST ES /WEM HILFT ES WODURCH c. WIE FUNKTIONIERT ES	CC-BY-SA	https://www.netidee.at/open-pdf-sign
5	Veröffentlichungsfähiger Einseiter * Kurzfassung WAS FÜR WEN WIE * Liste Projektergebnisse - also diese Liste, ggf. kompromiert * mit Angabe Open Source Lizenz/Webadresse * wo finden Dritte die Projektergebnisse (inkl. Dokumentation Anwender_innen bzw. Entwickler_innen) * mögliche Weiterentwicklungen/	CC-BY-SA	https://www.netidee.at/open-pdf-sign

	weitere Einsatz-/ Nutzungsmöglichkeiten		
6	<p>Dokumentation Externkommunikation zur Erreichung Sichtbarkeit /Nachhaltigkeit (separates Dokument oder als Teil des Endberichtes)</p> <p>* Welche Maßnahmen wurden in welchem Umfang gesetzt * Jeweils Bewertung Aufwand / Nutzen * Lessons Learned / Empfehlungen für andere Projekte</p> <p>=> ist Teil des Endberichts</p>	CC-BY-SA	https://www.netidee.at/open-pdf-sign
7	<p>SW-Projektergebnis- Teil_1 Software</p> <p>CLI laufend auf Linux, mac und windows npm module Nginx integration</p>	APL 2.0	https://github.com/open-pdf-sign/open-pdf-sign https://github.com/open-pdf-sign/open-pdf-sign-configurator https://github.com/open-pdf-sign/open-pdf-sign-node https://github.com/open-pdf-sign/open-pdf-sign-website https://www.netidee.at/open-pdf-sign
8	<p>SW-Projektergebnis- Teil_2 Website allgemeine Beschreibung und Dokumentation für</p>	Text licensed CC-BY-SA 4.0, code licensed APL- 2.0.	openpdfsign.org https://www.netidee.at/open-pdf-sign

	die Software		
9	SW-Projektergebnis-Teil_3 Demo Page & Tool Anleitung für Integration mit Server-Software, ähnlich https://certbot.eff.org/lets-encrypt/	APL 2.0	openpdfsign.org https://www.netidee.at/open-pdf-sign

5 Verwertung der Projektergebnisse in der Praxis

Open-pdf-sign wird aktuell bei der “Netzbeweis GmbH” dazu verwendet um alle erstellten Beweise zu signieren. Das sind mehrere hundert Beweise im Monat.

6 Öffentlichkeitsarbeit/ Vernetzung

Wir waren sehr fleißig beim Blogartikel erstellen. Die Website wurde erstellt.

Wir haben auf einigen Treffen Leute von unserer Lösung erzählt und gutes Feedback erhalten.

Wir haben Open-pdf-sign auf einschlägigen Webseiten veröffentlicht:

- Producthunt
- news.ycombinator.com
- LinkedIn
- Twitter

7 Eigene Projektwebsite

<https://openpdfsign.org/>

Die Website selbst ist auch als Open Source auf GitHub gehostet (Code unter der Apache 2.0-Lizenz, der Text unter CC-BY-SA)

8 Geplante Aktivitäten nach netidee-Projektende

Wir wollen den Launch abwarten und hoffen auf Nutzung durch die Community. Wir werden jedenfalls die Software weiterhin warten und auf Bedürfnisse von Nutzern agieren, um neue Features einzuarbeiten.

Es wäre möglich, den Konfigurator noch für mehrere Plattformen zu erweitern. Jedoch wollen wir zunächst ein paar Monate abwarten, wie unser Projekt ankommt. Idealerweise werden Leute zu unserem Projekt beitragen oder uns Feedback geben, damit wir wissen, welche Plattformen am meisten gefragt sind.

9 Anregungen für Weiterentwicklungen durch Dritte

Unsere Bibliothek ist mit dem Zweck geschaffen worden, anderen Entwicklern das Leben leichter zu machen und PDFs zu signieren. So wäre es zum Beispiel relativ einfach möglich, mit unserem Projekt eine API zu kreieren und als Service anzubieten, über das man PDFs direkt signieren kann.

Auch Firmen die sich mit Dokumentenverwaltung beschäftigen bzw. mit Digitalen Signaturen können auf unser Projekt aufbauen, ein Beispiel wäre hier wie schon im Antrag erwähnt Netzbeweis, das PDFs signiert um sie als Beweismittel vor Gericht bringen zu können, oder auch Stresscoach, das PDFs verwendet um seinen Nutzern eine Rückerstattung bei der Krankenkassa ermöglicht.