Richtlinie zum „Software-Sprint“

memoorje – Sicherer und selbstverwalteter digitaler Nachlass für alle

Schlussbericht

Zuwendungsempfänger:

Steffen Dabbert, Konrad Mohrfeldt, Robert Waltemath GbR

Das diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen 01IS21S55 gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt beim Autor.

Kurze Darstellung der Aufgabenstellung und Motivation

Das Projekt memoorje möchte allen Menschen, die mit einem Computer oder Smartphone umgehen können, ermöglichen, ihren digitalen Nachlass selbstbestimmt und unkompliziert zu regeln.

Nutzer_innen von memoorje können Kapseln mit Daten anlegen, die im Todesfall an ausgewählte Personen übersendet werden. Die Daten liegen verschlüsselt auf dem Server und werden so chiffriert, dass die Betreiber_innen keine Kenntnis des Schlüssels erhalten. Damit die Inhalte der Kapseln wiederhergestellt werden können, wird der Schlüssel mit "Shamir's Secret Sharing"-Algorithmus aufgeteilt. Jeder dieser Teile ist für sich unbrauchbar, aber werden eine Mindestmenge an Teilen zusammengefügt, lässt sich daraus der Schlüssel entlocken. Die Einzelteile werden an Vertrauenspersonen weitergegeben. Tritt der Todesfall ein, können diese den Tod bestätigen und mit ihren Teil-Schlüsseln den Zugriff auf die Kapseln gewähren.

Der Tod ist eine Angelegenheit, der ausnahmsweise wirklich alle betrifft. Mit memoorje wollen wir den Verwaltung und Weitergabe von digitalem Nachlass demokratischer gestalten. Gänge zu Notar_innen und Anwält_innen sind kostspielig und mit administrativen Aufwänden und rechtlichen Hürden verbunden. Das kann ausschließend auf bestimmte Gruppen unserer Gesellschaft wirken. Jede_r von uns hat das Recht auf einen selbstverwalteten Nachlass, was wir mit memoorje umsetzen wollen.

Das Projekt sollte anhand von drei Meilensteinen umgesetzt werden:

1.*P roof of Concept*

- Grundlegende Implementierung einer API, die Kapseln entgegen nimmt und verwaltet sowie Nutzer_innen zuordnet.
- Umsetzung eines minimalistischen Clients im Browser, der die Daten der Nutzer_innen entgegen nimmt, als Kapseln verschlüsselt und an die API überträgt.

- Die Entschlüsselung von Kapseln erfolgt in diesem Arbeitsschritt noch manuell auf dem Server.

2. User Interface und Kernfunktionalitäten

- Entwicklung von Bedienoberflächen für die Verwaltung der Kapseln, die Festlegung von Vertrauenspersonenkreisen, Anmeldung, Registrierung und der entsprechenden Unterstützung im Backend.
- Implementierung von serverseitigen Prozessen wie das Entschlüsseln von freigegebenen Kapseln.
- Versand von Benachrichtigungen an Vertrauenspersonen bei Einleitung des Nachlassprozess und allgemeine Erinnerungen zur Pflege der Kapseln.

3. Optionale praktische Erweiterungen

Ggf. Umsetzung von erweiterten Funktionen wie Totmenschschaltern, bei denen die Person, die Eigentümer_in einer Kapsel ist, fortwährend bestätigen muss, dass sie noch handlungsfähig ist.

Beitrag des Projektes zu den Zielen der Förderinitative „Software-Sprint“

Im Grunde sind alle Menschen vom Tod betroffen. Insofern haben wir eine ziemlich breite Zielgruppe. Eingrenzungen finden dann statt, wenn es konkret um einen digitalen Nachlass geht. Dieser muss natürlich vorhanden sein, was die Zielgruppe vermutlich etwas verjüngt.

Darüber hinaus zeigen wir beispielhaft auf, wie sich der verwendete Algorithmus zur Verschlüsselung der Daten in eigene Projekte integrieren lässt. Dementsprechend erweitert sich die Zielgruppe um Menschen aus der Freien-Software-Bewegung und um Forschende im Bereich von Sicherheitstechniken.

Das Projekt lässt sich damit in die Förderbereiche Civic Tech und Datensicherheit einordnen.

Ausführliche Darstellung der Ergebnisse

Die Anwendung ist in einem lauffähigen Zustand und im Rahmen des Projektes konnten alle mit den ersten beiden Meilensteinen verbundenen Ziele erreicht werden. Die Anwendung bietet unter anderem folgende Funktionen:

- Kontenverwaltung: Nutzer_innen können sich in der Anwendung mit ihrer E-Mailadresse und einem Passwort registrieren. Die Registrierung löst eine Bestätigungsmail aus, die einen Aktivierungslink enthält. Vergessene Passworte können über einen Passwort-Reset zurück gesetzt werden.
- Verwaltung von Kapseln: Kapseln sind unser Konzept eines Ortes, in dem ein digitales Erbe gespeichert werden kann. In der Anwendung können beliebig viele Kapsel angelegt, bearbeitet und gelöscht werden.
- Verwaltung von Daten: Daten können in den Kapseln gespeichert werden. Dazu können verschiedene Dateiformate (Bilder, Textdokumente, Videos, Passworte,

Briefe,…) über den Webbrowser in die Anwendung hochgeladen und einer Kapsel zugeordnet werden. Gespeicherte Daten können aus einer Kapsel ebenfalls wieder entfernt werden.

- Verschlüsselung der Daten: Die Inhalte der Kapsel liegen verschlüsselt auf dem memoorje-Server. Die Verschlüsselung erfolgt dabei bereits im Browser, so dass ein_e Serverbetreiber_in niemals Zugriff auf die Daten im Klartext hat.
- Verwaltung der Erben: Es kann festgelegt werden, wer den Inhalt einer Kapsel später (also nach dem Ableben) erhalten soll. Dazu können in der Anwendung E-Mail-Adressen hinterlegt werden.
- Verwaltung von Vertrauenspersonen: Angabe von Personen, die eine Kapsel freigeben können. Dabei können verschiedene E-Mailadresse über den Browser eine Kapsel zugeordnet werden.
- Verwaltung von Teilschlüsseln: Im Backend erzeugt die Anwendung so viele Teilschlüssel wie Vertrauenspersonen angegeben wurden. Im Frontend kann angegeben werden, wie viele Teilschlüssel zum Öffnen deiner Kapsel benötigt werden.
- Mailbenachrichtigungen aller Art: Das Backend versendet Mailbenachrichtigungen, sobald verschiedene Aktionen ausgelöst werden. Dazu gehören u.a.: Registrierung eines neuen Kontos, Erinnerungen, Benachrichtigungen von Kapselempfänger_innen
- Freigabe von Kapselinhalten: Über den Webbrowser können Kapseln durch Eingabe der definierten Anzahl der Teilschlüssel freigegeben und angezeigt werden.

Die Begleitung durch die OKF empfanden wir als sehr hilfreich und unterstützend. Durch den regelmäßigen Austausch in großen und kleinen Gruppen entstand auch in dieser „Remote“-Runde (durch die Corona-Situation gab es kein Treffen im realen Leben) eine stärkerer Bezug zum PTF selbst.

Zielgruppe, Nutzen und mögliche Weiterentwicklungen

Bei dem Projekt ging es neben der Entwicklung einer konkreten Anwendung auch um die Bewusstmachung von Fragen rund um den digitalen Nachlass. Bisher scheint ein Bewusstsein rund um die Frage „Wie übergebe ich meinen digitalen Nachlass?“ wenig ausgeprägt zu sein. Neben der nutzbaren Demoversion lenkt das Projekt die Aufmerksamkeit also auch auf das Thema digitaler Nachlass allgemein.

Ideen zur Weiterentwicklung gibt es ausreichend. Nach Abschluss des Projektes werden wir die Anwendung ausreichend testen, um eine stabilen Betrieb sicher zu stellen. Das Projekt soll sich aus freiwilligen Spenden finanzieren. Insofern steht weiterhin an, die Bekanntheit über verschiedenen Kanäle zu steigern und ein Spendenmodell zu formulieren.

Neben dem Nutzen für die Öffentlichkeit hat das Projekt unsere Fähigkeiten zur vernetzten Arbeit im Team gestärkt – auch dadurch, dass die Mitglieder des Teams aus verschiedenen Städten kamen. Mit dem gewählten Algorithmus zur Verschlüsselung waren wir bisher nicht vertraut. Insofern konnten wir uns auch intensiv mit dem Thema Datensicherheit auf technischer und gesellschaftlicher Ebene auseinander setzen.

Kurze Darstellung der Arbeiten, die zu keiner Lösung geführt haben

Im Rahmen des dritten Meilensteins wollten wir erweiterte Funktionen evaluieren und ggf. umsetzen. Konkret war geplant, eine Art Totmenschschalter einzubauen, der bei Nicht-Betätigung bestimmte Aktionen auslöst. Unsere Analyse ergab, dass dies aus Sicht der Usability nicht sinnvoll gewesen wäre. Insofern haben wir auf dieses Feature verzichtet.

Kurze Angabe von Präsentationsmöglichkeiten für mögliche Nutzer

Der Stand der Anwendung wurde mit einer Demoversion veröffentlicht. Unter https://demo.memoorje.org/ können somit alle Funktionen getestet werden. Der Quellcode ist über https://git.hack-hro.de/memoorje verfügbar.

Kurze Erläuterung zur Einhaltung der Arbeits- und Kostenplanung

Wir haben das Projekt in drei Arbeitsphasen eingeteilt, die sich ungefähr mit den Meilensteinen decken. Diesen Phasen haben wir im Vorfeld unterschiedliche Zeitkontingente zugeordnet, um das Projekt zu strukturieren. Gleich zu Beginn des Projekts haben wir einen großen Stundenanteil in die Grundfunktionalität der Anwendung investiert. Darauf aufbauend fand in der zweiten Phase ein Sicherheitscoaching statt, bei dem wir unsere Ideen für die Implementierung der Verschlüsselungsfunktionen diskutieren konnten. Das Coaching war Grundlage für einige Design-Entscheidungen, wie beispielsweise die Wahl einer passenden Verschlüsselungsbibliothek. Geplant war ebenfalls ein zweites Sicherheitscoaching und die Durchführung eines Audits zur Umsetzung der Verschlüsselungsfunktionen. Trotz verschiedener Anläufe kam ein erneuter Termin nicht zustande.

Kurze Darstellung von etwaigen Ergebnissen bei anderen Stellen

Funktionierende Datensicherheit ist ein wesentliches Element des Projektes. Insofern war die Begleitung durch ein Sicherheitscoaching wichtig und hilfreich. Die Durchführung des ersten Coachings hat sich zeitlich verzögert, so dass wir die o.g. Design-Entscheidungen verschieben und unseren Arbeitsplan anpassen mussten. Grundsätzlich stellte dies jedoch keine Schwierigkeit dar, da wir uns anderen Aufgaben widmen konnten. Da das zweite geplante Coaching nicht zustande kam, mussten wir uns selbst tiefer in Implementierung der Verschlüsselungsfunktionen einarbeiten.