



MARTIN-LUTHER-UNIVERSITÄT
HALLE-WITTENBERG

MAX-PLANCK-INSTITUT
FÜR ETHNOLOGISCHE FORSCHUNG



Planung und Entwicklung einer Datenbankanwendung für das Forschungsdatenmanagement

Max Brauer (ma.brauer@live.de)

Bachelor für Informatik

Juli 2022

Erstgutachter: Dr. Stefan Brass

Zweitgutachter: Sebastian Ehser

Inhaltsverzeichnis

1	Einleitung	7
2	Anforderungen	9
2.1	Inhaltliche Anforderungen	9
2.2	Technische Anforderungen	10
2.2.1	System	10
2.2.2	Back-ups	11
2.3	Wahl der Komponenten	11
2.3.1	Front-End (UI)	11
2.3.2	Back-End (Server)	14
2.3.3	Datenbank	16
2.3.4	Interne Schnittstellen	18
3	Sicherheit	21
3.1	Grundsätze der IT-Sicherheit	21
3.1.1	Vertraulichkeit	21
3.1.2	Integrität	22
3.1.3	Verfügbarkeit	23
3.1.4	Authentizität	23
3.1.5	Verbindlichkeit	24
3.1.6	Zurechenbarkeit	24
3.1.7	Resilienz	24
3.2	Datenschutz	25
3.2.1	Schutz vor Fremdzugriff	25
3.2.2	Schutz der Betroffenen	27
3.3	Technische Basis	27
3.4	FIDO	28
4	Technisches System	31
4.1	Überblick	31
4.1.1	Front-End (UI)	32
4.1.2	Back-End (Server)	32
4.1.3	Datenbank	32
4.1.4	Interne APIs	32
4.2	Externe Apis	32
4.3	Anmeldung	33
4.4	Datenbank	35
4.4.1	LiteDB	35
4.4.2	Datenbankschema	38
4.4.3	Schemadateien	39
4.4.4	Schlüsselverwaltung	40
4.4.5	Dateisystem	42
5	Umsetzung	45
5.1	Bildschirmfotos	45
5.2	Hürden und Herausforderungen	48
5.2.1	WebAuthn	49
5.2.2	Tests beim Nutzer	49

6	Tests	51
6.1	Automatisierte Tests	51
6.1.1	Kompilierung	51
6.1.2	GitLab CI Tests	51
6.2	Nutzungsdaten	52
7	Rollout	55
7.1	Installation	55
7.1.1	Manuelle Installation	55
7.1.2	Halbautomatische Installation mit Docker und CI Pipeline	55
7.1.3	Vollautomatische Installation mit Wix (Windows)	56
7.1.4	Vollautomatische Installation unter Linux	56
7.2	Stages	57
8	Ausblick	59
8.1	Nachnutzung	59
8.2	Erweiterungen	59
8.2.1	Webseite	59
8.2.2	Schnittstellen	59
8.2.3	Cloud-Dienst	60
8.2.4	Suchoptimierungen	60
8.3	Wartung und Update	61
9	Abschlussbetrachtung	63
	Literatur und Quellen	65
	Abbildungsverzeichnis	68
	Tabellenverzeichnis	69
	Anhang	70
A	Entity Relationship Diagramm v0.6	71
B	Projektsteckbrief	72
C	config.json Schema	72
D	Rollenschema	78
E	Dacrypto - Internal WebSocket API	80
E.1	PUB /ws/ Operation	80
E.1.1	AccountLogin	80
E.1.2	AccountRegister	80
E.1.3	DatabaseAddFinish	81
E.1.4	DatabaseAddRequest	82
E.1.5	DatabaseCancelCreation	82
E.1.6	DatabaseConnect	83
E.1.7	DatabaseRemoveUser	83
E.1.8	DatabaseUnlock	84
E.1.9	DataInterviewAddRequest	84
E.1.10	DataInterviewGet	85
E.1.11	DataInterviewListPersonRequest	85
E.1.12	DataPersonAddRequest	86
E.1.13	DataPersonGet	86

	E.1.14	DatabaseUnlock	87
	E.1.15	EditAttributeSend	87
	E.1.16	EditPersonSend	88
	E.1.17	FidoReceive	88
	E.1.18	FileChangeConfidential	89
	E.1.19	FileDelete	90
	E.1.20	FileFetch	90
	E.1.21	FileMove	91
	E.1.22	FilePersonFetch	91
	E.1.23	FileRename	92
	E.1.24	InfoRequest	92
	E.1.25	PerformReindex	92
	E.1.26	SchemaRequest	93
	E.1.27	SearchCancel	93
	E.1.28	SearchSend	94
E.2	SUB /ws/	Operation	94
	E.2.1	AccountFidoRequest	95
	E.2.2	DatabaseAddRequestInfo	95
	E.2.3	DataInterviewAddSend	96
	E.2.4	DataInterviewListPersonSend	96
	E.2.5	DataInterviewSend	97
	E.2.6	DataPersonAddSend	98
	E.2.7	DataPersonSend	100
	E.2.8	DatabaseCreated	102
	E.2.9	EditAccept	102
	E.2.10	EditDenied	103
	E.2.11	FidoResult	104
	E.2.12	FileMoved	105
	E.2.13	FilePersonSend	107
	E.2.14	FileSend	109
	E.2.15	FileUpdated	111
	E.2.16	InfoSend	113
	E.2.17	LoginRequest	114
	E.2.18	SchemaResponse	115
	E.2.19	SearchResponse	116
	E.2.20	SendNotification	118
F	Suchquery	121
	F.1	Sonderzeichen	121
	F.2	Begriffe	121
	F.3	Explizite Ausdrücke	122
	F.4	Optionen	122
		F.4.1 Attribute	123
		F.4.2 Felder	124
		F.4.3 Typ	125
		F.4.4 Rolle	125
		F.4.5 Sortierung	125
	F.5	Operatoren	126
		F.5.1 Negation	126
		F.5.2 AND, OR, XOR	127

	F.5.3	Gruppen	128
	F.5.4	Auflistung	128
F.6		Scoring	129
F.7		Query-Optimierung	129
F.8		Beispiele:	131

1 Einleitung

Diese Arbeit wurde am Max-Planck-Institut für ethnologische Forschung (MPI) und dem Institut der Informatik der Martin-Luther-Universität Halle-Wittenberg erstellt. Das Ziel ist das Forschungsdatenmanagement von ethnologischen Instituten (in diesem Fall das MPI) mithilfe aktueller Techniken und Software zu verbessern.

"Das Max-Planck-Institut für ethnologische Forschung ist eines der führenden Forschungszentren auf dem Gebiet der Ethnologie. Forschungsleitend ist die vergleichende Untersuchung gegenwärtiger sozialer Wandlungsprozesse. Auf diesem Gebiet leisten die Wissenschaftlerinnen und Wissenschaftler des Instituts einen wichtigen Beitrag zur ethnologischen Theoriebildung. Sie befassen sich darüber hinaus in ihren Projekten oft auch mit Themen, die im Mittelpunkt politischer Debatten stehen."(Quelle: [27])

Die Forscher des MPI begeben sich bedingt durch ihre Tätigkeit auf weltweite Reisen, um mit einer großen Vielfalt an Personen Interviews zu führen und Daten für ihre Forschung zu sammeln. Hauptsächlich werden diese Interviews in Papierform (handschriftliche Notizen) oder als einfache Audioaufnahmen dokumentiert. Letzteres wird in viel manueller Arbeit als Textdatei transkribiert und alles zusammen in einer großen Sammlung an Word-Dokumenten abgespeichert und archiviert.

Eine weitere Verarbeitung mit diesen Dokumenten erfolgt dann nur noch über das Programm Microsoft Word und/oder mit den Ausdrucken in Papierform. Diese Dokumente erfahren häufig keine richtige Versionierung (Änderungen sind nicht mehr oder schwer nachvollziehbar) und spätestens beim Teilen mit Forschungskollegen entstehen Duplikate, die später nur sehr aufwendig händisch vereinigt werden.

Ein weiterer wichtiger Aspekt ist die Sicherheit der aufgenommenen Daten. Die Daten waren bisher ungesichert auf Papier oder auf elektronischen Datenträgern hinterlegt und es war bisher schwierig, diese vor unbefugten Einsehen oder vor Zerstörung zu schützen. Dies kann mitunter an Grenzübertritten in Staaten wie China ([43] und [42]), USA (siehe Absatz "Besondere Sicherheitsmaßnahmen", [7]) und Neuseeland (siehe Absatz "Einfuhrbestimmungen", [6]) geschehen, bei denen das Gepäck inklusive Datenträger oder Computer/Mobiltelefone durchsucht, einbehalten oder mit Trojanern versehen werden. In dieser Arbeit wird dieser Aspekt der Sicherheit sehr hoch angesehen und es wurden verschiedene Leitlinien für den sicheren Umgang mit Daten umgesetzt.

Zur Sicherheit gehört auch der Datenschutz selbst, welcher gesetzlich durch das europäische Datenschutzgrundgesetz (DSGVO, GDPR) und durch das Bundesamt für Sicherheit und Informationstechnik (BSI) geregelt ist. Nur berechnigte Personen sollen Zugang zu den Daten haben, diese einsehen oder modifizieren können. Dazu wurde in erster Linie eine Zwei-Faktor-Authentifizierung eingeführt. Zum Datenschutz gehört es auch, dass bestimmte Daten ab einen bestimmten Zeitpunkt nicht mehr für die Forschung relevant und deshalb anonymisiert, das heißt für den Forscher nicht mehr zugänglich sein sollen. Als Beispiel lassen sich hier besonders schützenswerte Daten wie Name, Kontakt, Religionsangehörigkeit und Gesundheitsstatus der Befragten nennen. Außerdem sollen bestimmte Daten mit Forschungskollegen auf sicheren Wegen geteilt werden können, bei dem die Anonymisierung und der Datenschutz nicht verletzt werden.

Ein strukturiertes Abspeichern der Daten und eine schnelle Suche in diesen ist der zweite große Punkt, der in dieser Arbeit verfolgt wird. Dem Forscher soll es möglich sein, seine

Daten schnell, einfach und sicher eingeben zu können und sehen, was sich wann geändert hat. Dadurch wurde auch der Grundsatz der Versionierung berücksichtigt.

Der letzte große Punkt ist das einfache Teilen und Erstellen eines Back-ups der Daten selbst. Diese wurde mit Imports und Exports der Datenbanken selbst geregelt.

In dieser Arbeit kommen unterschiedliche moderne Techniken zum Einsatz. Dazu zählen das Datenbankmanagementsystem LiteDB, die Programmiersprachen C# und Elm, eine moderne Oberfläche im Webbrowser, die 2-Faktor-Authentifizierung mittels WebAuthn und Fido2 und Datensicherheit und Verschlüsselung per Design.

Diese Arbeit ist um den Entwicklungsprozess der Anwendung strukturiert. Im ersten Kapitel nach dieser Einleitung geht es um die inhaltlichen und technischen Anforderungen, die an die Anwendung gestellt werden und eine Auswahl der Komponenten wird getroffen. Im nächsten Kapitel geht es um die Sicherheit, den Datenschutz und die technische Basis dazu. Danach wird das technische System entworfen und die einzelnen Komponenten werden genauer beleuchtet. Schließlich geht es um die Umsetzung und die Stolpersteine, die dabei aufgetreten sind. Im darauffolgenden Kapitel geht es um die Tests, welche genutzt wurden und welche Vor- bzw. Nachteile dabei auftraten. Anschließend geht es darum, wie die Anwendung an alle Nutzer ausgerollt wird und welche Zyklen dabei durchlaufen werden. Nach diesem Kapitel kommt dann der Ausblick, in dem die Nachnutzung, Erweiterungen, Wartung und Updates genauer beleuchtet werden. Das letzte Kapitel enthält das Fazit der Arbeit.

2 Anforderungen

In den Gesprächen mit den Forschern und dem Auftraggeber wurde eine Liste an Anforderungen erstellt, die für das Projekt zu erfüllen sind. Dazu gehören inhaltliche Anforderungen, welche besagen, was die Anwendung für den Forscher primär leisten soll. Aber auch strukturelle Anforderungen, wie mit dem Daten, die der Forscher bei seinen Forschungen erstellt oder welche bei der Arbeit mit dem Programm entstehen, verarbeitet und gespeichert werden sollen. Weiterhin müssen auch technische Anforderungen über den Aufbau der Anwendung, die Speicherdauer und Architektur erfüllt werden.

2.1 Inhaltliche Anforderungen

Die Anwendung soll die Daten, welche bei den Forschungsreisen und Interviews eines Forschers anfallen, aufnehmen, übersichtlich darstellen und organisieren. Zu diesen Daten gehören folgende:

- **Informationen über den Interviewpartner**

Dazu zählen Kontaktinformationen wie Name, Adresse und Telefonnummer. Außerdem müssen je nach Interviewpartner auch bestimmte Dokumente hinterlegt werden, wie die unterschriebene Datenschutzerklärung.

- **Arten der Interviewpartner**

Diese sind je nach Forschungsthema unterschiedlich und können zum Beispiel Patient, Arzt, Krankenpfleger, familiäre Angehörige und religiöse Beistehende sein.

- **Familiäre Beziehungen zwischen den Interviewpartnern**

Dies ist je nach Forschungsthema unterschiedlich, ob diese überhaupt aufgenommen werden sollen oder dürfen.

- **Informationen wann und wo ein Interview stattgefunden hat und wer dort interviewt wurde**

- **Antworten auf bestimmte Fragen**

Dies ist vom Forschungsthema abhängig und die Antworten darauf können sehr unterschiedlich ausfallen. Die Fragen sind zudem von der Art des Interviewpartners abhängig.

- **Dateien zu den Interviewpartnern**

Das können Familienfotos, Tonbandaufnahmen, Fotos vom Wohnhaus oder Skizzen sein. Hier ist die Art der Dokumente je nach Interviewpartner unterschiedlich. Zum Teil lassen sich auch mehrere Dateien gruppieren.

Ein Teil der Daten unterliegt besonderen Regeln des Datenschutzes (besonders schützenswerte Daten wie Name und Kontaktinformation) und dürfen zu bestimmten Zeitpunkten nicht mehr für die Forschung genutzt werden. Diese müssen anonymisiert und Daten, welche auf Personen zurückschließen lassen, entfernt werden. Die entfernten Daten müssen an einen sicheren Platz für eine spätere Einsicht aufbewahrt werden. Dies betrifft zum Beispiel den Klar-Namen und Kontaktdaten des Betroffenen. Für die Aufnahme und Durchführung des Interviews sind diese Daten noch relevant. Bei der Auswertung der Daten sollen diese nicht mehr verfügbar sein und spätestens bei der Veröffentlichung darf nichts mehr enthalten sein, was eine spätere Identifikation der Person ermöglicht (z. B. "Chefarzt im Krankenhaus

der Stadt X, welcher einen Schnurrbart trägt, ...”). Die betroffene Person kann später immer die Löschung der eigenen Daten verlangen. Dafür werden wieder die Kontaktdaten und eine Zuordnung, welche anonymisierte Daten dadurch betroffen sind, gebraucht. Daher ist ein einfaches Löschen der Zuordnungen nicht möglich.

In der Praxis werden Zuordnungstabellen zu den Kontaktinformationen erstellt. Diese werden dann in gedruckter Form oder als digitales Medium in einem sicheren physischen Tresor verwahrt. Für die Forschung steht die Person dann nur noch als anonyme ID zur Verfügung.

2.2 Technische Anforderungen

Zusätzlich zu den inhaltlichen Anforderungen kommen noch die technischen Anforderungen. Hier werden nur das System selbst und die Back-ups genauer beleuchtet.

2.2.1 System

An dem technischen System werden bedingt durch das Nutzungsszenario eine große Vielfalt an Bedingungen gestellt, die es erfüllen muss:

1. Die Forscher sollen die Anwendung auf ihren Forschungsreisen nutzen, weswegen es vorkommen kann, dass es dabei zeitweise keinen Internetzugriff gibt. Daher müssen alle Daten offline verfügbar sein. Dennoch können online Back-ups erstellt werden, sobald eine Internetverbindung wieder besteht.
2. Es ist von sehr großen Datenmengen auszugehen. Die Forscher werden auf ihren Reisen mehrere hundert bis tausend Bildern und Videos aufnehmen. Daher muss das Zielgerät entsprechend Speicherplatz für die Anwendung bereitstellen. Für die externen Geräte (z. B. Kamera) müssen außerdem Anschlüsse vorhanden sein, um Daten übertragen zu können.
3. Des Weiteren muss für den Verschlüsselungsprozess auch die benötigte Rechenleistung zur Verfügung stehen.
4. Der Forscher wird mit vielen Daten gleichzeitig arbeiten müssen. Daher ist eine Oberfläche erforderlich, die dies einfach und effizient ermöglicht.
5. Die Geräte müssen relativ kostengünstig sein, da diese auf Forschungsreisen kaputt gehen, verloren oder gestohlen werden können und daher leicht zu ersetzen sein müssen.
6. Die Geräte sollten dem Forscher vertraut sein, damit sie den Arbeitsfluss erleichtert.

Aus diesen Anforderungen ergibt sich nach aktuellem Stand ein günstiger Laptop. Ein Mobiltelefon, welches derzeit eine größere Verbreitung als ein Laptop gefunden hat, kommt aus folgenden Punkten leider derzeit nicht infrage:

1. Die 2. Bedingung kann bei vielen Mobiltelefonen nur bedingt erfüllt werden. Es werden große Datenmengen von deutlich mehreren GB (hauptsächlich durch Bilder und Videos) erwartet, welche auf den begrenzten internen Speicher nur schlecht gespeichert werden können. Es gibt zwar Möglichkeiten der SD-Karten Erweiterung, welche aber immer seltener werden. Stattdessen bieten Hersteller immer größeren internen Speicher zu einen schlechterem Preis-Leistungsverhältnis an.
2. Da hier günstige Geräte erwartet werden, kann die benötigte Rechenleistung nur bedingt bereitgestellt werden. Zwar sind einzelne Ver- und Entschlüsselung im Hinblick auf die Rechenzeit relativ günstig, dafür aber viel aufwendiger, wenn von mehreren

Hundert Megabyte bis Gigabyte geredet wird. Dies ist besonders bei der Arbeit mit einer verschlüsselten Datenbank der Fall.

3. Mobiltelefone haben relativ kleine Oberflächen, wodurch die Übersichtlichkeit stark eingeschränkt wird. Außerdem ist die Arbeit mit der virtuellen Tastatur langsamer als mit einer realen. Zwar ist es hier möglich externes Zubehör zur Verfügung zu stellen (Maus, Tastatur und Bildschirm über spezielle USB-Hubs oder Bluetooth), welche aber die Kompaktheit reduzieren und auch wieder Geld kosten.

Zwar lassen sich die oberen drei Gegenargumente leicht widerlegen, indem dafür spezielle Systeme und Oberflächen erstellt werden, die dafür speziell ausgelegt sind, das erhöht aber nur den Umfang der Arbeit enorm. Dies kann aber eine Möglichkeit der zukünftigen Fortentwicklung sein.

Es gäbe noch die Möglichkeit, neben der Bereitstellung auf einem Laptop oder Mobiltelefon dies auch als Web-App (eigenständige Anwendung im Webbrowser) bereitzustellen. Dies beinhaltet leider das Problem, dass die Daten auch offline verfügbar sein müssen. Zwar ist es hier möglich, den Browser-Cache und -Speicher zu nutzen, um bestimmte Daten zwischenspeichern, dieser ist aber leider in seiner maximalen Größe sehr stark begrenzt und es ist nicht möglich die komplette Datenbank dort unterzubekommen. Aufgrund der Komplexität wird diese Möglichkeit daher derzeit nicht in Betracht gezogen.

Das Max-Planck-Institut für ethnologische Forschung stellt seit Jahren seinen Forschern Windows-Laptops zur Verfügung, wenn diese sich auf eine Forschungsreise begeben. Nach dem aktuellen Mobile-Device-Management-Plan sollen iPhone-Mobiltelefonie zum Reporteau hinzugefügt werden. Aus oben genannten Gründen werden diese iPhones vorerst nicht berücksichtigt. Das primäre Entwicklungsziel ist daher ein Laptop mit dem Betriebssystem Windows.

2.2.2 Back-ups

Es ist erforderlich, in regelmäßigen Abständen Back-ups von den Daten erstellen zu können. Dies beinhaltet die komplette Datenbank inklusiver Metadaten, damit bei einem Ausfall, Verlust, etc. die Daten leicht wiederhergestellt und daran weitergearbeitet werden kann.

Hierzu ist die Nutzung eines Cloud-Speicher-Dienstes geplant, welcher die Daten aus einem lokalen Ordner automatisch mit der Cloud synchronisiert. Eine Herausforderung hierbei ist, dass es zu Problemen mit der Synchronisierung kommen kann, wenn die gleiche Datenbank auf zwei Geräten offen ist und über die gleiche Cloud synchronisiert wird. Hier kann es zu Kollisionen kommen, welche sich nur schwer beheben lassen. Das ist vor allem deshalb der Fall, weil die Daten nur verschlüsselt und binär vorliegen und sich daher eher schlecht vergleichen lassen.

2.3 Wahl der Komponenten

Für die jeweiligen Komponenten stehen verschiedene Optionen zur Verfügung. Hier wird für jede Komponente verglichen und ausgewählt, welche Option genutzt wird.

2.3.1 Front-End (UI)

Für die Oberfläche wurde eine Web-Oberfläche gewählt. Diese bietet den Vorteil, dass ohne viel Änderungen an der Codebasis die Oberfläche auf verschiedenen Geräten und Systemen angewandt werden kann. Außerdem modularisiert eine Web-Oberfläche die Codebasis mehr,

was die Austauschbarkeit und Wartung verbessert. Zudem lässt sich dadurch leichter für verschiedene Plattformen entwickeln (Windows, Linux, Mac, Android, ...).

Im Browser, der die Web-Oberfläche darstellt, gibt es derzeit zwei Technologien, die dafür genutzt werden können, um Code auszuführen: Javascript und Web-Assembly (kurz: WASM). Javascript ist eine Skriptsprache, welche früher vom Browser interpretiert wurde (derzeit wird sie meistens vor der Ausführung übersetzt) und hat den vollen Umfang der Browser APIs. WASM ist eine neuere Technologie, welche als Byte Code von einer virtuellen Maschine des Browsers ausgeführt wird. WASM hat nur Zugang zu den meisten Browser APIs, indem es über eine Javascript-Schnittstelle kommuniziert.

Tabelle 1: Übersicht Programmiersprachen

Sprache	C#	Java	C/C++	Rust	Java-Script	Elm	Type-Script
Erscheinungsjahr	2001	1995	1985	2015	1995	2012	2012
Browser	WASM	WASM	WASM	WASM	nativ	JS	JS

Bei Browser wird aufgelistet, welche Technologie genutzt wird, um den Code im Browser auszuführen. WASM steht für Web-Assembly und JS für Javascript. Nur Javascript selbst kann direkt im Browser ausgeführt werden und muss nicht erst in eine andere Sprache übersetzt werden.

Für die Gestaltung der Web-Oberfläche gibt es eine Vielzahl an Werkzeugen und Systemen (siehe Tabelle 1), die alle ihre Vor- und Nachteile haben und sich mehr oder weniger für dieses Projekt eignen. Bei der Vorauswahl wurde mit Absicht nur eine Teilmenge der Möglichkeiten herausgesucht, da es den Rahmen dieser Arbeit sonst sprengen würde, wenn alle berücksichtigt werden. In dem Vergleich wurden in erster Linie Programmiersprachen herausgesucht, mit denen der Autor vertraut ist oder sich relativ schnell aneignen kann. In diesem Vergleich kommen C#, Java, C/C++, Rust, Javascript, Type-Script und Elm zum Einsatz.

C# ist eine objektorientierte Sprache, welche 2001 von Microsoft veröffentlicht wurde. Über die Umgebung Blazor ist es möglich, diese als WASM im Browser auszuführen. Dazu gibt es Nuget, einen Paketmanager für Dotnet (dazu gehört auch C#) Bibliotheken, welcher es ermöglicht, einfach eine Vielzahl bereits vorhandener Bibliotheken einzubinden. Dies erleichtert die Entwicklung deutlich, da so eine Fokussierung auf die individuellen Projektanforderungen möglich ist.

Java ist 1995 von Sun Microsystems veröffentlicht wurden. Früher wurde dies gern für Java Applets im Browser genutzt, seit der Einführung von HTML 5 wird es aber mehr und mehr von Browsern nicht mehr unterstützt. Einen großen Einfluss darauf hatte auch, dass dies generell nicht auf Mobilgeräten genutzt werden konnte. Mittlerweile lässt sich dies über extra Build-Prozesse in WASM übersetzen und im Browser ausführen.

C/C++ ist die älteste Programmiersprache, welche in dieser Auswahl einbezogen wurde, und wurde 1972 (C) bzw. 1985 (C++) veröffentlicht. Diese Programmiersprache ist sehr hardwarenah und ist quasi das Schweizer Taschenmesser für alle möglichen Zwecke und Umgebungen. Über einen speziellen Compiler lässt sich dies in WASM übersetzen.

Rust ist 2015 von Mozilla veröffentlicht wurden und soll genauso wie C/C++ hardwarenah

Code erlauben, aber auch wie C# oder Java sehr abstrakt sein können. Rust arbeitet sehr effizient mit dem Arbeitsspeicher und das ohne Garbage Collection oder einer Runtime (wie in C# oder Java). In Rust geschriebene Programme sind sehr speichersicher, da der Compiler viele Fehler entdeckt und prüft oder es durch die Programmiersprache nicht möglich ist, diese zu machen. Zu solchen Fehlern zählen noch benutzten Speicher freizugeben oder auf die gleiche Speicherstelle von unterschiedlichen Stellen gleichzeitig schreibend zuzugreifen. Ein großes Argument für Rust ist also die Nähe am Arbeitsspeicher und die hohe Abstraktion ohne zusätzliche Laufzeit, die zur Verfügung gestellt wird. Zudem kann der Compiler direkt nach WASM übersetzen.

Javascript (1995) ist eine Script-Sprache, welche für Anwendungen im Browser entwickelt wurde. Diese ist dynamisch typisiert und prototypisch. Dies führt leicht zu schwer erkenn- und wartbaren Fehlern, da oftmals der genaue Typ und die Daten erst bei der Ausführung bekannt sind. Zudem lassen sich die Prototypen zur Laufzeit jederzeit bearbeiten, was zu ungewünschten Seiteneffekten führen kann.

Type-Script wurde 2012 von Microsoft als Erweiterung zu Javascript herausgebracht, in der versucht wurde, ein paar Probleme von Javascript anzugehen. Zum Beispiel ist es jetzt möglich, Typen zu annotieren, welche von einem Compiler geprüft werden. Es ist aber erlaubt, Type-Script und Javascript beliebig zu mischen, wodurch es sehr leicht ist, die oben genannten Fehler einzubauen oder zu verursachen. Für Javascript und Type-Script gibt es eine große Anzahl Frameworks, die die Entwicklung vereinfachen sollen, aber auf die hier nicht weiter eingegangen wird.

Elm wurde im gleichen Jahr wie Type-Script veröffentlicht, ist funktional und an die Programmiersprache Haskell angelehnt. Elm wurde für den Browser entworfen, wodurch der Compiler direkt in Javascript übersetzt. Es gibt derzeit Anstrengungen auch nach WASM zu übersetzen, was aber derzeit noch nicht vollständig unterstützt wird (siehe [13]). Elm hatte sich auch das Ziel gesetzt, die oben genannten Probleme in Javascript anzugehen. Zum Beispiel schließt dazu der Elm Compiler Laufzeitfehler generell aus und die Sprache ist typsicher. Weiterhin übersetzt der Compiler den Quellcode in optimierten Javascript-Code, welcher möglichst kompakt und schnell ausgeführt werden kann (siehe [18]).

Diese Technologien sind alle sehr unterschiedlich weit verbreitet, was unter anderem auch daran liegt, wer diese gefördert hatte. Hinter C# und Type-Script zum Beispiel steht Microsoft und unterstützt seit Langem die Verbreitung. Dies zeigt sich zum Beispiel an der Menge an verfügbaren Bibliotheken, Dokumentation und existierenden Projekten.

Hinter Rust stehen primär Mozilla und die Rust Foundation und es gewinnt in den letzten Jahren immer mehr an Popularität (siehe [34]). Es wird vor allem die hohe Performance gelobt, hat aber auf der anderen Seite eine äußerst steile Lernkurve.

Es ist zwar, wie oben gesagt, möglich Java und C/C++ im Browser auszuführen, aber dies ist eher weniger dokumentiert und es gibt vergleichsweise wenige Projekte dazu.

Im Gegensatz dazu steht Elm, was sehr gut dokumentiert ist, eine große Bibliothek hat und recht leicht zu erlernen ist. Die Verbreitung dahinter ist vergleichsweise eher gering einzuschätzen.

Für diese Arbeit wurden folgende Kriterien für die Auswahl der Programmiersprache festgelegt:

1. Sie muss im Browser ausführbar sein.
2. Sie muss sicher und möglichst ohne Laufzeitfehler funktionieren.

3. Sie muss leicht zu debuggen und zu warten sein.
4. Sie muss eine gute Dokumentation existieren.

Zumindest Punkt 1 und 4 lässt sich bei allen mit “Ja” beantworten. Punkt 2 lässt sich aus Erfahrungssicht des Autors nur bei Rust und Elm mit “Ja” beantworten. Es ist aber möglich, bei den anderen Programmiersprachen dies mit mehr oder weniger Aufwand zu erreichen.

Bei Punkt 3 muss hier eine Unterscheidung getroffen werden. Das Problem ist hierbei WASM, was nur über eine virtuelle Maschine im Browser ausgeführt wird und daher keinen direkten Zugang hat. Hierfür muss erst eine spezielle Umgebung eingerichtet werden, was je nach Programmiersprache mehr oder weniger aufwendig ist. Klar im Vorteil ist hier Javascript, da die meisten modernen Browser genügend Werkzeuge mitliefern.

Ein Ausreißer ist hierbei Elm, da es von einer anderen Sprache in Javascript übersetzt wird, sind die Werkzeuge des Browsers teilweise nicht hilfreich (zumindest die, auf die der Code genauer eingehen) oder nutzlos (da das Konzept von Elm diese nicht braucht). Dafür ist Elm stark modularisiert und funktional aufgebaut und bietet für sein Modell-Update-View-Konzept genügend eigene Werkzeuge, um zu debuggen.

Insgesamt wurde sich hier für Elm entschieden, da es zum einen alle Kriterien erfüllen kann und zum anderen der Entwicklungsprozess damit vergleichsweise leicht und schnell vonstattengehen kann.

2.3.2 Back-End (Server)

Die Anwendung ist modular aufgebaut mit einer Web-Oberfläche und einem dazugehörigen Server. Dieser kümmert sich um die Verwaltung der Datenbanken, die Verschlüsselung, Verifikation und Back-ups. Das ist eine vergleichsweise große Palette an Aufgaben. Außerdem muss der serverseitige Teil eine Schnittstelle zur Oberfläche bereitstellen, damit diese auch Daten austauschen können.

Tabelle 2: Übersicht Programmiersprachen

Sprache	C#	Java	C/C++	Rust	Java-Script	Elm	Type-Script
Erscheinungsjahr	2001	1995	1985	2015	1995	2012	2012
Windows	nativ	nativ	nativ	nativ	Node.js -		Node.js
Linux	nativ	nativ	nativ	nativ	Node.js	-	Node.js
Docker	nativ	nativ	nativ	nativ	Node.js	-	Node.js

Hier wurde geschaut, wie Programme in der Programmiersprache auf dem Rechner ausgeführt werden kann. Nativ kann ohne externe Werkzeuge und Node.js nur mit dem Programm Node.js. Bei Docker wurde nur geschaut, ob sich dies in einem Dockercontainer ausführen lässt. Zur Anwendung kommt dies aber in dieser Arbeit nicht. Bei Elm ist dieser Vergleich nicht anwendbar.

Hierfür wurden verschiedene Programmiersprachen verglichen (siehe Tabelle 2). Dabei gilt hier, dass die Programme auf dem Computer des Nutzers und nicht im Web-Browser ausgeführt werden soll. Ein Teil der Programmiersprachen kann nativ ohne externe Werkzeuge auf dem Zielrechner ausgeführt werden. C# und Java übersetzen hierbei aber nicht in

Maschinensprache, sondern in eine Zwischensprache, die von einer Art virtuellen Maschine ausgeführt wird. Alle anderen Sprachen, die nach Javascript übersetzen oder es selbst schon sind, können über das Programm NodeJS direkt auf dem Rechner ausgeführt werden.

Auch hier wurden ein paar Kriterien für die Auswahl definiert:

1. Es muss auf einem Windows- und Linux-Rechner ausführbar sein.
2. Es muss recht schnell und zuverlässig seine Aufgaben ausführen. Das bedeutet, dass die Laufzeiten für Aufgaben in einem für den Nutzer angemessenen Rahmen sein müssen.
3. Es muss sicher und möglichst ohne Laufzeitfehler funktionieren.
4. Es muss leicht zu debuggen und zu warten sein.
5. Es muss eine gute Dokumentation existieren.
6. Es muss ein großer Umfang an Bibliotheken existieren, um die Aufgaben zu bewältigen.
7. Es muss multi-threaded arbeiten, um die gesamte Rechenleistung des Computers für die Aufgaben nutzen zu können.
8. Es muss möglichst weit verbreitet sein, damit das Projekt langfristig gewartet werden kann. Dies ist insbesondere für die Daten in der Datenbank wichtig.

Hier stellt sich schnell heraus, dass Elm für diese Aufgaben völlig ungeeignet ist, da diese Programmiersprache nicht dafür designt wurde. Es ist zwar theoretisch möglich, Programme in Elm auf dem Rechner ohne Web-Browser ausführen zu lassen, aber dies ist mit enormem Aufwand verbunden, da hier ein Großteil der nötigen Bibliotheken fehlt (z. B. zum Netzwerk oder zum Dateisystem).

Ansonsten treffen fast alle Kriterien auf alle anderen Kandidaten zu. Punkt 3 lässt sich am besten bei Rust umsetzen. Hier wird der Entwickler durch Sprache und Compiler dazu gezwungen, den Speicher sicher und sauber zu halten, und es kommt nicht zu Laufzeitfehlern (was nicht heißt, dass das Programm abstürzen, quasi “panicken”, kann). Dafür ist es aber eher weniger verbreitet (Punkt 8) und hat eine steile Lernkurve und braucht daher einiges an Einarbeitungszeit.

Der Punkt 7 ist in NodeJS zwar möglich, aber umständlicher zu erreichen als bei den anderen Kandidaten. Daher eignen sich hier Programmiersprachen, die nicht auf NodeJS angewiesen sind.

Zwar ist es praktisch, wenn der Entwickler eine Programmiersprache hat, die sehr maschinennah arbeitet (C/C++), um den letzten Funken Geschwindigkeit rauszuholen, aber für dieses Projekt ist es auch in Ordnung, wenn eine andere genutzt wird. Solange die gesamte Reaktionszeit sich im akzeptablen Rahmen hält. Da für diese Arbeit die Entwicklungszeit relativ knapp bemessen ist, wird hier auch eine Programmiersprache bevorzugt, die einfacher und schneller zu schreiben ist.

Unter Berücksichtigung der oben genannten Punkte hat sich der Autor für die Programmiersprache C# entschieden. Diese ist mit über einer Millionen GitHub Repository (siehe [35]) sehr weit verbreitet, arbeitet schnell und zuverlässig und kann auch in den restlichen Anforderungen gut punkten. Durch den Compiler und die Interpretationsschicht ist sie gleichzeitig auch so weit von der Maschine abstrahiert, dass es mit ihr möglich ist, schnell Code zu schreiben, ohne auf die zugrunde liegende Maschine genauer eingehen zu müssen.

2.3.3 Datenbank

Die Datenbank ist ein kritisches Thema, da sie alle sensiblen Daten des Forschers enthält und speichern muss. Gleichzeitig reicht es für die Datenbank nicht aus alle Daten einfach zu speichern, sondern diese muss diese Daten auch in angemessener Zeit wieder bereitstellen, damit die Daten weiterverarbeitet werden können. Dies kann eine einfache Anzeige der Daten oder eine Suche nach bestimmten Datensätzen sein.

Daher wurden folgende Kriterien für die Auswahl des Datenbankenmanagementsystems (DBMS) festgelegt:

1. Sicherheit: Die Daten müssen verschlüsselt auf der Festplatte vorliegen. Auch der Schlüssel muss sicher sein.
2. Zugriff: Der Server braucht einen schnellen und einfachen Zugriff auf die Daten. Dies bedeutet, dass die API einfach für den Server und Programmierer zu nutzen und zu verstehen sein muss. Gleichzeitig müssen die Daten in angemessener Zeit verfügbar sein, damit nicht lange Wartezeiten verursacht werden.
3. Back-ups: Sicherheitskopien müssen sich leicht erstellen lassen.
4. Angriffsoberfläche: Je mehr Funktionen ein DBMS liefert, desto mehr Schwachstellen kann diese haben. Diese müssen alle einzeln abgesichert werden. Das kann erhöhten Konfigurationsaufwand für den Anwender bedeuten. Weniger oder das komplette Deaktivieren nicht benötigter Funktionen kann eine Erleichterung für die Einrichtung und Verwaltung einer Datenbank bedeuten.
5. Lizenzen: Die Lizenz muss mit dieser Arbeit kompatibel sein. Daher ist es schwierig, kommerzielle Lizenzen zu nutzen.

Tabelle 3: Übersicht der DBMS

Katego- rie	MariaDB	MySQL	SQLite	MongoDB	LiteDB
Webseite	mariadb.org [31]	mysql.com [46]	sqlite.org [16]	mongodb.com [38]	litedb.org [22]
Relatio- nal	x	x	x		
Art	server- basiert	server- basiert	embedded	server- basiert	embedded
Lizenz	GPL 2.0	GPL 2.0*	public domain	SSPL v1 [40]	MIT
Open Source	GitHub [30]	GitHub [49]	Sqlite.org (Fossil) [17]	GitHub [39]	GitHub [23]
Preis	free	free*	free	free	free
Erster Release	29.10.2009	23.05.1995	17.08.2000	11.02.2009	17.09.2016

MySQL ist nur dann kostenlos und unter GPL 2.0, wenn das gesamte Produkt auch unter der GPL 2.0 veröffentlicht wird. Ansonsten handelt es sich um eine kostenpflichtige Lizenz. Siehe [47].

Für den Vergleich wurden MariaDB, MySQL, SQLite, MongoDB und LiteDB einbezogen (siehe Tabelle 3). Es mag noch mehr Möglichkeiten geben, aber diese fünf sind die Gebräuchlichsten mit Bibliotheken für C#.

Tabelle 4: Lokale Verschlüsselung der DBMS

Kategorie	MariaDB	MySQL	SQLite	MongoDB	LiteDB
komplette Datenbank	supported [28]	nur in kostenpflichtiger Enterprise-Version [48]an	alternativer Fork [32]	aufwendig und nur Felder [37]	supported [21]
einzelne Tabellen	supported		nur komplette Datenbank	nur Felder	nur komplette Datenbank
Engines	XtraDB, InnoDB, teilw. Aria		alle	alle	alle
Speicherort der Schlüssel	lokale Datei	zentral in einer Schlüsselverwaltung	frei	frei	frei
Methode	AES	AES	AES	AES	AES

MariaDB: Bei aktivierter Verschlüsselung kann es zu Back-up-Problemen kommen, da externe Programme die Logs nicht lesen können (mit Ausnahme von MariaDB Back-up). Weiterhin ist der Galera gcache in der Community Version unverschlüsselt - in der kostenpflichtigen Version dagegen schon. Die Logs **general query log**, **slow query log**, **aria log** und **error log** sind unverschlüsselt. Es müssen viele Konfigurationen am Server angepasst und ein Verschlüsselungs-Plugin installiert werden. Der Verschlüsselungs-Key muss in irgendeiner Art und Weise als lesbare, unverschlüsselte Datei auf der Festplatte liegen. (siehe [29])

Punkt 1 ließ sich von keinen DBMS außer LiteDB zufriedenstellend erfüllen (siehe Tabelle 4). Zum Teil ist ein enormer Aufbau nötig, der Schlüssel liegt unverschlüsselt auf der Festplatte, es müssen unbekannte Patches genutzt werden oder es ist nur möglich, die Werte innerhalb der Zellen zu verschlüsseln. Was auch nicht sein darf, ist, dass Daten unverschlüsselt in Logs stehen können (MariaDB).

Punkt 2 ist nur bei MongoDB unzufriedenstellend. Bei allen anderen reicht es beim Verbindungsaufbau den Schlüssel auszutauschen oder zu authentifizieren und danach läuft alles transparent ab. Bei MongoDB muss dagegen bei jedem Einfügen, Bearbeiten oder Suchen ein Schlüssel übermittelt werden und die Anfrage muss gleichzeitig den Ver- und Entschlüsselungsprozess beinhalten.

Back-ups von einzelnen Datenbanken lassen sich bei Standalone DBMS schwieriger anlegen. Hier sind die Daten z. T. an mehrere Orte verteilt und es gibt aufwendige Prozesse, lokale Back-ups wiederherzustellen. Alternativ ist es möglich, alle Daten in ein allgemein lesbares Format (z. B. SQL) zu exportieren und später wieder importieren. Dies dauert aber in der Regel deutlich länger als eine einfache lokale Kopie der Daten. DBMS, die im Prozess der Anwendung laufen, sind dagegen meist so gestrickt, dass 1-2 lokale Dateien mit allen Daten existieren, welche einfach nur kopiert werden müssen.

Ein weiterer Nachteil bei Standalone-DBMS ist, dass diese naturgemäß eine größere Angriffsfläche nach außen bieten, da sie eine Vielzahl von Nutzern Zugriff gewährt.

Tabelle 5: Autorisierung der DBMS

Kategorie	MariaDB	MySQL	SQLite	MongoDB	LiteDB
Nutzerautorisierung	x	x	-	x	-
Mehrere Accounts	x	x	-	x	-
Rollen	x	x	-	x	-
Rechtmanagement	detailliert	detailliert	-	detailliert	-

Hier wurde geschaut, ob die jeweiligen DBMS die bestimmten Funktionen haben.

Um dies möglichst gut abzusichern, ist eine Konfiguration des Webservers und Einrichten von Accounts, Rollen und Rechten notwendig (siehe Tabelle 5). Die getesteten Embedded-Datenbanken weisen keine dieser besonderen Funktionen auf, da diese in der Regel nur von einer Anwendung genutzt werden und die sich selbst um die Rechtevergabe kümmern muss. In diesem Projekt wird eine lokale Datenbank benötigt, auf die nur ein Nutzer gleichzeitig Zugriff hat - und dies ist der Server. Daher reicht eine Datenbank aus, die im Anwendungsprozess läuft.

Vom Kostenfaktor sind alle bis auf MySQL kostenlos und unter Open-Source-Lizenzen verfügbar. MySQL ist nur dann kostenlos, falls alles unter GPL 2.0 veröffentlicht wird.

Unter Berücksichtigung aller Punkte wurde sich für LiteDB entschieden, da es als einzige die Anforderungen an die Sicherheit vollkommen unterstützt.

2.3.4 Interne Schnittstellen

Zwischen den einzelnen Modulen gibt es interne Schnittstellen, damit diese kommunizieren können. Zwischen Datenbank und Server wird dies über die verwendete Bibliothek geregelt und muss daher nicht weiter berücksichtigt werden. Zwischen FIDO Key und Web-Oberfläche wird das hauptsächlich vom Browser übernommen. Übrig bleibt nur noch die Schnittstelle zwischen dem Server und der Web-Oberfläche. Hierfür gibt es die Bedingung, dass die Schnittstelle über einen herkömmlichen Browser erreichbar, leicht erweiterbar und leicht verständlich sein soll.

Für den Großteil der Kommunikation wird eine WebSocket-Schnittstelle gewählt. Dazu wird ein Nachrichtentunnel zwischen Oberfläche und Server aufgebaut, in denen verschiedene JSON formatierte Nachrichtenpakete hin und her verschickt werden können. Dieses Protokoll ist nicht zustandsbasiert und die Kommunikation kann jederzeit in beide Richtungen erfolgen. Weiterhin ist der Tunnel zwischen beiden Teilnehmern sicher. Es kann sich keine dritte Partei (außer dem Webbrowser, da dieser ein Vermittler zwischen Weboberfläche und Server ist) einmischen und zur Laufzeit der Verbindung, was meist über die gesamte Dauer der Ausführung der Anwendung hinweg geht, sind beide Teilnehmer immer authentifiziert.

Über diese WebSocket-Schnittstelle werden so gut wie alle Nachrichten übermittelt. Das hat den Vorteil, dass beide Seiten sofort auf Ereignisse reagieren können.

Des Weiteren gibt es eine kleine REST-Schnittstelle. Hier werden über verschiedene URLs hauptsächlich Dateien angeboten, da sie meist zu groß sind, um sie über WebSocket zu übertragen. Damit wird versucht die Latenz über WebSocket möglichst gering zu halten und wichtigen Pakete jederzeit den Vorrang geben zu können.

Ein Problem besteht bei der REST-Schnittstelle, da bei jedem Aufruf eine neue Verbindung

aufgebaut wird. Dadurch ist eine Authentifizierung nicht durchgehend möglich. Dafür wird ein kurzlebiger Authentifizierungstoken über die WebSocket-Schnittstelle mitgeteilt, den die Web-Oberfläche nutzen kann, um die REST Anfragen authentifizieren zu können.

Dieses Modell wurde an der üblichen Cookie-Authentifizierung abgeschaut, die bei sehr vielen Webseiten zum Einsatz kommt. Auch hier wird einmal authentifiziert und dann wird ein Token als kurzlebiger Cookie (Session-Cookie) immer wieder von der Oberfläche an dem Server weitergereicht. Für dieses Projekt hat sich der Autor gegen einen Session-Cookie entschieden, da er die WebSocket-Verbindung als Basis für die Authentifizierung nutzen wollte.

3 Sicherheit

Dem Sicherheitsaspekt wurde eine hohe Bedeutung und Priorität zugewiesen. Dafür gibt es eine Liste an Gesetzen, die eingehalten, oder Richtlinien, welche zu befolgen sind. Das Wichtigste daraus ist die europäische Datenschutz-Grundverordnung DSGVO (im Englischen die General Data Protection Regulation GDPR).

Zu den angewandten Richtlinien zählt auch die der Europäischen Kommission [41], welche zudem auf die Sicherheit und den Schutz der Forschungsdaten eingeht.

Außerdem hat sich in der IT eine Liste an Grundsätzen durchgesetzt, auf welche in Kapitel 3.1 genauer eingegangen wird.

3.1 Grundsätze der IT-Sicherheit

Die IT-Sicherheit unterscheidet folgende Ziele: Vertraulichkeit (3.1.1), Integrität (3.1.2) und Verfügbarkeit (3.1.3; siehe [26, S. 6–11]). Dazu kommen noch weitere Schutzziele wie Authentizität (3.1.4), Verbindlichkeit (3.1.5), Zurechenbarkeit (3.1.6) und Resilienz (3.1.7) hinzu. Was diese Begriffe bedeuten und wie diese im Vergleich zu der DSGVO und Richtlinien der Europäischen Kommission stehen, wird in den folgenden Unterkapiteln beleuchtet.

3.1.1 Vertraulichkeit

Die Daten selbst dürfen nur von autorisierten Nutzern gelesen und bearbeitet werden. Dies gilt auch für den Zugriff auf gespeicherte Daten oder die Übertragung dieser.

Für eine Autorisierung stehen einem eine große Liste an Möglichkeiten zur Auswahl. Hier ein paar Beispiele:

- Verwendung von Benutzername und Passwort
- Nutzung eines Auth-Tokens (z. B. ID-Karte mit Chip und/oder NFC, USB-Sticks)
- Biometrische Daten wie Gesichtserkennung oder Fingerabdrucksensor
- externe Anbieter über die Schnittstelle LDAP oder OAuth nutzen
- physische Liste mit Einmalpasswörtern (z. B. die TAN Liste, welche früher von Banken genutzt wurde)
- Anmeldecodes per SMS oder E-Mail (wird meist zur Verifizierung als 2. Faktor genutzt)
- Kurzlebige Codes über Apps externer Anbieter (z. B. Google Auth, Microsoft Authenticator)

Es wird empfohlen, mindestens zwei dieser Möglichkeiten zu verbinden (Zwei-Faktor-Authentifizierung [53]), um einen möglichst guten Schutz erhalten.

Den Zugriff auf die gespeicherten Daten lassen sich mit folgenden Möglichkeiten absichern:

- physisches Gerät mit Daten vor unbefugten Zugriff schützen: z. B. Laptop nicht stehen lassen, Gerät nicht weitergeben
- Datenspeicher vor Zugriff schützen: Dies lässt sich z. B. mit dem Rechtssystem des Betriebssystems erreichen.
- Daten vor Zugriff schützen: z. B. den kompletten Datenspeicher verschlüsseln und nur autorisierten Nutzern ermöglichen diesen Bereich zu entschlüsseln

Die sichere Übertragung der Daten geht vergleichsweise einfacher mit einer verschlüsselten Verbindung, auch wenn es hier ein paar Hürden gibt. So soll auf ein etabliertes System (wie TLS) gesetzt werden. Aber auch hier muss darauf geachtet werden, dass die verwendeten Verschlüsselungsmethoden noch aktuell sind (z. B. MD5 und SHA-1 gelten mittlerweile als veraltet) und die verwendeten Zertifikate noch gelten.

Zertifikate, solange diese von einer vertrauenswürdigen Stelle signiert sind, sind ein probates Mittel, um den Schlüsselaustausch und die Authentizität der Gegenseite zu gewährleisten. Hier empfiehlt es sich unter Umständen sogar Zertifikate in der Anwendung mitzuliefern und sich nicht auf die installierten des Betriebssystems zu verlassen, da Nutzer (oder Viren) jederzeit unwissentlich ein kompromittiertes Zertifikat installieren können.

3.1.2 Integrität

“Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen” [52, S. 34]

Es gibt eine große Anzahl an Faktoren, welche die Integrität von Daten beeinträchtigen können. Eine große Liste hat das BSI in seinem Grundschutzkompendium im Jahre 2021 aufgelistet (siehe [52, S. 41–89]).

Für dieses Projekt sind folgende Gefahrenquellen als besonders wichtig anerkannt wurden:

“Informationen oder Produkte aus unzuverlässiger Quelle” ([52, S. 62]) können die Integrität stark gefährden, indem Daten zum einen unvollständig durch den Forscher oder externe Anwendungen aufgenommen werden. Dies kann z. B. passieren, wenn Bilder beim Upload abgebrochen oder manipuliert werden oder fehlerhafte Imports vorgenommen werden. Gleichzeitig können aber auch Drittprogramme die Schnittstellen der Anwendung fehlerhaft ansprechen.

Um hier den Schaden möglichst gering zu halten, wird allen Anfragen (egal ob vom Nutzer oder anderen Anwendungen oder auch sich selbst) grundsätzlich nicht vertraut und geprüft. Das bedeutet zwar, dass in der Regel Daten mehrfach geprüft werden, erhöht dafür aber die Wahrscheinlichkeit der Korrektheit. Gleichzeitig wird an jeder Schnittstelle davon ausgegangen, dass Daten fehlerhaft oder unberechtigt aufgenommen werden können und dafür gibt es dann entsprechende Fehlermeldungen. Falls Daten nicht vollständig sind, so wird dies dem Nutzer auch mitgeteilt und nur vollständige Datensätze werden bestätigt und weiterverarbeitet.

Ein weiteres Problem ist die “Manipulation von Hard- oder Software” ([52, S. 63]), bei der ein Nutzer oder Programme (Viren, Trojaner, ...) sich einen Zugang zum Datenspeicher oder der Anwendung verschaffen und manipulieren.

Sämtliche gespeicherte Daten sind permanent verschlüsselt auf der Festplatte und lassen sich auch ohne mehrstufige Anmeldung nicht entschlüsseln. Eine Manipulation der gespeicherten Daten kann aber dazu führen, dass Anmeldungen und somit Entschlüsselung der Datenbank fehlschlagen, da die benötigten Daten entfernt wurden. Auch die Manipulation der Datenbankdateien selbst kann im schlimmsten Fall dazu führen, dass diese nicht mehr lesbar wird und daher die Daten verloren sind. Gleiches gilt auch für die verschlüsselten Datenbank-Logs und Dateien. Gegen diesen Integritätsverlust helfen nur Back-ups.

Bei einer “Fehlfunktion von Geräten oder Systemen” ([52, S. 68]) kann z. B. das komplette Gerät ausfallen oder unzuverlässig arbeiten. Dies kann durch verschiedene Faktoren wie Alter, Unfälle (wie z. B. Wasserschaden, siehe [52, S. 45]), fehlerhafte Programmierung

oder unsachgemäße Benutzung des Nutzers geschehen. Diese haben dann meist zur Folge, dass die Daten fehlerhaft auf die Festplatte geschrieben werden, unwiderruflich beschädigt oder verloren sind. Hier hilft nur eine gute Back-up-Strategie.

3.1.3 Verfügbarkeit

Systemausfälle müssen verhindert werden und die Daten sollen nach einen vorher vereinbarten Zeitrahmen wieder verfügbar sein. Systemausfälle lassen sich leider nicht immer vermeiden und wie sorgfältig der Forscher mit dem Gerät umgeht, hat einen großen Einfluss darauf, da sich dagegen kaum Vorbereitungen treffen lassen. Wofür sich Vorbereitungen treffen lassen, ist die Wiederherstellung der Daten durch Back-ups. Indem regelmäßig Back-ups erstellt werden, ist es in einem angemessenen Zeitrahmen wieder möglich, die Daten darüber wiederherstellen. Es besteht zwar immer noch das Problem, dass beides gleichzeitig ausfallen kann, aber dafür wird die Wahrscheinlichkeit als extrem gering angesehen.

Ein Problem bei der Wiederherstellung durch Back-ups ist, dass dies nur ein altes Abbild der Daten darstellt. Sämtliche Daten, die danach generiert wurden, sind somit unwiederherstellbar verloren. Hier ist Abhilfe nur darüber möglich, indem das Back-up-Zeitfenster relativ kurz gewählt wird, damit der Umfang an verlorenen Daten nicht so groß ist.

Für die erste Iteration der Softwareentwicklung des Projektes soll behelfsmäßig zunächst ein Cloud-Speicher zur zusätzlichen Speicherung der Daten verwendet werden. Dies ist keine Back-up-Strategie per se und muss zusammen mit den Auftraggebern noch entwickelt werden.

Als Back-up-Zeitfenster wird maximal 1 Tag empfohlen. Das ist ein guter Kompromiss zwischen zu vielen Back-ups (Cloud-Speicher wird schnell voll) und der Menge an Daten, die verloren gehen können. Im schlimmsten Fall verliert der Forscher einen Tag seiner Arbeit.

3.1.4 Authentizität

Die Daten müssen auf Echtheit und Vertrauenswürdigkeit geprüft werden können. Dies erfolgt in erster Linie dadurch, dass sämtliche Daten verschlüsselt auf der Festplatte liegen. Sämtliche Schlüssel lassen sich nur erhalten, indem sich der Nutzer in der Anwendung anmeldet und somit die Daten für ihn zugänglich macht. Ist eine Anmeldung nicht möglich, so kann dies an ungültigen Anmeldedaten oder der Authentizität der gespeicherten Daten liegen.

Eine weitere Stelle, wo die Authentizität geprüft wird, ist die Kommunikation zwischen der Oberfläche und dem Hintergrundserver. Die meiste Kommunikation erfolgt über eine WebSocket-Schnittstelle. Da dies einen festen Tunnel darstellt, wird hier die Authentizität beim Aufbau der WebSocket-Verbindung geprüft. Auch hier gilt: Dem Nutzer wird nicht vertraut. Sämtliche Anfragen werden geprüft, ob der Nutzer überhaupt befugt ist, die Anfragen zu machen. Die Anmeldung erfolgt über den gleichen Tunnel und stellt somit sicher, dass alles zusammengehört und sich kein Dritter einmischen kann.

Nicht jede Kommunikation zwischen Oberfläche und Hintergrundserver erfolgt über die WebSocket-Verbindung. Für den Zugriff auf einzelne Dateien und Up- oder Downloads gibt es eine REST-API. Hierfür gibt es kurzlebige Tokens, welche direkt mit einer WebSocket-Verbindung verknüpft sind und sich auch nur über diese erhalten lassen. Ohne diese Tokens wird die Anfrage nicht vertraut und die Anfrage wird nicht beantwortet.

Des Weiteren werden externe Anfragen von anderen Geräten in der Standardkonfiguration nicht vertraut. Daher ist der Hintergrundserver so eingestellt, dass nur Anfragen vom gleichen Gerät angenommen werden. Somit wird versucht, sicher zu stellen, dass der aktuelle Nutzer möglichst vor dem Gerät sitzt. Dies garantiert einem zwar nicht, dass kein Proxy genutzt wird, dafür reduziert es aber ein potenzielles Einfallstor für Angriffe.

3.1.5 Verbindlichkeit

Ein unzulässiges Abstreiten durchgeführter Handlungen ist nicht möglich. Sämtliche Aktionen werden durch den Nutzer induziert und werden auch nur von ihm akzeptiert. Sobald der Nutzer sich angemeldet und eine Datenbank geöffnet hat, ist er somit berechtigt, diese auch zu bearbeiten. Jede Aktion wie erstellen, bearbeiten oder löschen von Daten wird direkt durch den Nutzer ausgelöst. Die Anwendung macht nichts, ohne den Befehl des Nutzers.

Für kritische Aktionen wie Löschen von Daten sind entweder die Menüs so strukturiert, dass diese sehr übersichtlich sind, was gerade getan wird und der Nutzer dies bestätigen muss, oder es gibt Wiederherstellungsfunktionen.

Es gibt aber auch Aktionen, die indirekt durch den Nutzer ausgelöst werden. Dazu zählt in erster Linie die automatische Speicherung der Änderung von Einträgen. Dies verhindert Datenverlust und sorgt für eine bequemere Nutzung.

Eine zweite Aktion wäre die automatische Erstellung und Aktualisierung des Suchindexes. Dies ist notwendig, damit die Suche von Einträgen schnell vorangeht und der Nutzer nicht gezwungen ist, dies selbst nach jedem Bearbeitungsschritt durchzuführen. Dies geschieht aber nur nach Neuanlegen von neuen Einträgen oder der Speicherung von Bearbeitungen dieser.

3.1.6 Zurechenbarkeit

Eine durchgeführte Handlung lässt sich den Verantwortlichen jederzeit zuordnen. Da die Anwendung nur lokal auf dem Gerät des Forschers betrieben wird und auch jede Aktion auch nur von einem Nutzer ausgehen darf, lässt sich diese Frage jederzeit beantworten: vom Nutzer selbst.

3.1.7 Resilienz

Das System muss widerstandsfähig gegen Ausspähungen, irrtümliche oder mutwillige Störungen oder absichtlichen Schädigungen (Sabotage) sein. Alle Aktionen geschehen nur auf dem Gerät des Forschers und Störungen können daher nur vom Gerät selbst kommen. Von außen ist in der Standardkonfiguration kein Eingreifen möglich.

Das Ausspähen von Daten ist relativ schwierig, da die Daten nur verschlüsselt auf der Festplatte vorliegen. Doch können diese vom Bildschirm aufgezeichnet werden, wenn diese gerade entschlüsselt dem Forscher im Browser angezeigt werden. Genauso lässt sich nicht ausschließen, dass mit verschiedenen Proxys die Kommunikation zwischen Browser und Server ausgespäht wird. Dies ist auf der anderen Seite recht schwierig durchzuführen, da Server und Oberfläche prüfen, ob gleiche Ports genutzt werden.

Eine irrtümliche oder mutwillige Störung am gleichen Gerät lässt sich nicht ausschließen. So können Prozesse einfach beendet, Werte im Arbeitsspeicher verändert oder ausgelesen oder Daten auf der Festplatte verändert werden. Dies kann dazu führen, dass die Anwendung

abstürzt und die Datenbanken unbrauchbar werden. Nur mit Back-ups und Neustarts lässt sich dies wiederherstellen.

Außerdem ist die Anwendung nicht davor gewappnet, dass der Programmcode dekompiert und verändert wird. Mit einer veränderten Version der Anwendung können sämtliche Daten offengelegt oder neue Schwachstellen eingebaut werden. Eine Änderung der Anwendung könnte mit einer Prüfung der Signatur der Anwendung geprüft werden. Dies findet aktuell nicht statt, kann aber durch eine zukünftige Erweiterung hinzugefügt werden.

3.2 Datenschutz

Datenschutz ist in der europäischen Datenschutzgrundverordnung DSGVO (GDPR), den Landesdatenschutzgesetzen der einzelnen Bundesländer und den Datenschutzgesetzen der Staaten, in dem die betroffenen Bürger wohnen, gesetzlich geregelt. Der gesetzliche Umfang sprengt den Umfang dieser Arbeit bei Weitem, wodurch nur kurz auf die gesetzliche Lage zum Schutz vor Fremden und der Betroffenen genauer eingegangen wird.

Auf viele dieser Regelungen wird im Kapitel 3 nur grob eingegangen, da diese zudem Handlungsempfehlungen des BSI oder Grundsätze der IT haben.

3.2.1 Schutz vor Fremdzugriff

Die Daten befinden sich auf physischen Geräten (Laptop, Festplatte, USB-Stick, ...), welche mit dem Forscher weltweit mitgenommen werden. Dabei kann es sein, dass die Datenträger in fremde Hände gelangen können. Um hierbei die Daten selbst zu schützen, ist es zwingend erforderlich, die Daten so zu schützen, dass sie selbst mit vertretbarem Aufwand nicht les- oder manipulierbar sind.

In erster Linie hierzu werden hierzu die gespeicherten Dateien verschlüsselt und sind somit ohne ihren Schlüssel nicht mehr auszulesen. Zusätzlich wird noch ein Hashwert über die verschlüsselte Datei ermittelt, welcher es ermöglicht, Manipulationen an der Datei zu entdecken, aber nicht zu beheben.

Die Namen, Pfade, Schlüssel und Hashwerte der Dateien sind alles Metadaten, welche alle in einer Datenbank hinterlegt werden. Mithilfe dieser Informationen erhält die Anwendung (oder auch der Angreifer) Zugriff auf alle Daten, die in den Dateien gespeichert wurden. Ohne diese ist auch gleichzeitig kein Zugriff möglich. Damit die Datenbank selbst wiederum geschützt ist, wird diese verschlüsselt. Hierfür gibt es verschiedene Möglichkeiten (siehe 2.3.3). Damit existiert nur noch eine Stelle, wo ein Schlüssel notwendig ist, welcher alles andere freischaltet.

Zusätzlich zur Verschlüsselung der Dateien und der Datenbank ist es auch möglich, die komplette Festplatte (bzw. Partition) inklusive der Daten da drauf zu verschlüsseln. Dies geht unter Linux mit Luks und unter Windows mit BitLocker sehr gut. Das hat den Vorteil, dass ohne den Schlüssel für die Festplatte einen Zugriff auf die Datenbank oder Dateien nicht mehr möglich ist. Sobald die Festplatte aber geöffnet ist (Schlüssel wurde Luks, BitLocker, etc. übermittelt), dann sind alle Dateien darauf allen Prozessen vom Rechner transparent verfügbar, so als wären die nicht verschlüsselt gewesen.

Eine Verschlüsselung der Festplatte schützt somit nur vor Fremden, die von außen versuchen, auf das Gerät zuzugreifen. Andere Prozesse auf dem gleichen Gerät hätten nach wie vor Zugriff auf alle Daten, wenn diese nicht noch zusätzlich verschlüsselt wären.

Ein weiteres Problem stellt der verwendete Schlüssel dar, der für die Ent- und Verschlüsselung der Festplatte, der Dateien und der Datenbank genutzt wird. Wird immer wieder der gleiche Schlüssel verwendet, wird somit Fremden es erleichtert, diese einmal auszulesen und in Zukunft erneut für gleiche oder andere Datensätze einzugeben. Dies wird in der IT auch als Replay-Angriff bezeichnet. Eine Möglichkeit, dies zu umgehen, stellen Einmal-Passwörter (engl. One-Time-Pad) dar, bei der für jede Ent- und Verschlüsselung ein neuer, bisher nicht verwendeter Schlüssel genutzt wird. In der Regel wird versucht, dass aus der Historie bisheriger Schlüssel der nächste Schlüssel nicht abgeleitet werden kann.

Und schließlich stellt sich für die Anwendung die Frage, wann diese den Schlüssel erhält, um die benötigten Daten zu entschlüsseln. Dies könnte direkt beim Start der Anwendung über ein Argument oder Konfigurationsdatei geschehen. Das hätte aber zur Folge, dass für den kompletten Lebenszyklus der Anwendung der Schlüssel bekannt wäre. Bei einer Konfigurationsdatei sogar über diesen hinaus. Bei der Übergabe als Argument können sogar alle anderen Prozesse auf dem Rechner den Schlüssel sehen, wenn diese kurz in die Prozesstabelle reinschauen. Alternativ könnte die Anwendung zu einem beliebigen Zeitpunkt den Schlüssel erhalten und diesen auch nur für die einzelne Aufgabe oder Sitzung des Nutzers verwenden. Das hätte den Vorteil, dass der Schlüssel möglichst kurz bekannt ist und die Anwendung dennoch Zugriff auf die Daten erhält, wenn diese gerade benötigt werden.

Eine weitere wichtige Möglichkeit zum Schutz vor Fremdzugriff ist eine 2-Faktor-Authentifizierung. Hiermit wird zusätzlich zu einem Geheimnis, was in diesem Fall der Schlüssel für die Entschlüsselung sein kann, ein weiterer Faktor, z. B. Besitz abgefragt. Nur wenn der Nutzer den zweiten Faktor bereitstellt und dieser verifiziert werden kann, wird eine Anmeldung als erfolgreich angesehen und dem Nutzer die Daten bereitgestellt. Für den zweiten Faktor gibt es derzeit eine Fülle an Möglichkeiten. Ein paar Ausgewählte sind:

- Versand eines kurzlebigen Einmal-Codes per SMS an eine bekannte Nummer. Wird derzeit noch von PayPal, Google und früher für Online-Banking genutzt.
- Vorher generierte Liste an Einmal-Codes, welche ausgedruckt vorliegt. Wurde früher gern für Online-Banking genutzt. Die Martin-Luther-Universität Halle-Wittenberg nutzt dies noch heute für ihr Selbstverwaltungsportal.
- Versand eines kurzlebigen Einmal-Codes per E-Mail an eine bekannte Adresse. Wird derzeit von vielen System gern verwendet (u.A. Microsoft, Steam).
- Bereitstellen von kurzlebigen Einmal-Codes per Handy-App. Das bekannteste und verbreitetste hierzu ist der Google Authenticator, bei der beliebige Dienstleister (z. B. GitHub, Nintendo, Rockstar, Ubisoft, Discord, NVIDIA, ...) ihre Codes abfragen können. Viele Banken (z. B. Commerzbank, Postbank und Sparkasse) stellen hierzu eigene Apps bereit.
- Nutzung von Hardware-Tokens, die kryptografische Schlüssel austauschen und somit ihre Identität verifizieren. Dies gibt es in verschiedenen Formen, unter anderem SIM-Karten (z. B. Autorisierung gegenüber dem Provider), elektronischen Ausweisen (z. B. Personalausweis) und USB-Sticks (z. B. FIDO).

Generell gilt, jeder zweite Faktor ist besser als gar kein zweiter Faktor. Manche brauchen mehr Aufwand in der Bereitstellung, da extra Server und Dienstleister kontaktiert werden müssen und andere können direkt zwischen Nutzer und Anwendung geregelt werden. Außerdem bieten alle auch eine unterschiedliche Sicherheit anderen gegenüber. Bei E-Mails wird sich auf die Sicherheit des Übertragungsweges der Server und des Postfachs des Empfängers verlassen. Bei Handy-Apps auf den jeweiligen Dienstleister. Und bei

Hardwaretokens vor Manipulation der Hardware (was mit erhöhten Aufwand verbunden ist).

Für diese Anwendung wird als zweiter Faktor eine FIDO USB Key genutzt (siehe Kapitel 3.4). Dies hat den Vorteil, dass dies lokal am gleichen Rechner funktioniert, eine hohe Sicherheit hat und leicht zu benutzen ist.

3.2.2 Schutz der Betroffenen

In der Datenbank können Patienteninformationen oder persönliche Meinungen und Weltanschauungen vorhanden sein, welche nicht nachträglich mit dem Interviewten wieder verknüpft werden dürfen. Selbst für den Forscher dürfen diese Zusammenhänge nicht mehr nachträglich (alleinig über die Datenbank) gezogen werden. Dadurch wird auch das Datenbankschema maßgeblich beeinflusst.

Des Weiteren gibt es in den Daten mit erhöhtem Schutzbedarf, da diese Rückschlüsse auf die Identität der Person ermöglichen und somit der Schutz der Betroffenen nicht gewährleistet werden kann. Diese müssen anonymisiert werden können. Außerdem hat der Betroffene jederzeit das Recht, seine Daten löschen zu lassen. Dies gilt auch für anonymisierte Daten.

Von daher ist die Datenbank in zwei Teile aufgeteilt. Die eine enthält alle normalen Daten, welche für die Forschung relevant sind. Die andere enthält besonders schützenswerte Daten, die nach der Anonymisierung nicht mehr benötigt werden. Der zweite Teil, auch Confidential Database in dieser Arbeit genannt, soll zu jeder Zeit entfernt und in speziellen Archiven gesichert werden könne. Für den Forscher steht diese dann nicht mehr zur Verfügung. Wünscht der Betroffene eine Löschung, so kann die Confidential Database wieder zurückgespielt werden und die Daten lassen sich somit auffinden und löschen.

3.3 Technische Basis

Aufgrund von den Grundsätzen der IT-Sicherheit (siehe 3.1), und dem Datenschutz (siehe 3.2) lässt sich die technische Basis für die Sicherheit herleiten.

Der Forscher arbeitet mit hoch sensitiven Daten (Patientenakten, religiöse Einstellungen, persönliche Meinung, ...), welche den höchsten Schutz genießen und nicht in fremde Hände geraten oder missbraucht werden dürfen. Dies hat eine höhere Priorität als der Verlust der Daten an sich.

Daher werden die komplette Datenbank und die gespeicherten Dateien durch die Anwendung verschlüsselt und sind auch ohne den Schlüssel nicht entschlüsselbar. Es wird empfohlen, zusätzlich die Festplatte zu verschlüsseln. Dies ändert nichts an der Verschlüsselung der Daten selbst, dafür wurde aber eine zusätzliche Hürde vor dem Zugriff von außen eingeführt.

Des Weiteren muss sichergestellt werden, dass auch nur der Nutzer (in diesem Fall der Forscher) Zugriff auf seine Daten hat und auch sonst niemand anderes. Dafür übergibt der Nutzer beim Start der Sitzung den Schlüssel an die Anwendung, welcher direkt wieder weggeschmissen wird, sobald der Nutzer die Sitzung beendet. Zusätzlich muss der Nutzer vor dem Start der Sitzung einen zweiten Faktor für die Autorisierung bereitstellen. Hier wird ein Hardwaretoken verwendet. Das hat den Vorteil, dass sich nicht auf externe Dienstleister oder Infrastruktur verlassen werden muss, da alles lokal am Rechner geprüft wird.

Die Daten aus der Datenbank (und den gespeicherten Dateien) werden nur dann entschlüsselt, wenn dies auch vom Nutzer gewünscht oder indirekt gefordert wird. Diese sind dann

nur für den benötigten Zweck im Arbeitsspeicher bereitgehalten und werden direkt im Anschluss wieder gelöscht.

Daten können mit einem Forschungskollegen nur dann freigegeben werden, wenn dies explizit vom Forscher gewünscht wird. Ohne das ist das Einlesen der Daten nicht möglich. Insbesondere der Hardwaretoken verhindert den Zugriff über die gleichen Zugangsdaten von unterschiedlichen Standorten aus.

Damit der Zugriff zur Datenbank durch Verlust oder Beschädigung des Hardwaretokens oder das Vergessen des Passworts nicht verloren geht, wird im Vorfeld ein Masterpasswort für die Datenbank erzeugt. Dies allein reicht aus, um den Zugriff wiederherzustellen.

3.4 FIDO

Abbildung 1: FIDO2 USB Key von NitroKey



Ein FIDO2 USB Key vom deutschen Hersteller NitroKey. Dieser hat einen Touchsensor verbaut, um die Nutzerpräsenz zu prüfen. [33]

Ein wichtiger Teil in der Sicherheitsarchitektur nimmt die 2-Faktor-Authentifizierung ein, damit zusätzlich zum Wissen (Nutzername + Passwort) auch Besitz (Hardware) geprüft werden kann. Für dieses Projekt wurde sich für einen FIDO2 kompatiblen USB-Stick entschieden. Das ist ein kleiner Chip, welcher ein Kryptografie-Modul und einen Zertifikatsspeicher enthält. Dieser wird per USB an den Computer (oder Handy) angeschlossen und tauscht mit diesem Daten aus.

Der Computer kann Anfragen an den USB Key senden, damit bestimmte Datensätze von diesen signiert werden. Die privaten Schlüssel für die Signatur sind nur auf dem USB Key gespeichert und lassen sich nicht von außen auslesen.

Alle gängigen Webbrowser (Mozilla Firefox, Google Chrome, Safari, Chromium und Opera) unterstützen ein Protokoll namens WebAuthn, welches FIDO2 nutzt. Dies ist derzeit zwar

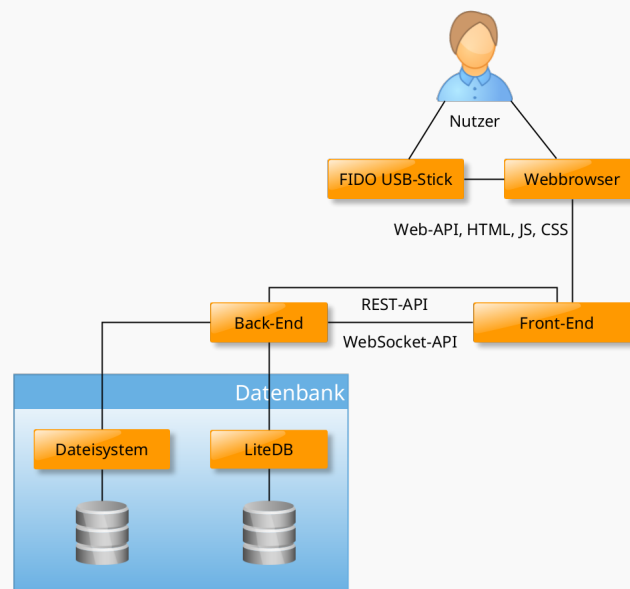
noch im Entwurfsstadium ([2]), findet aber mittlerweile bei immer mehr Webseiten Einsatz (z. B. alle von Google, Amazon, Microsoft, GitHub, GitLab; Quelle: [44]).

Dabei können Webseiten über den Browser nach einen Public Key fragen und sich Daten signieren lassen (für eine Anleitung siehe [14], für Demonstration siehe [15]). Darüber hinaus ist eine Registrierung und Anmeldung nur mit dem USB Key möglich, welche nicht abgegriffen oder ausgespäht werden kann.

4 Technisches System

Hier wird ein Überblick (siehe Abbildung 2) über das technische System geliefert, dazu zählen die einzelnen Komponenten, die Apis, die Datenbank und wie ein Anmeldeprozess aussieht.

Abbildung 2: Überblick über das technische System



Diese Grafik zeigt einen Überblick über das technische System. Dazu sind alle Module und deren Schnittstellen gekennzeichnet. Die Module sind Back-End (siehe Kapitel 4.1.2), Front-End (siehe Kapitel 4.1.1) und Datenbank (siehe Kapitel 4.4). Dazu wurden die internen API von WebSocket und REST in Kapitel 4.1.4 und den Anmeldeprozess über FIDO in Kapitel 4.3 behandelt.

4.1 Überblick

Die gesamte Anwendung ist in mehrere Module geteilt, welche für sich abgeschlossen und auch austauschbar sind. Sie sprechen über eine einfache API miteinander und lassen sich separat voneinander testen.

Hier wird ein lokaler HTTP Webserver genutzt, welcher nur Anfragen von localhost entgegennimmt, verarbeitet und die Antworten zurückliefert. Der Nutzer kann dann eine beliebige Anwendung (in den meisten Fällen ein moderner Webbrowser wie Firefox oder Chromium) nutzen und diesen Server ansprechen. In den folgenden Fällen wird von diesem Modul als Back-End oder auch Server gesprochen.

Hinter dem Webserver wird eine lokale verschlüsselte Datenbank genutzt, bei der die komplette Verwaltung im Prozess des Webserver eingebettet ist. Dazu wird die Open Source Bibliothek LiteDB genutzt, die sich um die komplette Verwaltung dazu kümmert.

Des Weiteren gibt es das Front-End, welches aus einer Webseite besteht, welche von einem beliebigen modernen Webbrowser dargestellt werden kann. Mit dieser Oberfläche wird der Nutzer hauptsächlich kommunizieren und von den Vorgängen im Hintergrund sollte

dieser eigentlich nichts mitbekommen. Im Folgenden wird vom Front-End auch von der Oberfläche oder auch UI gesprochen.

4.1.1 Front-End (UI)

Für das Front-End wurde eine moderne HTML-Oberfläche gewählt. Diese hat den Vorteil, dass sich diese auch später ohne großen Aufwand auf andere Plattformen oder Systeme übertragen lässt. (Webbrowser sind fast überall verfügbar.) Außerdem hat sich das Web mittlerweile so weit entwickelt, dass viele Office Tätigkeiten sich auch heute schon komplett im Browser erledigen lassen (z. B. Dokumente schreiben, E-Mails lesen, einfache Videobearbeitung, ...) und auf Spezialanwendungen auf dem Rechner verzichtet.

Als Programmiersprache für die UI hat der Autor die Sprache Elm gewählt (für den Vergleich siehe Kapitel 2.3.1). Das Styling wird durch handgeschriebenes CSS gemacht. Hier wird kein Framework genutzt.

4.1.2 Back-End (Server)

Der Server ist eine kleine C# Anwendung, welche sich um alles Wichtige im Hintergrund kümmert. Sie nimmt alle Anfragen von der Oberfläche entgegen und informiert diese über Änderungen. Dann kümmert dieser sich um die Verwaltung der Datenbanken und der verschlüsselten Dateien. Hier ist der komplette Sicherheitsaspekt gelagert.

4.1.3 Datenbank

Auf die Datenbank wird im Kapitel 4.4 genauer eingegangen.

4.1.4 Interne APIs

All diese Module werden über verschiedenen Apis zusammengehalten und darüber wird auch kommuniziert.

Der Server und die UI kommunizieren hauptsächlich über eine einzelne WebSocket-Verbindung (siehe RFC 6455 [1]). Das hat den Vorteil, dass die Authentifizierung nur einmal am Anfang erledigt werden muss und danach kann sich gegenseitig vertraut werden, solange die Verbindung nicht abbricht (z. B. wenn der Nutzer die Seite im Browser neu lädt). Außerdem können jederzeit Nachrichten vom Server zur UI und auch anders herum sendet werden und so schneller auf neue Ereignisse reagieren.

Für Datei-Up- und Downloads wird zusätzlich eine kleine REST-API genutzt, damit zum einen hierfür die Verbindungskapazität der WebSocket-Verbindung nicht ausgelastet wird und zum anderen die Einbettung in die Oberfläche einfacher geschieht.

Der Server und die Datenbank kommunizieren über eine Open-Source-Bibliothek, welche im Prozess des Servers angesiedelt ist. Über die API der Bibliothek wird dann die Datenbank verwaltet. Es findet keine Inter-Process-Kommunikation statt - alle Daten sind sofort beim Server verfügbar und können nicht mit einfachen Mitteln ausgespäht werden.

4.2 Externe Apis

Um den Zugang der Daten zu anderen Anwendungen zu ermöglichen, soll die Anwendung Schnittstellen bereitstellen. Die einfachste Form hierzu ist der Export der gesicherten

Dokumente, welche im sicheren Speicher hinterlegt wurden. Nachdem diese exportiert (heruntergeladen) wurden, können diese in einem anderen Programm betrachtet werden.

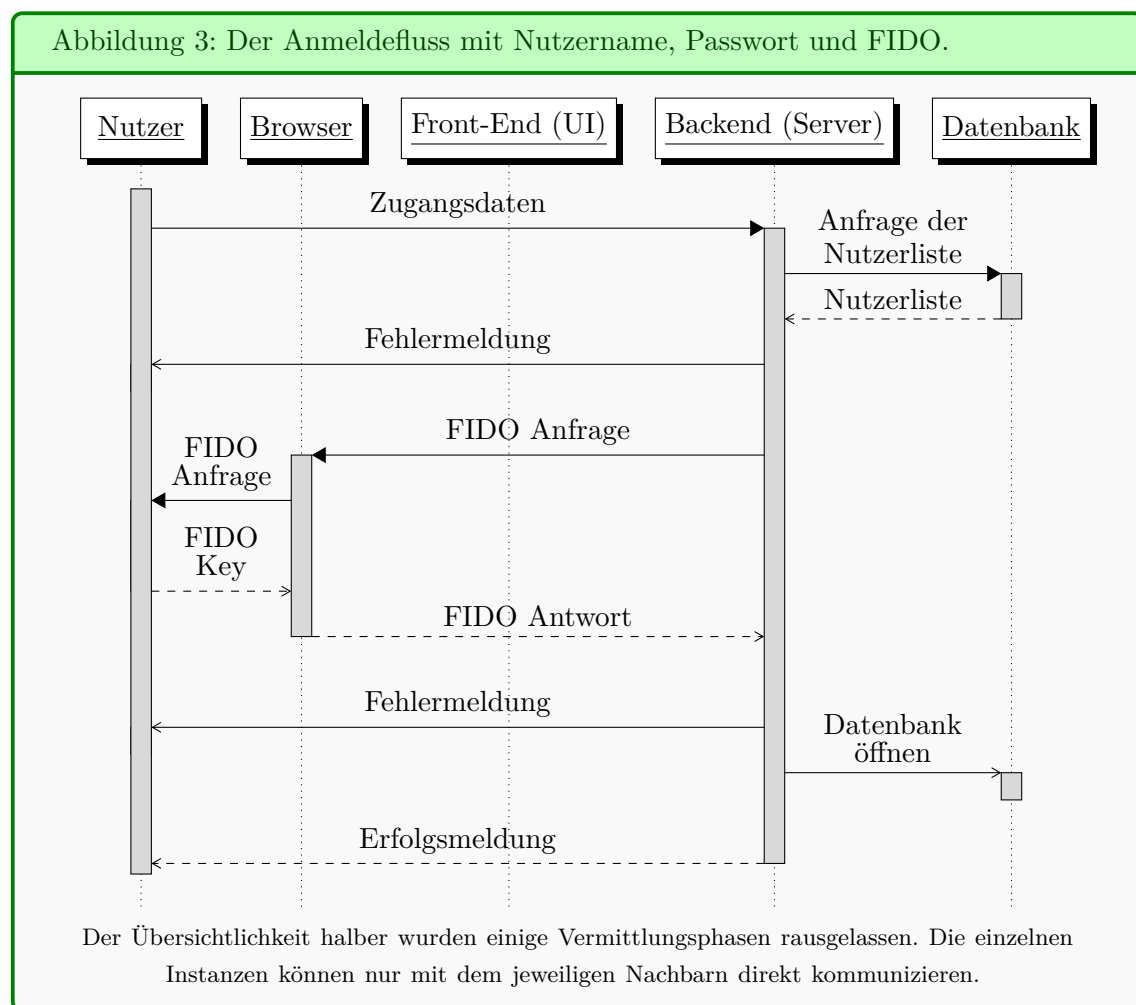
Genauso funktioniert der Prozess für den Import von Daten aus anderen Programmen in die Anwendung hinein. Hier übernimmt die Anwendung nur die Aufgabe eines sicheren Speichers, in dessen die Daten vor Manipulation von außen sicher sind.

Für die Daten in den Eingabefeldern gibt es bisher nur die Möglichkeit, die aktuelle Seite als PDF über den Browser zu exportieren. Mehr Möglichkeiten sind hierzu als Erweiterungen (siehe 8.2) geplant.

4.3 Anmeldung

Die zu speichernden Daten haben einen sehr hohen Schutzbedarf und müssen dementsprechend verschlüsselt gespeichert und übertragen werden und brauchen eine Zugriffskontrolle. Das BSI verlangt hierfür eine Zwei-Faktor-Authentifizierung.

Für die Anwendung wurde eine Zwei-Faktor-Authentifizierung ausgewählt, welche auf Wissen (Passwort) und Besitz (FIDO-Key) basiert. Die Authentisierung erfolgt in folgenden Schritten (vergleiche Abbildung 3):



1. Der Nutzer öffnet die Oberfläche in seinem Browser und wird nach Benutzernamen und Passwort gefragt.

2. Der Server prüft, ob eine Datenbank diesen Nutzer hinterlegt hat. Wenn nein gibt es eine Fehlermeldung und die Authentifizierung werden abgebrochen.
3. Dann wird geprüft, ob der Wert von `SHA256(Passwort + Salt)` mit dem gespeicherten Wert übereinstimmt. Der Salt ist ein zufälliger Wert, welcher bei der Erstellung der Datenbank angelegt wurde. Falls es hier ein Fehler gab, wird dies angezeigt.
4. Die Oberfläche fragt über die WebAuthn Schnittstelle des Browsers (ist in jeden modernen Browser implementiert) nach dem FIDO Key. Das ist ein kleiner spezieller USB-Stick, welcher eingesteckt werden muss.
5. Der FIDO Key bekommt 1024 zufällige Bytes vom Server und soll diesen mit seinen lokalen privaten Key signieren.
6. Der Browser liefert die Signatur an die Oberfläche und diese an den Server.
7. Die Signatur wird mit dem gespeicherten Public Key geprüft. Wenn nicht gibt es wieder eine Fehlermeldung und ein anderer FIDO-Key wird verlangt.
8. Die Datenbank wird geöffnet.

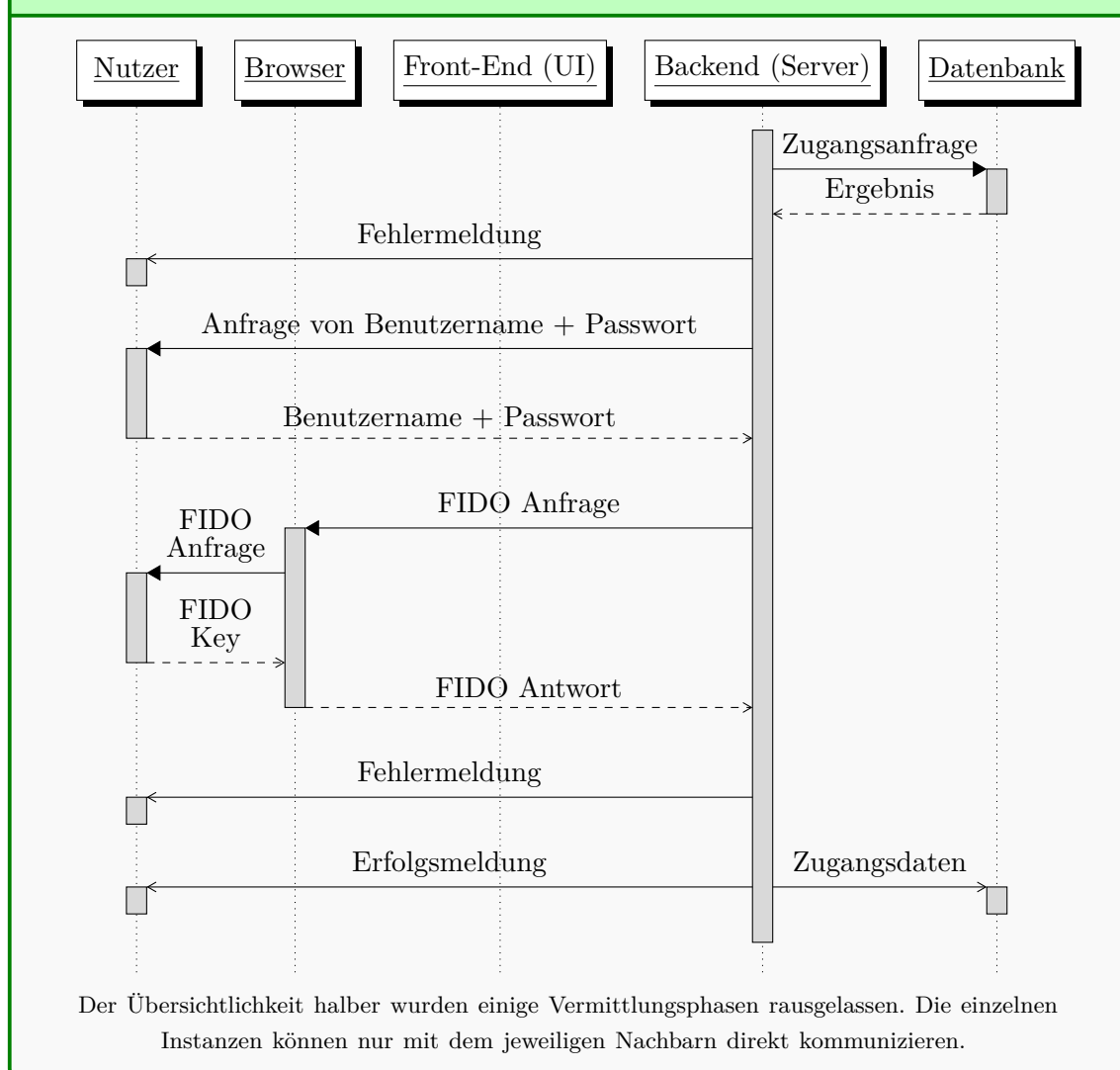
Es können in einer Anwendung mehrere Datenbanken hinterlegt werden, bei der der Nutzer für jede Datenbank ein anderes Passwort oder FIDO-Key nutzen kann. Am Anfang wird mit jeder Datenbank verglichen und nach und nach werden die noch gültige Datenbank ausgesiebt, welche noch damit angemeldet werden können. Sobald zu einem Zeitpunkt keine Datenbank mehr möglich ist, so wird dies als Fehler ausgegeben. Am Ende können mehrere Datenbanken gleichzeitig authentifiziert werden (sofern Nutzernamen, Passwort und FIDO bei allen gleich sind). Datenbanken, welche gerade nicht geöffnet werden konnten, können auch noch nachträglich geöffnet werden. Dazu wird der Anmeldeprozess wiederholt und schon offene Datenbanken ignoriert.

Das Neuanlegen einer Anmeldemöglichkeit (z. B. bei Neuerzeugung einer Datenbank oder Hinzufügen eines weiteren Nutzers) werden folgende Schritte abgehandelt (vergleiche Abbildung 4):

1. Zuerst wird geprüft, ob Zugang überhaupt besteht. Bei neuen Datenbanken ist dies implizit. Bei bestehenden muss der Nutzer sich erneut anmelden, da der Server den Entschlüsselungs-Key nicht permanent im RAM hält.
2. Der Nutzer muss einen Benutzernamen und Passwort angeben und bestätigen.
3. Nutzer wird von der Oberfläche nach einem FIDO-Key gefragt.
4. Es wird der Public-Key und eine Prüfung abgefragt.
5. Der Server prüft das. Bei Misserfolg wird dies angezeigt.
6. Die Prüfsummen für die Anmeldung werden erzeugt und bei der Datenbank parallel hinterlegt.
7. Datenbank wird verbunden, sofern noch nicht geschehen.

Des Weiteren wird bei der Anmeldung nicht der eigentliche Key für die Datenbank erzeugt. Stattdessen wird für jede Anmeldemöglichkeit der eigentliche Key für die Datenbank separat verschlüsselt und ist nur mit dem gesalzenen Passwort aus der Anmeldung entschlüsselbar. Dadurch ist es auch relativ einfach möglich, mehreren Nutzern Zugang zur gleichen Datenbank zu geben, ihnen zu erlauben, ihre Passwörter zu ändern oder den Zugang wiederherzustellen, falls der mal verloren gegangen ist.

Abbildung 4: Erstellung neuer Datenbankzugangsdaten



4.4 Datenbank

Die Datenbank umfasst verschiedene Arten von Daten. Darunter zählen die Einstellungen, Zugangsberechtigungen, die Dateien, die eingegebenen Daten und die Metadaten des Forschers. Dadurch ist diese auch relativ groß und komplex. In den folgenden Unterkapiteln wird genauer auf das DBMS LiteDB, die Herleitung des Schemas, die Speicherung von Daten und die Arbeit mit diesen eingegangen.

4.4.1 LiteDB

LiteDB ist eine OpenSource ([23]) NoSQL Datenbank, welche als eingebettete Datenbank für eine Dotnet (u.a. auch C#) Anwendung fungiert. Diese ist komplett in C# geschrieben ([22]) und bietet eine große Palette an Funktionen und Anbindungen für Dotnet.

LiteDB speichert seine Daten in einem BSON (Binary JSON) Format. Dieses ist an JSON angelehnt und soll die Verarbeitung erleichtern. LiteDB nutzt nur ein Subset der vom offiziellen BSON Schema [36] unterstützten Datentypen (siehe [20]). Das ist hauptsächlich aus dem Grund, damit sich die Arbeit mit den Erweiterungen, die BSON unterstützt,


```

    {
        Filename = "der Pfad zu der Datenbankdatei",
        // das Passwort, falls eins gesetzt wurde. Andernfalls einfach
        // null.
        Password = "pa$$w0rd",
    }
};
// Nun kann über "Database" direkt auf alle Informationen der Datenbank
// zugegriffen werden.

```

Um Daten auszulesen, wird dann eine Collection von der Datenbank abgefragt. Dies geht auch allgemein ohne C# Typinformationen und der Entwickler erhält die BSON Rohdaten. Für die Entwicklung ist es aber praktischer, dies direkt in Objekte überführt zu bekommen. Hier wird ein einfaches Beispiel genutzt. Ausführliches dazu gibt es im Quellcode der Arbeit in `server/Dacryptero/DB/DBSingleController.cs`.

```

// Beispielklasse für die Daten. Diese wird genutzt, um das Schema für
// eine Collection zu definieren. LiteDB nutzt Reflection, um alle
// Parameter und Typen auszulesen und auszuwerten und versucht dann
// die Daten von BSON in Person oder anders herum zu übertragen.
// Als Programmierer gibt es dazu nichts extra zu beachten.
public class Person
{
    // Id der Person. ObjectId wird von LiteDB bereitgestellt und ist
    // eine 12 Byte große Zahl.
    public ObjectId Id { get; set; }
    // Ein weiteres Feld. In diesem Fall Name. Es können beliebig
    // weitere Felder, Listen oder auch verschachtelte Typen genutzt
    // werden.
    public string Name { get; set; }
}

// Abrufen der Collection der Datenbank. Dazu wird ein C# Typ und der
// Name der Collection übergeben. Falls die Collection noch nicht
// existiert, so wird diese angelegt. Der C# Typ sagt LiteDB, in
// welchen Schema alle Daten dieser Collection dargestellt werden
// sollen. Um das Umwandeln kümmert sich LiteDB selbst. Falls die
// Roh-BSON Daten verlangt werden, so kann der Typ weggelassen werden
// und es wird eine Collection von BsonDocument zurückgegeben.
var people = Database.GetCollection<Person>("people");

// === Hinzufügen der Person ===
// Hier wird zuerst die Person nur mit dem Namen angelegt. Der Name
// wird explizit gesetzt. Die Id wird auf den Standardwert gelassen.
var person = new Person { Name = "Max Mustermann" };
// Die neue Person wird zur Collection hinzugefügt. Um das Umwandeln
// kümmert sich LiteDB selbst. Nach dem Aufruf hat LiteDB automatisch
// den Wert von Id gesetzt.
people.Insert(person);

```

```
// Finden aller Personen dessen Name mit Max anfangen.
var peopleWithMax = people.Find(x => x.Name.StartsWith("Max"));

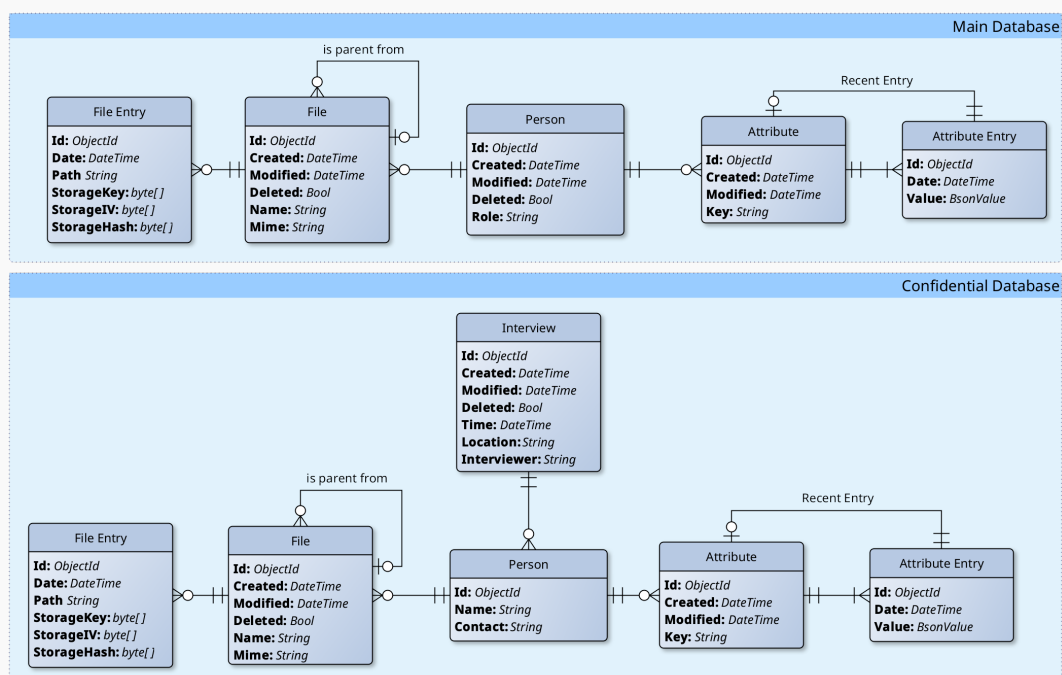
// Finden der ersten Person anhand der Id
var person2 = people.FindById(person.Id);
```

Wie an den Beispielen sehr leicht erkenntlich ist, ist die Nutzung der Datenbank recht leicht und die Abfragen können direkt im Nutzercode gemacht werden. Das Zusammenbauen einer Abfrage in textueller Form wie SQL ist nicht notwendig. Für komplexere Aufgaben gibt es weitere Funktionen, die in der Dokumentation [25] nachzulesen sind.

4.4.2 Datenbankschema

Das Erstellen des Datenbankschemas stellte sich als schwierig heraus. Das größte Problem war, dass zuerst unklar war, was die Auftraggeber erwarten und welche Daten diese benötigen. Dabei entstanden verschiedene Iterationen des Datenbankschemas. Im späteren Verlauf haben sich Autor und Auftraggeber darauf geeinigt, das Datenbankschema allgemeingültig für verschiedene Forschungszwecke zu machen und dann über ein separates Schema dies zu konfigurieren und einzuschränken (siehe 4.4.3).

Abbildung 6: Entity Relationship Diagram



Diese Abbildung gibt es noch einmal im Anhang A als große Grafik.

Dies ist ein Entity Relationship Diagram in der Krähenfuß-Notation (siehe [51]) oder auch Martin-Notation ([55]). Die Krähenfüße geben die Kardinalitäten der Beziehungen an. So ist in diesem Beispiel ein File mit 0 – n FileEntry und ein FileEntry mit 1 File verbunden. Ein Attribute ist mit 1 – n AttributeEntry und über Recent Entry ist ein AttributeEntry mit 0 – 1 Attribute verbunden.

Was sofort am Schema auffällt, ist die Aufteilung in verschiedene Bereiche. Es gibt hier die

Main Database und die Confidential Database. Die Aufteilung der beiden ergibt sich aus den Anforderungen siehe 3.2.2. Beide enthalten zusammen die Datensätze, die der Forscher im Laufe der Forschung eingibt. Diese Datensätze sind je nach Priorität entweder in der Confidential Database oder in der Main Database. Die Anwendung braucht auf jeden Fall die Main Database, um mit den Daten zu arbeiten. Die Confidential Database kann zu einem beliebigen Zeitpunkt entfernt oder wieder hinzugefügt werden.

Zentrale Objekte in der Datenbank ist die **Person**, **Interview**, **File** und **Attribute**, welche alle in Beziehung zueinanderstehen. Alle vier Objekttypen finden sich in beiden Datenbanken wieder. Einzig **Interview** ist nur in der Confidential Datenbank enthalten. Von **Person** gibt es immer zwei Varianten, welche jeweils in der Main Database und in der Confidential Database enthalten sind. Beide Varianten sind über die gleiche Id verbunden.

File und **Attribute** sind als Objekte nur in einen von beiden Datenbanken enthalten, je nachdem, ob sie derzeit confidential deklariert wurden oder nicht. Jeweils von **File** und von **Attribute** wird eine Historie angelegt, welche sich auch im Datenbankschema widerspiegelt. Somit ist der Bearbeitungsverlauf der Daten immer ersichtlich.

Das Verhalten und die Nutzung von **Attribute** ist in Kapitel 4.4.3 näher erläutert.

Die Objekte von **File** enthalten nur die Metainformationen zu den Dateien. Die Inhalte selbst werden parallel zu den Datenbankdateien verschlüsselt gespeichert. Der Schlüssel für jede Datei ist einzigartig und für jede neu generiert. Diese werden alle in die Datenbank mitgespeichert.

Zu dem oben genannten Schema wurden dann C# Klassen erstellt, die dem Schema entsprechen. Diese sind im Quellcode im Ordner `/server/Dacrypto/Data` zu finden. LiteDB selbst kümmert sich mittels Reflection automatisch um die Übersetzung zwischen der internen BSON Repräsentation und den Daten in den C# Klassen (siehe Beispiel in Kapitel 4.4.1). Mehr Informationen dazu, wie das in LiteDB funktioniert, findet sich hier [24].

4.4.3 Schemadateien

Schemadateien sind ein Konzept, welches zusätzlich eingeführt wurde, um die Daten in der Datenbank genauer zu spezifizieren und an die Bedürfnisse des Forschers und dessen Projekt anzupassen. Hierbei wird das Datenbankschema nicht verändert. Die Datenbank speichert seine Daten weiterhin im sehr allgemeinen Format. In der Schemadatei wird eine Liste von Rollen angegeben, die eine befragte Person haben kann. Zu jeder Rolle wird zusätzlich eine Liste von Attributen spezifiziert und angegeben, welchen Typ diese haben und wie diese verwaltet oder bearbeitet werden sollen.

Alle Schemadateien sind JSON Dateien und befinden sich in einem vom Nutzer konfigurierten Ordner. In diesem können sie in einem beliebigen Unterordner befinden. Alle JSON Dateien darin werden von der Anwendung als Schemadateien betrachtet. Bei der Namensgebung der Pfade haben das Institut und der Nutzer freie Wahl. Einzig `/internal/**/*.json` wird für interne Testzwecke für die Zukunft reserviert.

Der Aufbau der Schemadatei wird im Anhang D genauer erklärt. Jede Schemadatei enthält eine Liste von Rollen mit Attributen, die von oben nach unten ausgewertet werden. Jede Person in der Datenbank (das ist der Datensatz zu einer befragten realen Person), welche vom Forscher in der Anwendung angelegt wird, entspricht genau einer dieser Rollen, welche derzeit nicht nachträglich geändert werden kann.

Falls mehrere Rollen gleiche Attribute enthalten, kann eine neue Rolle (Eltern-Rolle) angelegt werden, welche die gleichen Attribute enthält, und alle Rollen erben dann von der neuen Rolle. Dadurch übernehmen alle Kinder-Rollen (das sind die Rollen, die von der Eltern-Rolle erben), alle Attribute der Eltern-Rolle. Jede Rolle kann nur von einer anderen Rolle direkt erben, aber eine Rolle kann von einer Rolle erben, die schon von einer anderen Rolle erbt.

Eine Rolle kann nur von einer anderen Rolle erben, die im Schema vorher definiert wurde. Dadurch wird das Problem mit der zyklischen Vererbung umgangen. Falls die Eltern-Rolle nicht vom Forscher direkt genutzt werden soll, dann empfiehlt es sich, diese Eltern-Rolle als abstrakt zu markieren.

Jede Rolle hat eine Liste von Attributen. Ein Attribut ist eine Eigenschaft, die der Nutzer bei der Person einstellen kann. Diese bekommt exakt den Namen, der im Schema als Schlüssel definiert wurde. Als Typ lässt sich hier die Art des Editors bestimmen, welche wiederum auch den Wertetyp definiert (siehe Tabelle 6). Eine genauere Einschränkung für den Editor gibt es derzeit nicht.

Tabelle 6: Editortypen

Editortyp	Wertetyp	Beschreibung
DateTime	string , <date-time>	Angabe von Datum und Zeit. Angezeigt wird in lokaler Zeitzone des Anwenders. Gespeichert in UTC.
SingleLine	string	einzeiliger Text
MultiLine	string	mehrzeiliger Text
Number	number	Fließkommazahl
Int	int	Ganzzahl
Bool	bool	Checkbox mit Ja, Nein

Alle Editortypen für Attribute, die von der Oberfläche unterstützt werden.

Weiterhin lässt sich zu jedem Attribut sagen, ob dies protected ist, also in der Confidential Datenbank gespeichert wird. Diese Einstellung ist durch das Schema vorgegeben und lässt sich nicht im Nachhinein ändern. Sobald die Confidential Datenbank entfernt wurde, kann der Wert nicht mehr eingesehen werden, aber auch eine Bearbeitung ist nicht mehr möglich.

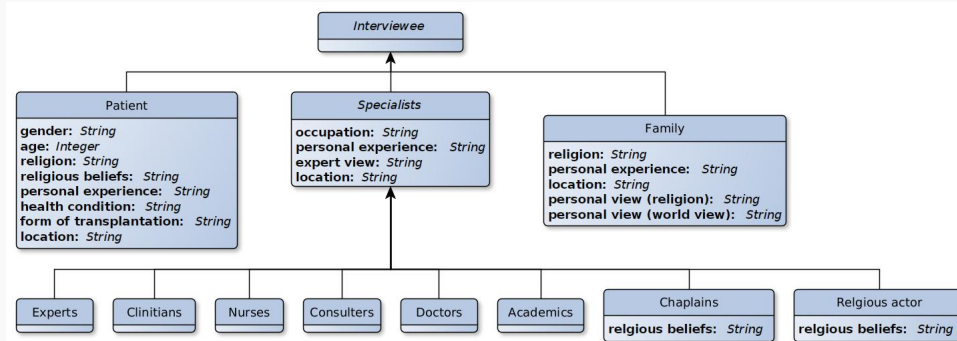
Außerdem lässt sich für jedes Attribut festlegen, ob es eine Historie anlegen soll. Falls diese Option aktiviert ist, wird jeder historische Zustand in der Datenbank abgespeichert und lässt sich durch den Nutzer ansehen. Ist die Option deaktiviert, so ist immer nur der aktuelle Wert zu sehen und eine Bearbeitung ist nicht möglich.

In Abbildung 7 wird das Rollenschema, welches für das Forschungsthema des Auftraggebers erstellt wurde, dargestellt. Hier ist deutlich zu erkennen, dass je nach Rolle unterschiedliche Informationen abgefragt und gespeichert werden.

4.4.4 Schlüsselverwaltung

Die Schlüssel für die Entschlüsselung der Datenbankdatei befindet sich im Datenbankordner in der `config.json` Datei. Hier sind alle Informationen enthalten, die benötigt werden, um Nutzer zu autorisieren und authentifizieren. Die Datei nach dem Schema im Kapitel C (Anhang) aufgebaut.

Abbildung 7: Rollenschema für das Projekt



Dies ist eine grafische Visualisierung wie das Rollenschema für das Forschungsthema des Auftraggebers aussieht. In kursiv sind die Namen von abstrakten Rollen gekennzeichnet. Die Pfeile geben an, von welcher Rolle diese ihre Attribute erben. Bei den Attributen wurde nur der Wertetyp angegeben. Die Schemadatei ist im Quellcode unter `/server/Dacrypto/schemas/eth/dev/v1.json` zu finden.

Die Datei enthält einen Hash vom MasterKey, damit immer nachgeschaut werden kann, ob der aktuell eingegebene MasterKey der Richtige sein könnte, bevor dieser direkt an der Datenbank angewandt wird.

Dann ist da eine Liste an Nutzerzugängen aufgelistet. Jeder Nutzer kann beliebig viele Zugänge hinterlegt haben. Diese können sich in Benutzernamen, Passwort oder Fido gleichen oder unterscheiden. Das macht für die Anwendung keinen Unterschied.

Zu jedem Passwort wird der gesalzene Hash hinterlegt. Gesalzene Hashes werden generiert, indem zu dem Passwort ein zufällig generierter Hash angehängen wird und dann zusammen gehasht wird. In dieser Anwendung wird der Prozess 10.000-mal wiederholt. Der Prozess des gesalzenen Hashens hat den Vorteil, dass es deutlich erschwert wird, mithilfe von den Hashes die Passwörter zu knacken (siehe [8]).

Zusätzlich dazu werden Informationen zum genutzten Fido-Key hinterlegt. Das Format dieser Werte ist durch die verwendete Fido-Bibliothek vorbestimmt und wird durch die Anwendung nur gespeichert und weitergereicht. Diese Daten werden genutzt, um den FIDO USB-Stick zu authentifizieren und zu validieren.

Zum Schluss gibt es noch das verschlüsselte Datenbankpasswort, welches durch das Nutzerpasswort und einem Salt entschlüsselt werden kann. Das entschlüsselte Datenbankpasswort entspricht dem MasterKey, wird aber im späteren Verlauf durch die Anwendung nicht mehr bereitgestellt oder angezeigt.

Es ist mithilfe des Datenbankpassworts möglich, neue Zugänge in die JSON Datei einzutragen. Existierende Einträge können jederzeit durch den Nutzer entfernt werden. Es ist technisch nicht nötig, das Passwort hierzu zu wissen, da die JSON Datei einfach bearbeitet werden kann. Für die Anwendung wäre es dann so, als ob es die Zugangsdaten nie gegeben hätte.

Wenn die Datei vom Nutzer in anderer Art verändert wird (Hinzufügen von nicht validen Einträgen oder Löschen von validen), dann ist es möglich, dass der Zugang zur Datenbank verloren geht. Die Anwendung kann damit umgehen, wenn an einer beliebigen Stelle die

Authentifizierung fehlschlägt und meldet dies auch dem Nutzer.

Falls die Datei verloren gegangen ist, dann lässt sich der Zugang nur über den MasterKey wiederherstellen, da dieser das eigentliche Datenbankpasswort ist.

4.4.5 Dateisystem

Die Anwendung speichert verschiedene Dateien im Dateisystem für die Datenbanken. Für die Datenbanken gibt es einen vom Nutzer konfigurierten Haupt-Ordner. In diesen werden alle Datenbanken gespeichert. Für jede Datenbank gibt es hierfür einen eigenen Unterordner. Der Namen des Unterordners darf nur aus Buchstaben von **a** bis **z**, Ziffern, Bindestrich (-) oder Unterstrich (_) bestehen, zudem dürfen sich zwei Datenbanken nicht den gleichen Ordner teilen und die Unterordner dürfen nicht verschaltet sein.

In dem Datenbankordner gibt es dann eine Liste von Dateien und Ordnern, die von der Anwendung genutzt werden:

- **config.json**: Die Konfiguration der Datenbank. Genauere Informationen dazu im Kapitel 4.4.4.
- **config.json.backup**: Wird vor der Aktualisierung von **config.json** von der Anwendung automatisch angelegt, um Fehler zu vermeiden.
- **confidential.db**: Die LiteDB Datei zur Confidential Datenbank
- **confidential-log.db**: Wird von LiteDB automatisch für **confidential.db** angelegt.
- **confidential.index.db**: Der LiteDB Index zur Confidential Datenbank
- **confidential.index-log.db**: Wird von LiteDB automatisch für **confidential.index.db** angelegt.
- **data.db**: Die LiteDB Datei zur Main Datenbank
- **data-log.db**: Wird von LiteDB automatisch für **data.db** angelegt.
- **data.index.db**: Der LiteDB Index zur Main Datenbank
- **data.index-log.db**: Wird von LiteDB automatisch für **data.index.db** angelegt.
- **files/**: Die gespeicherten verschlüsselten Dateien. Mehr siehe unten
- **upload/**: Die Dateien, die gerade vom Nutzer zum Server hochgeladen werden.

Zu den LiteDB-Dateien gibt es immer jeweils ein **-log.db** Datei. Diese wird automatisch vom System angelegt und dient zur Wiederherstellung ungesicherter Daten. LiteDB sichert zuerst alle Änderungen in diese Log-Datei und schreibt nach einer gewissen Zeit diese dann in die eigentliche Datenbank rein. Dies geschieht alles automatisch, ohne dass der Entwickler eingreifen muss. Wenn Sicherungen angelegt werden, so sind die Logdateien auch immer mitzusichern, da diese noch ungesicherte Daten enthalten können.

Des Weiteren gibt es zur Main und Confidential Datenbank jeweils einen Index. Dieser kann jederzeit vom Nutzer gelöscht werden. Die Anwendung legt diesen dann wieder neu an, indem die komplette Datenbank neu indiziert wird. Dies können je nach Größe der Datenbank und Rechenleistung einige Minuten bis eine Stunde dauern.

Wenn die Confidential Datenbank entfernt werden soll, so reicht es einfach aus den Dateien **confidential.db** und **confidential-log.db** zu entfernen (Anwendung muss dabei neugestartet werden). Die Anwendung kann dann problemlos damit weiterarbeiten. Ein einfaches Rücksichern ist möglich, indem diese Dateien jederzeit wieder hinzugefügt werden.

Wenn Dateien vom Nutzer hochgeladen werden, dann landen diese zuerst im Ordner **upload/**. Dazu wird ein zufälliger Schlüssel generiert und mittels AES in Echtzeit ver-

schlüsselt. Die Daten sind also zu jeder Zeit verschlüsselt auf der Festplatte, auch wenn die Übertragung nicht vollständig ist. Als Dateiname wird Hex-Wert einer zufälligen 12 Byte großen Zahl gewählt. Fall der Upload abbricht, wird einfach diese Datei gelöscht.

Sobald der Upload vollständig ist, wird die Datei in `files/` verschoben. Dafür wird zuerst der SHA512 Hashwert der verschlüsselten Datei ermittelt. Als Pfad wird der Hex-Wert des SHA512 Hash-Werts genutzt, bei der die ersten beiden Bytes einen Unterordner und die nächsten beiden Bytes einen Unterunterordner bilden. Zum Beispiel: `files/0D48/60D6/FA4F66CCB0C0D35C9FEAC8B...` (der Pfad wurde gekürzt dargestellt). Die Wahrscheinlichkeit für eine Kollision ist hier äußerst gering. SHA512 kann $1,3 \cdot 10^{154}$ verschiedene Zahlen abbilden (zum Vergleich, es gibt ca. 10^{80} Atome im beobachtbaren Universum [54]). Und selbst für den äußerst unwahrscheinlichen Fall gibt es ein Fallback: Es wird an den Dateinamen ein Bindestrich ("-") und eine dezimale Zahl beginnend bei 1 angefügt, falls es zu einer Kollision kommt.

Nach dem Verschieben werden die Metainformationen in die Datenbank eingetragen und der Oberfläche mitgeteilt.

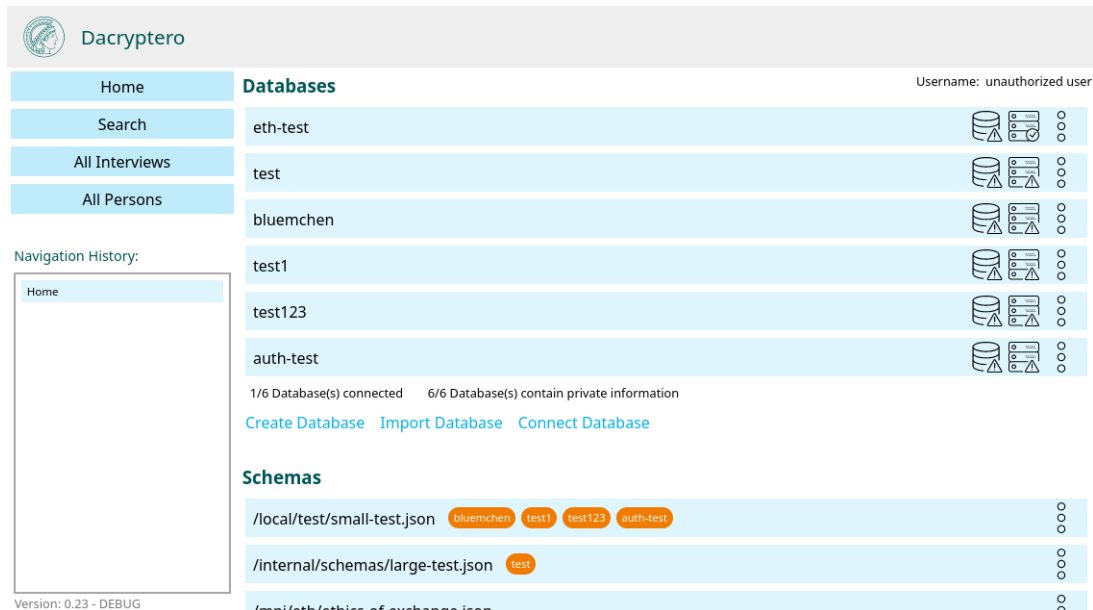
Die Dateien in `files/` werden nicht entfernt oder exportiert, wenn die Confidential Datenbank entfernt wird. Diese werden einfach von der Anwendung nicht mehr erkannt und können nicht gelesen werden, da der Schlüssel fehlt. Für den Nutzer oder externe ist also der Inhalt der Dateien nicht mehr erkenntlich. Einzig über die Dateigröße ließen sich Rückschlüsse ziehen. Dies wurde aber mit dem Betreuer und dem Auftraggeber besprochen und dies soll nicht geändert werden.

Theoretisch ist es möglich, Dateien aus `files/` heraus zu löschen. Dies wird zwar nicht empfohlen, aber die Anwendung erkennt dies und zeigt auch an, dass die Datei nicht mehr verfügbar ist. Es würde nur für das Szenario, bei der der Nutzer alte Dateien aus der Historie entfernt haben möchte, Sinn ergeben. Für diesen Fall ist derzeit kein Support in der Anwendung eingebaut.

5 Umsetzung

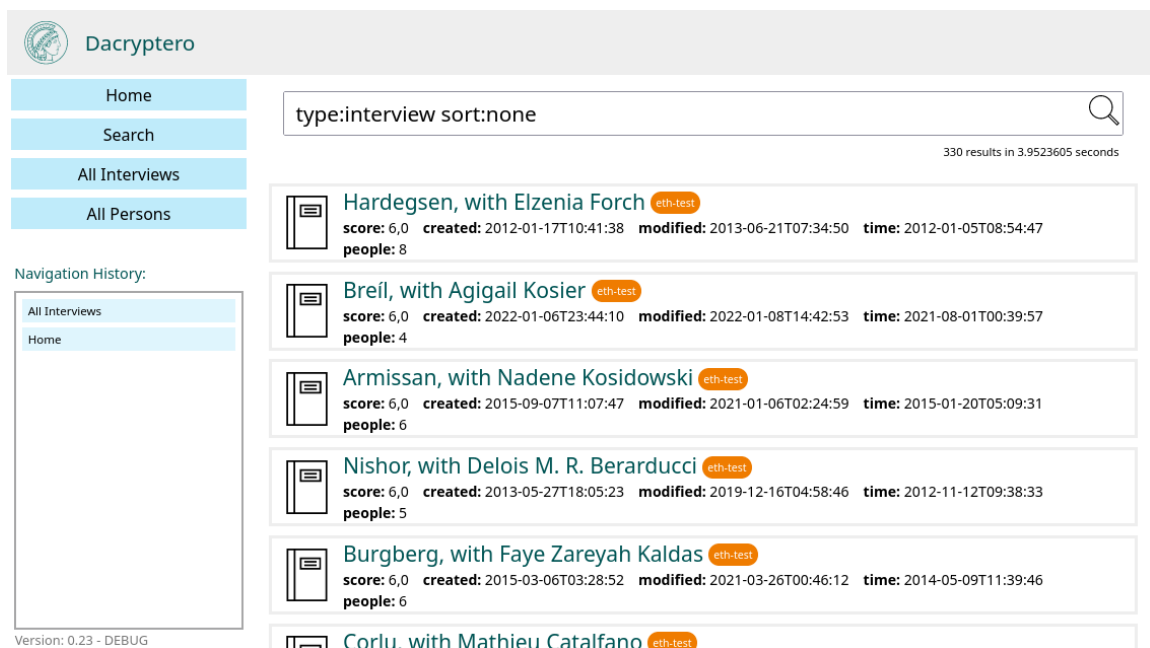
5.1 Bildschirmfotos

Hier werden ein paar Bildschirmfotos von der Weboberfläche der Anwendung gezeigt.



Dieses Bild zeigt die Startseite der Anwendung. Hier sind schon einige Datenbanken und Schemas eingetragen. Diese wurden alle nur zu Testzwecken hinzugefügt und haben keine Realdaten.

Hier ist auch die Aufteilung der Oberfläche erkenntlich. Auf der linken Seite ist die Navigation mit einer Sprungliste der zuletzt besuchten Seiten. Im rechten Hauptteil ist je nach Oberfläche der Hauptinhalt zu sehen.



Hier wird eine Suche gezeigt, bei der noch die Ergebnisse ermittelt werden.

The screenshot shows the Dacrypto application interface. On the left is a navigation menu with 'Home', 'Search', 'All Interviews', and 'All Persons'. Below it is a 'Navigation History' section. The main area displays an 'Interview' form for ID #61e13fc9d29032132f89db2f. The form includes fields for 'created' (2012-01-17), 'modified' (2013-06-21), 'interviewer' (Elzenia Forch), and 'location' (Hardeggen). A 'time' section shows a calendar for January 2012 with the 5th highlighted, and a 'Local Time in Europe/Berlin' display showing 'Thu 5 Jan 2012 08:54'. A 'People' section is partially visible at the bottom.


Version: 0.23 - DEBUG

Dies zeigt eine Ansicht eines Interviews.

The screenshot shows the Dacrypto application with a modal dialog titled 'Add Person to Interview #61e13fc9d29032132f89db2f'. The dialog prompts the user to 'Select a role for the person' and lists various roles: Academic, Chaplain, Clinician, Consulter, Doctor, Expert, Family, Nurse, Patient, and Religious Actor. The 'Chaplain' role is selected, and its details are shown on the right: 'expert view: MultiLine', 'location: SingleLine', 'occupation: SingleLine', 'personal experience: MultiLine', and 'religious beliefs: MultiLine'. An 'Add Chaplain' button is at the bottom of the dialog. In the background, the 'People' section shows two entries: 'Academic' and 'Religious Actor'.

Version: 0.23 - DEBUG

Hier wird eine neue Person zu einem Interview hinzugefügt. Dabei wird eine Liste der Rollen angezeigt, welche für die Datenbank zur Verfügung stehen.


Dacrypto

[Home](#)
[Search](#)
[All Interviews](#)
[All Persons](#)

Academic #61e13fd5d29032132f8a0f0c eth-test


created 2020-02-09
modified 2021-12-06
interview [Open](#)
name
contact

Attributes
expert view

Navigation History:
 Person: 61e13fd5d29032132f8a0f0c
 Interview: 61e13fc9d29032132f89...
 All Interviews
 Home

Version: 0.23 - DEBUG

Hier wird eine Person mit ein paar Eingaben zu dieser gezeigt.


Dacrypto

[Home](#)
[Search](#)
[All Interviews](#)
[All Persons](#)

religion

Files

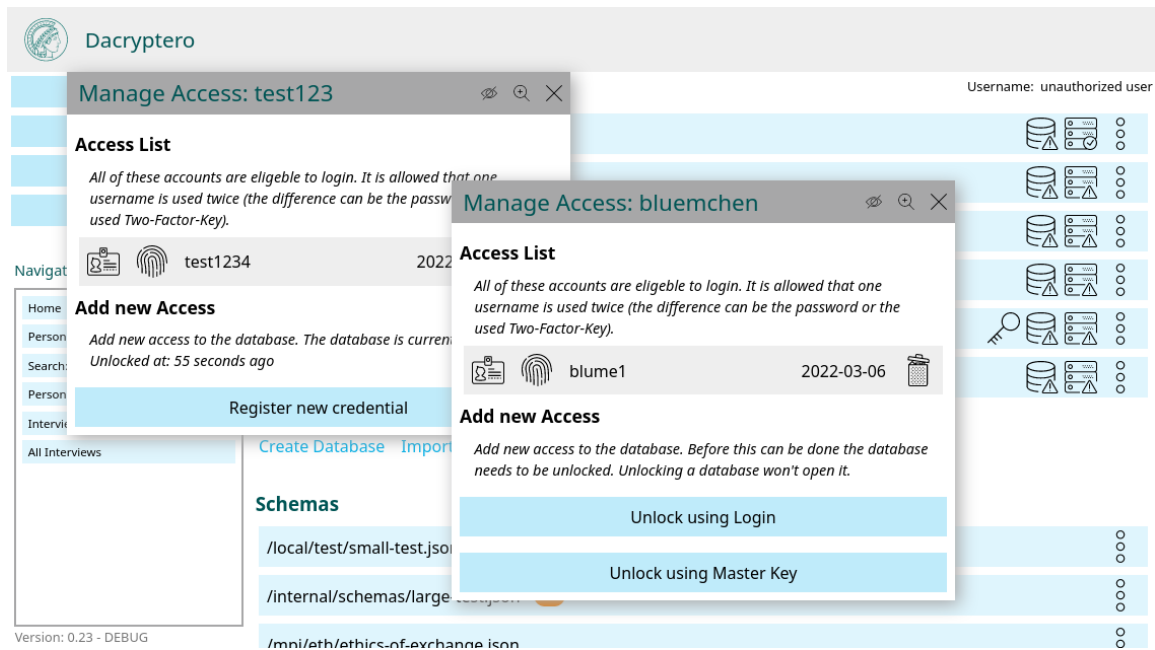
	2022-02-04 New Folder	2022-02-04	
	2022-02-05 New Folder	2022-02-05	
	CKQwXQQHodZkIBZwIGUBFtd.jpg	2022-02-04	
	ABC.jpg	2022-02-04	
	aiEhcDemUNbmXygtixSawjjj.jpg	2022-02-04	
	2022-02-06 New Folder	2022-02-06	

[Add folder to root](#) [Upload file to root](#)

Navigation History:
 Person: 61e13fcad29032132f89df17
 Search: type:file
 Person: 61e13fd5d29032132f8a0f0c
 Interview: 61e13fc9d29032132f89...
 All Interviews
 Home

Version: 0.23 - DEBUG

Dies ist eine Liste von Dateien, die mit der einen Person verknüpft sind.



Das Bild zeigt die Zugriffssteuerung einer Datenbank. Hier können Zugänge für eine Datenbank hinterlegt, bearbeitet oder gelöscht werden. Außerdem lässt sich hier auch der Zugang zu einer Datenbank mit einem Master Key wiederherstellen.



Login into your Account
Database: bluemchen

Username

Password

Continue

Das Bild zeigt die Anmeldung. In diesem Fall soll eine bestimmte Datenbank freigeschaltet werden.

5.2 Hürden und Herausforderungen

Auch bei diesem Projekt gab es bei der Umsetzung ein paar Stolpersteine, auf die in den folgenden Unterkapiteln genauer eingegangen wird.

5.2.1 WebAuthn

WebAuthn ist ein relativ neuer Standard. So neu, dass es zwar schon in jeden modernen Browser unterstützt wird, es aber derzeit keine offizielle Spezifikation gibt (nur Entwürfe). Des Weiteren ist diese jetzt auch nicht so verbreitet, dass der Entwickler sofort auch die nötige Technik parat hat, um das zu testen.

So konnte der Autor sich am Anfang nur auf das eigene Mobilgerät verlassen, da der eigene Fingerabdrucksensor als Hardwaretoken genutzt wird. Für die Umsetzung auf den Laptop wurden FIDO-USB-Sticks bestellt, da zum einen nicht jeder Laptop einen Fingerabdrucksensor hat und zum anderen der Sicherheitstoken als eigenständige physische Komponente genutzt werden soll.

Sobald die bestellten Hardwaretokens angekommen waren, ging es an die Implementierung der Schnittstelle. Hier war das größte Problem, dass es nur wenige Beispiele und eine ausführliche, aber leicht verwirrende Spezifikation online verfügbar ist. Ein weiteres Problem war die schier große Menge an Funktionen und Variabilität an Schlüsseln, die WebAuthn bereitstellt. Nicht alles wird von allen Tokens unterstützt und es ist schwierig herauszufinden, was benötigt wird und was nicht. Schwierig wird es aber erst recht, wenn sämtliche Möglichkeiten der unterstützten Schlüsselalgorithmen berücksichtigen werden sollen (z. B. ES256, EdDSA, HMAC in unterschiedlichen Varianten, AES in unterschiedlichen Varianten, ...). Und dann gibt es eine Authentifizierung (siehe [3]), welche 24 Schritten beinhaltet.

Einen Großteil dieser Schwierigkeiten können verschiedene Bibliotheken (in diesem Projekt wurde `fido2-net-lib` [4] genutzt) übernehmen, welche aber alle wiederum eigene Schnittstellen und Schwierigkeiten haben.

5.2.2 Tests beim Nutzer

Es ist immer gut, schon frühzeitig Versionen den zukünftigen Nutzern zu zeigen, damit Feedback schnell an den Entwickler gelangt. Dies wurde auch in dieser Arbeit versucht. Doch leider konnte durch zeittechnische Schwierigkeiten seitens Nutzers und Autors nicht genauer auf Probleme eingegangen werden.

6 Tests

Hier wird auf die Tests genauer eingegangen, die bei der Entwicklung der Anwendung durchgeführt wurden. Aufgrund der Größe und des Umfangs des Projektes und gleichzeitig dem knappen Zeitrahmen wurde auf viele Tests verzichtet. Vieles wurde manuell getestet und es wurden so gut wie keine automatischen Tests vorgenommen. Dafür wurde bei der Entwicklung darauf geachtet, das alles so zu entwickeln, dass ein Testen möglichst leicht ist und möglichst viele Fehler ausgeschlossen werden.

Es ist nicht auszuschließen, dass das derzeitige Produkt noch Fehler enthält. In der aktuellen Version läuft dies aber zuverlässig auf sämtlichen Testgeräten ohne Abstürze oder Datenverlust.

6.1 Automatisierte Tests

Ein großer Vorteil an den automatisierten Tests ist, dass die ohne menschliches Zutun gestartet, durchgeführt und ausgewertet werden können. Dadurch lassen diese sich gut in den Entwicklungsprozess einbinden, da diese regelmäßig mit den neuesten Änderungen am Code ausgeführt werden. Das hat zur Folge, dass Probleme am Code relativ frühzeitig erkannt und somit auch behoben werden können.

Je nachdem, ob nun das Front-End, Back-End oder die API testen werden sollen, gibt es unterschiedliche Testarten, die sich mehr oder weniger gut dafür eignen. Aus zeitlichen Gründen wurde bei vielen darauf verzichtet, diese im Projekt umzusetzen. Stattdessen wurden die manuell vom Entwickler durchgeführt. Daher wird nur auf die Testarten genauer eingegangen, die auch ihre Anwendung gefunden haben.

6.1.1 Kompilierung

Dies ist ein relativ einfacher Test, da nur geschaut wird, ob der Compiler syntaktische Fehler im Quellcode findet. Zum Teil kann der Compiler noch auf andere Fehlerquellen wie zum Beispiel Typfehler untersuchen. In der Ausführung wird der Compiler auf dem Quellcode gestartet und geschaut, ob es Fehler oder Warnungen gibt.

Die Compiler von den verwendeten Programmiersprachen C# und Elm sind sehr gut im Finden vieler Fehler und geben hilfreiche Fehlermeldungen aus. Übrig bleiben hauptsächlich logische Fehler, die sich dann manuell oder mit anderen Testarten testen lassen.

Bei diesem Projekt wurden alles korrigiert, was der Compiler als Fehler oder Warnung gemeldet hat.

6.1.2 GitLab CI Tests

GitLab bietet verschiedene automatische Tests an, die mit wenigen Zeilen zur CI Pipeline hinzugefügt werden können. Genutzt wurden dazu folgende Tests:

- **Static Application Security Testing (SAST)** (Quelle: [12])

Der Code wird statisch nach bekannten Schwachstellen geprüft. Dazu gibt es eine große Liste an Programmiersprachen und Frameworks, die unterstützt und automatisch erkannt werden.

- **Infrastructure as Code (IaC) Scanning** (Quelle: [10])

Der Infrastruktur Code, z. B. für Docker-Container, wird auf Schwachstellen überprüft. Dies ähnelt dem SAST Test. In diesem Projekt wird kaum mit Docker-Containern gearbeitet, von daher hatte dieser Test kaum einen Effekt.

- **Dependency Scanning** (Quelle: [9])

Überprüft die Abhängigkeiten der Projekte, ob für diese Schwachstellen bekannt sind. Auch hier werden unterschiedliche Programmiersprachen und Frameworks unterstützt.

- **Secret Detection** (Quelle: [11])

Durchsucht den Quellcode, ob Passwörter, Schlüssel, Api-Tokens oder andere sensitive Informationen enthalten sind. Dies kann bei einem Entwickler durch Zufall passieren und gleichzeitig die Infrastruktur gefährden, wenn diese Informationen immer gültig sind.

Diese Tests liefen bei jedem Durchlauf der CI Pipeline mit und konnten somit schnell Probleme aufzeigen. Das ist äußerst praktisch, da dies dem Entwickler dabei hilft, sicheren Quellcode zu schreiben.

Einige dieser Tests benötigen eine bestimmte Lizenz von GitLab. Zum Start der Entwicklung hatte der Provider der GitLab Instanz (GWDG) noch all seinen Nutzern eine Ultimate-Lizenz bereitgestellt, wodurch alle Funktionen verfügbar waren. Im Laufe der Entwicklung wurde diese auf eine Community-Lizenz umgestellt (siehe [19]), wodurch einige Tests (in diesem Fall “Dependency Scanning”) nicht mehr zur Verfügung standen. Dies hat natürlich auch Einfluss auf die zukünftige Entwicklung, da Tests, die bisher genutzt wurden, von nun an nicht mehr funktionieren.

6.2 Nutzungsdaten

Der Forscher wird im Laufe seiner Arbeit die Anwendung mit Daten füllen. Dabei wachsen die Datenbank und die Menge der zu verwaltenden Dateien. Ziel ist es, dass die Anwendung auch nach einer langfristigen Arbeit noch gefühlt genauso schnell arbeitet wie zum Anfang auch.

Um die Last der Nutzungsdaten zu testen, wurde eine einheitliche Testumgebung und Grenzwerte für die Zeiten definiert. Als Testumgebung wurde ein 10 Jahre alter Laptop mit 4 Kernen, 8 GB RAM und 256 GB SSD festgelegt. Für alle Tests wurde immer wieder die gleiche Umgebung gewählt. Die Datenbank wurde mit Daten gefüllt und dann wurden verschiedene Suchanfragen gestellt oder durch die Daten navigiert. Der Vorteil an dieser beschränkten Umgebung ist, dass die verwendeten Laptops der Forscher alle neuer und leistungstärker sind, wodurch auszugehen ist, dass diese es leichter haben werden, mit der Menge an Daten umzugehen.

Für die Grenzwerte bei den Zeiten wurde definiert, dass eine einfache Navigation nie länger als 1 Sekunde dauern darf. Bei einer Suchanfrage müssen schon nach maximal 3 Sekunden erste Ergebnisse zu sehen sein. Nach 10 Sekunden ist die Suche beendet. Ist der gewählte Suchausdruck komplexer, dann sind 60 Sekunden erlaubt. Das Öffnen der aggregierten Ansicht von Einträgen muss nach 3 Sekunden fertig sein. Die Oberfläche muss flüssig auf Nutzereingaben reagieren. Diese Schwellwerte wurden dahingehend festgelegt, dass diese zum einen für einen Nutzer vertretbar sind und zum anderen ein ungestörtes Arbeiten ermöglichen.

Nachdem die Umgebung und die Grenzwerte definiert sind, geht es darum festzustellen,

wie viele Daten ein Forscher überhaupt anlegen wird. Dazu wurden die Forscher aus der Testgruppe befragt, was sie sich vorstellen könnten und es wurden alte Projekte angesehen, um eine gute Abschätzung zu erhalten.

Tabelle 7: Größe der Testdatenbank

Kategorie	Erzeugte Datenbank	Erwartete Realwerte	Kommentar
Anzahl von Interviews	1000	ca. 10-15	
Anzahl von Personen	5000	ca. 50	
Anzahl an genutzten Rollen	2	ca. 5-10	dies hat keine Auswirkung auf die Suchperformance
Anzahl an Attributen pro Rolle	7 und 182	ca. 10-15	jeweils zu ca. 50% genutzt
Anzahl an Attributen	ca. 472.000	ca. 625	
Länge der Texte	ca. 2,5 KB	ca. 50 KB	Für die Suche wurden kürzere Texte mit mehr Attributen gewählt
Anzahl der Einträge in der Historie	ca. 5	ca. 50	Historie wird für die Suche ignoriert
Speicher	ca. 2,3 GB	ca. 650 MB	

Für die Testfälle wurden dann diese Zahlen großzügig multipliziert (siehe Tabelle 7), um eine deutlich größere Datenbank zu erhalten. Für die Textgenerierung wurden Markov-Ketten von diversen Wikipedia-Artikeln genutzt. Dadurch werden einer natürlichen Sprache ähnliche Texte erzeugt, die beliebig lang sein können, aber keine Bedeutung haben. Die Texte wurden mit Absicht kürzer gewählt als in den erwarteten Werten, da die Textgenerierung über Markov-Ketten recht lange braucht (in der aktuellen Konfiguration schon 5-10 Minuten für die komplette Datenbank). Die resultierende Datenbank ist trotzdem groß genug.

Dabei stellte sich heraus, dass der anfängliche naive Suchalgorithmus sehr langsam ist. Es werden 30 bis 120 Sekunden für Suchanfragen benötigt. Bei dem naiven Suchalgorithmus wurden alle Einträge aus der Datenbank einzeln ausgelesen, mit dem Suchquery abgeglichen und dann weitergereicht. Sobald alle Einträge überprüft wurden, wurde das an die Oberfläche weitergereicht. Auch das Abrufen der aggregierten Seiten ist unverhältnismäßig lang mit 5-10 Sekunden.

Danach wurden mehrere Optimierungen an den Algorithmus vorgenommen, die aber aus zeitlichen Gründen nicht einzeln auf ihre Effektivität überprüft wurden. Stattdessen wurde jede Optimierung beibehalten und wirkte somit auch auf die weiteren Optimierungen aus.

Zuerst wurden die Verknüpfungen von Objekten nun auf beiden Seiten hinterlegt. Vorher wurde eine 1-n Verknüpfung so abgebildet, dass beim n-Element nur die ID des 1-Elements

hinterlegt wurde, anders herum nicht. Das bedeutete also, wenn alle Verknüpfungen des 1-Elements abrufen werden sollen, musste die komplette Datenbank durchsucht werden. Nun ist zusätzlich beim 1-Element eine Liste der IDs hinterlegt. Das erhöht den Synchronisierungsaufwand, dafür sind Beziehungen schneller verfügbar. Außerdem wurden verschiedene Elemente (Attribute, Attributshistorie, Einträge von Dateien) aus den jeweiligen Elternelementen ausgegliedert und erhielten ihre jeweils eigenen Collections. Das erhöht auch wieder den Verwaltungsaufwand, da mehr Objekte verwaltet werden müssen.

Diese Änderungen hatten zur Folge, dass sich an der Größe der Datenbank nicht wirklich etwas geändert hat. Dafür sind die Abfragen für aggregierte Ansichten auf unter 200 ms gesunken. An der Suchperformance hat dies nicht viel geändert.

Als Nächstes wurde ein Such-Index (nicht zu verwechseln mit dem Index, den LiteDB bereitstellt), aufgebaut. Dazu werden alle aktuellen Texte (die aus der Historie werden derzeit ignoriert) in Tokens aufgespalten und umgewandelt. Ein Token ist eine Folge von Kleinbuchstaben und Zahlen. Großbuchstaben werden in Kleinbuchstaben umgewandelt. Akzente und Sonderzeichen werden entfernt. Der Index enthält dann zu jedem Token den jeweiligen Fundort. Beim Fundort werden nur die ID und Art des Eintrags berücksichtigt. Jeder Suchstring wird auch in die entsprechenden Tokens umgewandelt und dann wird für jeden Suchtoken herausgesucht, welche Einträge infrage kommen. Die Mengen an Einträgen für jedes Suchtoken werden dann mengentheoretisch zusammengefasst. Heraus kommt eine Liste an in Frage kommenden Einträgen.

Da der Index unter Umständen auch vertrauenswürdige Daten enthält, wird für die Confidential und die normale Datenbank jeweils ein eigener Index angelegt.

Jeder Token kann wieder eine Menge an kürzeren Tokens enthalten, indem vom Anfang und Ende eine beliebige Menge an Zeichen entfernt wird. Dies ermöglicht die Suche nach Teilwörtern, ohne das ganze Wort zu kennen. Experimentell hat sich herausgestellt, dass es unpraktisch ist, als minimale Länge eines Tokens 1 zu nehmen. Hierbei ist der Index auf die 10-fache Größe der Datenbank angewachsen und das noch bevor ein Zehntel der Datenbank gelesen wurde. Stattdessen wurde als minimale Länge 3 genommen, da dies ein guter Vergleich zwischen Größe des Index und der Datenbank ist (2,3 GB Datenbank und 1,0 GB Index).

Der Einsatz eines Index hatte nun zur Folge, dass bei Suchanfragen, die Schlüsselwörter genutzt haben, nun eine Antwort in Sekundenbruchteilen zu sehen ist. Falls allgemeinere Sachen benötigt werden, so dauert eine Suche immer noch genauso lang.

Bis zu diesem Zeitpunkt wurden die Ergebnisse einer Suche auf dem Server zurückgehalten, um sie dann zu sortieren und im Anschluss an die Oberfläche weiterzureichen. Diese wurde damit behoben, dass sämtliche Ergebnisse, sobald sie verfügbar sind, nun direkt mit ein paar Hinweisen zur Sortierung an die Oberfläche weitergereicht werden. Die Oberfläche sortiert dann selbstständig die Ergebnisse und ordnet sie schon der Menge bekannter Ergebnisse ein. Dies hat zur Folge, dass erste Ergebnisse schnell zu sehen sind, die aber mit der Zeit weiter verbessert werden können.

Nach diesen Umstrukturierungen und Anpassungen haben sich Suche und die Anzeige aggregierter Ansichten stark verbessert. Zum Schluss hin konnten alle zeitlichen Grenzen auf der Testumgebung erreicht werden. Es gibt Ideen, die Suche noch weiter zu verbessern, welche all in zukünftigen Erweiterungen (siehe 8.2.4) kommen können.

7 Rollout

Dies ist der Weg, um die Anwendung vom Entwicklungsstadium bis zum Endnutzer zu bringen. Dies beinhaltet auf der einen Seite die Installation beim Nutzer an sich und zum anderen der Weg, den eine Änderung bei der Anwendung (ein neues Feature, eine Fehlerkorrektur, ...) macht, um dann beim Nutzer anzukommen.

7.1 Installation

Dies sind die Schritte, die notwendig sind, damit das Produkt (die Anwendung) auf dem Rechner des Nutzers läuft. Dafür gibt es verschiedene Methoden, die auch im Laufe der Entwicklung für diese Arbeit durchgelaufen sind. Vom Prinzip her bauen diese aufeinander auf und nehmen immer mehr manuelle Arbeit ab.

7.1.1 Manuelle Installation

Am Anfang der Entwicklung wurde alles manuell installiert. Dies hat den Vorteil, dass der Entwickler direkt sehen kann, was wie und wo benötigt wird. Außerdem erleichtert dies die Konfiguration selbst. Es ist von Vorteil, sich diese Schritte irgendwie zu notieren, da dies für die spätere Automatisierung benötigt wird.

Bei diesem Produkt bedeutete dies, dass folgende Produkte installieren bzw. Schritte durchgeführt werden müssen:

1. Herunterladen des Quellcodes in einen beliebigen temporären Ordner
2. Installation des Elm Compilers
3. Kompilieren des Elm Codes
4. Installation von Javascript Komprimierungswerkzeugen
5. Komprimierung des Javascript Codes
6. Installation von .NET SDK
7. Kompilieren des Server C# Codes
8. Kompilieren von Server Tools und Ausführung dieser
9. Anlegen der Programmverzeichnisstruktur auf dem Zielrechner
10. Kopieren der kompilierten Server- und Javascript-Dateien in die Programmverzeichnisstruktur
11. Kopieren der statischen Inhalte für die Web-Oberfläche in die Programmverzeichnisstruktur
12. Anlegen der Konfigurationsdatei
13. Anlegen der Verknüpfung zum starten der Anwendung

Diese Schritte sind vom Prinzip her unter Windows und Linux gleich, auch wenn diese sich im Detail leicht unterscheiden (z. B. Installationsort des Programms).

7.1.2 Halbautomatische Installation mit Docker und CI Pipeline

Einige Schritte aus der manuellen Installation, welche sich vereinfachen lassen, werden schon im Vorfeld kompiliert, um sie dann fertig auf den Zielrechner runterzuladen. Dazu eignet sich eine CI-Pipeline, so wie sie auch in dieser Arbeit genutzt wurde. Das ist ein spezielles Script, welches von einem Server gestartet wird, wenn ein Entwickler neuen Code in die Codeverwaltung (in diesem Fall GitLab, geht, aber auch mit anderen wie GitHub) hochlädt.

Der Server startet dann verschiedene Dockercontainer, was in sich abgeschlossene und konsistente Umgebungen sind, und führt darin vordefinierte Befehle aus. Das Ziel von Dockercontainern ist, dass immer die gleichen Bedingungen (installierte Software, Konfiguration, etc.) herrschen und daher genau ersichtlich ist, was genau getan werden muss.

Die Befehle der Schritte 1 bis 8 aus 7.1.1 werden zusammengefasst, und dadurch fallen diese Schritte auch bei der Installation beim Nutzer weg, da das Ergebnis schon fertig auf dem Server existiert. Dafür werden diese 8 Schritte beim Nutzer durch den Download der fertig gebauten Sachen und Installation von .NET Runtime (schmalere Version von .NET SDK) ersetzt. Auf dem Server kommt noch hinzu, dass alle notwendigen Dateien noch einmal zusammengefasst werden, damit sie besser für die Installation geeignet sind.

Einen weiteren Vorteil hat diese Vorgehensweise auch. So ist relativ früh erkenntlich, ob es Probleme beim Kompilieren und Zusammenstellen gibt und das, bevor die Installation beim Nutzer durchgeführt wird. Außerdem lässt sich auf dem Server noch automatische Tests ausführen (siehe 6.1) und die Versionierung erleichtern.

7.1.3 Vollautomatische Installation mit Wix (Windows)

An Automatisierung fehlen nur noch die letzten Schritte 9 bis 13 aus 7.1.1. Unter Windows eignet sich das von Microsoft veröffentlichte Softwaretool Wix. Hiermit wird eine XML-Datei angelegt, die alle Anweisungen enthält, die für die Installation notwendig sind. Danach gibt es einen Compiler, der die XML-Datei mit Anweisungen und alle zu installierenden Dateien einliest, zusammenpackt und eine ausführbare EXE- oder MSI-Datei erstellt.

Diese Schritte lassen sich auch automatisch auf dem Server in einen Dockercontainer ausführen, sodass am Ende nur noch die EXE- oder MSI-Datei übrig bleibt. Daher lässt sich die Installationsroutine am Nutzer so zusammenfassen:

1. Installer herunterladen
2. Installer starten und abwarten. Eventuell Konfiguration vornehmen
3. Fertig

Dies wurde für diese Arbeit nicht fertiggestellt und ist daher ein guter Punkt für zukünftige Erweiterungen.

7.1.4 Vollautomatische Installation unter Linux

Genauso wie sich die Installation am Nutzer bei Windows zusammenfassen lässt, geht dies auch unter Linux nur mit anderen Mitteln. Unter Linux gibt es eine große Palette an Werkzeugen, da je nach Linux Distribution einige Sachen anders funktionieren. So ist z. B. die Paketverwaltung (wird benötigt, um Abhängigkeiten zu installieren) bei einem Debian-Linux `apt` und bei einem Arch-Linux `pacman`, welche natürlich jeweils andere Formate sehen wollen.

Als Entwickler lässt sich dies vereinfachen, indem dieser sich ein Shellskript schreibt, was alle Installationsanweisungen enthält und dieses im Detail nachschaut, unter welcher Distribution es sich derzeit befindet.

Dies bedeutet natürlich aber auch viel Arbeit und das wurde aus Zeit- und Prioritätsgründen nicht vom Autor praktisch umgesetzt.

7.2 Stages

Von der Entwicklung des Codes bis zum Nutzer durchlaufen Änderungen an der Codebasis verschiedene Stages (Stadien). Üblicherweise wird hier mit einem Modell gearbeitet, was drei (Entwicklung, Staging, Produktiv) oder vier (Entwicklung, Test, Staging, Produktiv) Stages enthält.

Die Entwicklungsstage findet direkt beim Entwickler statt. Die Anwendung und ihre Daten können jederzeit vom Entwickler kaputtgemacht und wieder komplett neu aufgebaut werden. Hier kann und darf es passieren, dass sämtliche Nutzerdaten zerstört werden.

Danach geht es in die Test-Stage, bei der geschaut wird, ob das ganze Produkt mit allen Änderungen noch funktioniert und ob es Fehler gibt. Falls hier Probleme auftreten, dann werden diese direkt zurück zum Entwickler kommuniziert. Üblicherweise wird hier mit verschiedenen Daten gearbeitet, die Realdaten sehr ähnelt sollen, um sämtliche Szenarien besser abbilden zu können.

Danach geht es in die Stagingstage, die Änderungen enthält, die kurz vor Veröffentlichung stehen. Hier können experimentierfreudige Nutzer die nächste Version ausprobieren.

Und schlussendlich kommen die Änderung in die Produktiv-Stage, in der diese dann direkt bei allen Nutzern installiert werden. Hier sollten keine Fehler mehr in den Änderungen existieren, da hier mit realen Nutzerdaten gearbeitet wird, die nicht verloren gehen dürfen.

Der Autor hat sich für seine Entwicklung für das 3-Stage-Modell entschieden, da die Entwicklung noch am Anfang ist und die zusätzliche Test-Stage erhöhten Aufwand bedeutet. Die Test-Stage kann jederzeit nachträglich eingeführt werden.

Die 3 Stage spiegeln sich auch in der Quellcode-Organisation des Projekts wider. Die Entwicklungsstage sind sämtliche Feature- oder Fix-Branche, die der Autor in seiner Entwicklung anlegt. Da drin kann und darf alles passieren. Sobald die Änderungen an einem Branch abgeschlossen und in sich getestet sind, werden diese in den `develop`-Branch überführt. Dies entspricht derzeit der Staging-Stage. Hier wird alles insgesamt noch mal getestet. Oftmals mehrere Änderungen aus der Entwicklungsstage gleichzeitig. Nachdem alle Änderungen hier bestanden haben, werden diese in den `master`-Branch (Produktiv-Stage) überführt und eine neue Versionsnummer wird erstellt.

8 Ausblick

Nachdem das Projekt abgeschlossen und die Arbeit abgegeben ist, geht es darum, wie danach damit verfahren wird. Wird es weiterhin im Einsatz sein (siehe Nachnutzung 8.1)? Gibt es Erweiterungen und von welcher Art wäre vorstellbar (siehe 8.2)? Und wie wird mit Updates und Wartungen verfahren (siehe 8.3)?

8.1 Nachnutzung

Derzeit ist eine Nutzung am ethnologischen Institut der Max-Planck-Gesellschaft geplant und dafür war auch das Projekt erstellt wurden. Während der Entwicklung zeigten sich schon früh Bedarf und Interesse an dem Produkt und wünschte sich möglichst früh erste Ergebnisse zu sehen. So kam es auch zu einen regen Austausch zwischen dem Autor und den Bedarfsträgern bzw. Forschern, welche auch als erste Testgruppe fungierten.

Nach dem Abschluss des Projekts wird mit dem Auftraggeber und den Bedarfsträgern über den Erfolg erneut diskutiert und besprochen, wie die weitere Entwicklung (siehe 8.2) geschehen und das Produkt eingesetzt wird.

Eine Verbreitung an die anderen Institute ist derzeit noch nicht vorgesehen, aber in einem zukünftigen Stadium geplant.

8.2 Erweiterungen

Dies ist eine unvollständige Liste an Erweiterungen, die diese Anwendung in Zukunft erfahren kann. In vorherigen Kapiteln wurden schon einige Erweiterungen angesprochen, hier gibt es weitere.

8.2.1 Webseite

Im Rahmen dieser Arbeit ist eine Webseite leider nicht zustande gekommen. Eine Webseite wäre ein guter Ort, um neuen Nutzern einen ersten Eindruck über das Produkt, seine Funktion und die Nutzung zu vermitteln. Hier können auch Updates und Downloads bereitgestellt werden.

8.2.2 Schnittstellen

Schnittstellen sind Möglichkeiten, um Daten aus anderen Programmen für diese Anwendung oder auch anders herum bereitzustellen. Dazu können diese Daten importiert, exportiert oder auch direkt nativ unterstützt werden, um ein nahtloses Arbeiten mit den Programmen zu ermöglichen.

Dabei gibt es verschiedene Formate zur Gestaltung dieser. Ein bekanntes, welches sich in der ethnologischen Forschung etabliert hat, wären die Datenaustauschformate der DDI Alliance (siehe [5]). Diese hat verschiedene Schemas für XML, JSON und andere Dateiformate bereitgestellt, damit sich hier Daten leichter von einer Anwendung in eine andere übertragen lassen.

Diese Formate zu unterstützen würde somit den Forscher erlauben, Daten aus beliebigen kompatiblen Programmen in dieses und auch anders herum zu übertragen, um die Arbeit stark zu erleichtern, da die Daten nicht mehrfach händisch neu angelegt werden müssen.

Es gibt aber weitere Formen von Daten, mit den ein Forscher eines ethnologischen Instituts häufig zu tun hat. Dazu zählen auch die Programme Word und Excel der Office-Suite aus

dem Hause Microsoft. Hier können Erweiterungen bezüglich des Einlesens oder Generierung von Dokumenten entstehen. Auch Plug-ins, damit direkt über die Programme Word oder Excel auf die Anwendung zugegriffen werden kann, wären möglich.

8.2.3 Cloud-Dienst

Derzeit ist die Anwendung nur lokal auf dem Laptop des Nutzers installiert und alle Daten sind auch nur dort verfügbar und müssen auch von diesem gesichert werden. Dies kommt mit der Einschränkung, dass die Daten nur umständlich geteilt und gesichert werden können. Eine Möglichkeit zu Erweiterung wäre hier die Bereitstellung eines Servers, über die alles zentral gesichert und verwaltet wird.

Hier sind alle Daten zentral gespeichert und die Nutzer haben dann die Wahl, ob sie mit den Live-Daten vom Server oder mit der lokalen Kopie (falls keine Internetverbindung besteht) arbeiten möchten.

Besondere Vorteile an dieser Erweiterung sind:

- Daten lassen sich leichter durch die IT sichern und es lassen sich Back-up-Richtlinien stringend durchsetzen
- Das Teilen von Daten unter den Forschern untereinander ist leichter. Auch das gleichzeitige Arbeiten an gleichen Datensätzen wäre somit möglich.
- Der Forscher muss nicht mehr alle Daten lokal bereithalten. Damit würden auch die Anforderungen an das Endgerät gelockert werden. Eine Nutzung von Handys oder Tablets wäre somit möglich.
- Eine Installation ist nicht mehr zwingend notwendig, da die Weboberfläche auch zentral bereitgestellt werden kann. Dadurch wäre die Nutzung von Gastrechnern denkbar.
- Updates lassen sich leichter durchsetzen.

An dieser Erweiterung entstehen aber auch Probleme, die dann direkt berücksichtigt und behandelt werden müssen:

- Die Daten müssen auf dem Server sicher vor externer Manipulation und Zugriff sein.
- Wie mit gleichzeitigen Änderungen umgegangen, die gegenseitig sich im Konflikt stehen?
- Wie lassen sich Rechte für die Datensätze vergeben? Wie granular geht das und wie wird das eingehalten? Das ist besonders für das Teilen der Datensätze notwendig.
- Wie werden nachträglich Daten synchronisiert, wenn der Nutzer wieder online ist?

8.2.4 Suchoptimierungen

Die Suche lässt sich über verschiedene Wege noch weiter optimieren. Wichtig dabei ist, dass bei allen Optimierungen darauf geachtet werden muss, dass sämtliche Daten weiterhin den gleichen Sicherheitsstandard genießen, wie sie zuvor auch hatten. Ein paar Möglichkeiten, dies zu erreichen, werden im Folgenden kurz ausgearbeitet.

Die erste Idee wäre, einen weiteren Suchindex für andere Datentypen aufzubauen. Derzeit existiert nur einer für Strings, der auch Substrings ab der Länge 3 abdeckt. Daher wäre es hilfreich, wenn jeweils für Ganzzahlen, Fließkommazahlen oder Datumsangaben ein weiterer Index existiert, der auch Bereiche zwischen zwei Werte oder ähnliche Werte abdeckt. Die Werte sind zum Teil direkt durch die Eingabefelder direkt zu ermitteln und zum Teil befinden die sich irgendwo in längeren Texten.

Ein weiterer Weg der Optimierung wäre, für besonders kurzen Strings einen Index aufzubauen, damit auch nach Sachen wie “EU” gesucht werden kann.

Die dritte Idee wäre, eine passende Speicherstruktur für den Index zu entwerfen. Derzeit wird der Index in einer Datenbank hinterlegt. Diese ermöglicht es zwar schnell einen bestimmten Schlüssel abzurufen, muss aber alle Einträge abfragen, wenn der Nutzer alle Schlüssel in einem Bereich haben möchte.

Weiterhin ist noch ein Index hilfreich, welcher auch historische Werte berücksichtigt. Mit diesen können dann Forscher nach alten Werten suchen, bevor sie eine Änderung durchgeführt haben.

Des Weiteren weniger eine Geschwindigkeitsoptimierung, dafür mehr eine für die Nutzerfreundlichkeit wäre ein einfacher Editor für die Suchanfragen. Somit muss ein Anfänger nicht erst verstehen und lernen, wie Suchanfragen aufgebaut sind und was mit diesen alles möglich ist (siehe Anhang F).

8.3 Wartung und Update

Geplant sind zukünftige Updates, welche Probleme und Fehler im aktuellen Produkt beheben, sowie weitere Funktionen (siehe 8.2) hinzufügen. Zur Verbreitung der Updates wird ein ähnlicher Mechanismus wie bei der Installation (siehe 7.1) verfolgt. Die Pakete werden zusammengepackt und online zum Download bereitgestellt. Das Produkt überprüft selbstständig im Hintergrund auf Updates, informiert den Nutzer und leitet ihn zum Download und Installation an.

Auch eine automatische Installation ist möglich, auch wenn dies unter Einschränkungen durch die Art der Installation stehen kann. Dies ist zum Beispiel der Fall, wenn die Anwendung im Programmverzeichnis installiert wurde und derzeit kein befugter Administrator verfügbar ist, der das Passwort eingeben kann. Auch hierfür existieren Lösungen (z. B. über einen autorisierten Updatedienst), welche aber speziell noch eingerichtet werden müssen.

In welcher Art und Weise die Wartung und Updates erfolgen, ist derzeit noch ein Bestandteil, der in der Nachnutzung (siehe 8.1) geklärt wird.

9 Abschlussbetrachtung

Der Kern am Projekt war das Sicherheitskonzept und die Wahrung des Datenschutzes, damit alle Daten in jeglicher Situation geschützt sind. Um dieses Konzept herum wurde eine Datenbankanwendung mit modernen Prinzipien und Techniken entworfen, die das erstellte Sicherheitskonzept nutzen und unterstützen.

Dabei hat sich schnell herausgestellt, dass es sehr wohl möglich ist, alle Anforderungen an die Sicherheit zu befolgen und gleichzeitig eine praktische Anwendung zu entwerfen, die ein Forscher bei seiner Arbeit unterstützen kann.

Leider wurde in der Analyse festgestellt, dass viele Datenbankmanagementsysteme sich nur sehr schwierig so absichern lassen, dass all ihre Daten auch sicher verschlüsselt auf der Festplatte gespeichert sind. Dass dies aber dennoch geht, wurde am Beispiel LiteDB sehr gut gezeigt.

Bei den Programmiersprachen kann der Entwickler relativ flexibel sein. Die meisten der betrachteten sind ähnlich gut für die Umsetzung des Projekts geeignet. Trotzdem kann die Auswahl einen großen Einfluss auf das Testen und somit die Entwicklung haben, da hier je nach Sprache bestimmte Fehler leichter entdeckt oder ausgeschlossen werden.

Es gibt zwar viele Möglichkeiten für eine Zwei-Faktor-Authentifizierung, aber nur wenige, die auch lokal, ohne Internetverbindung und externe Dienstleister funktionieren. In dieser Arbeit wurde ein Hardwaretoken genutzt, welcher das Fido2-Protokoll benutzt. Leider ist dies noch im Entwurfsstadium und noch nicht so stark verbreitet, dass nur die wenigsten Nutzer einen zu Hause haben und auch nur große Webseiten bieten derzeit eine Unterstützung dafür an.

Ein weiteres, aber großes Problem für diese Arbeit war der zeitliche Aspekt. Es wurden sehr viele Funktionen für die Anwendung angedacht, sodass es zum einen für den Autor schwierig war, diese alle einzubauen, aber auch zum anderen diese zu dokumentieren. So bleibt zum Schluss eine große Liste an Funktionen für künftige Erweiterungen, die noch ausgearbeitet und in die Anwendung eingebaut werden können.

Abschließend lässt sich sagen, dass das Ziel, die Erleichterung der Arbeit mit Interviewdaten von einer Feldforschung und die sichere Aufbewahrung dieser für Forscher an einem ethnologischen Institut erreicht wurde.

Literatur und Quellen

- [1] Internet Engineering Task Force (IETF). *RFC 6455: The WebSocket Protocol*. URL: <https://www.rfc-editor.org/rfc/rfc6455.html> (besucht am 29.06.2022).
- [2] World Wide Web Consortium (W3C). *Web Authentication: An API for accessing Public Key Credentials - Level 3*. URL: <https://w3c.github.io/webauthn/> (besucht am 02.07.2022).
- [3] World Wide Web Consortium (W3C). *Web Authentication: An API for accessing Public Key Credentials - Level 3*. URL: <https://w3c.github.io/webauthn/#sectn-registering-a-new-credential> (besucht am 02.07.2022).
- [4] Make Something AB. *passwordless-lib/fido2-net-lib: FIDO2 .NET library for FIDO2 / WebAuthn Attestation and Assertion using .NET*. URL: <https://github.com/passwordless-lib/fido2-net-lib> (besucht am 02.07.2022).
- [5] DDI Alliance. *Overview of Current Products*. URL: <https://ddialliance.org/products/overview-of-current-products> (besucht am 03.07.2022).
- [6] Auswärtiges Amt. *Neuseeland: Reise- und Sicherheitshinweise - Auswärtiges Amt*. URL: <https://www.auswaertiges-amt.de/de/aussenpolitik/laender/neuseeland-node/neuseelandsicherheit/220146> (besucht am 30.06.2022).
- [7] Auswärtiges Amt. *USA / Vereinigte Staaten: Reise- und Sicherheitshinweise - Auswärtiges Amt*. URL: https://www.auswaertiges-amt.de/de/aussenpolitik/laender/usa-node/usaverinigtestaatensicherheit/201382#content_4 (besucht am 30.06.2022).
- [8] Dan Arias. *Adding Salt to Hashing: A Better Way to Store Passwords*. URL: <https://auth0.com/blog/adding-salt-to-hashing-a-better-way-to-store-passwords/> (besucht am 24.06.2022).
- [9] GitLab B.V. *Dependency Scanning (ULTIMATE)*. URL: https://gitlab.gwdg.de/help/user/application_security/dependency_scanning/index (besucht am 02.07.2022).
- [10] GitLab B.V. *Infrastructure as Code (IaC) Scanning*. URL: https://gitlab.gwdg.de/help/user/application_security/iac_scanning/index (besucht am 02.07.2022).
- [11] GitLab B.V. *Secret Detection (FREE)*. URL: https://gitlab.gwdg.de/help/user/application_security/secret_detection/index (besucht am 02.07.2022).
- [12] GitLab B.V. *Static Application Security Testing (SAST) (FREE)*. URL: https://gitlab.gwdg.de/help/user/application_security/sast/index (besucht am 02.07.2022).
- [13] Brian Carroll. *Porting Elm to WebAssembly*. URL: <https://dev.to/briancarroll/porting-elm-to-webassembly-2lp4> (besucht am 25.06.2022).
- [14] DUO - Cisco. *Guide to Web Authentication*. URL: <https://webauthn.guide/> (besucht am 02.07.2022).
- [15] DUO - Cisco. *WebAuthn.io*. URL: <https://webauthn.io/> (besucht am 02.07.2022).
- [16] SQLite Consortium. *SQLite Home Page*. URL: <https://sqlite.org/index.html> (besucht am 22.06.2022).
- [17] SQLite Consortium. *SQLite: Top-level Files of trunk*. URL: <https://sqlite.org/src/dir?ci=trunk> (besucht am 22.06.2022).
- [18] Evan Czaplicki. *Blazing Fast HTML*. URL: <https://elm-lang.org/news/blazing-fast-html-round-two> (besucht am 25.06.2022).
- [19] Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen. *Information: Umstellung von GWDG Gitlab auf Community Edition*. URL: <https://info.gwdg.de/news/information-umstellung-von-gwdg-gitlab-auf-community-edition/> (besucht am 02.07.2022).
- [20] Maurício David. *Data Structure - LiteDB :: A .NET embedded NoSQL database*. URL: <http://www.litedb.org/docs/data-structure/> (besucht am 24.06.2022).

-
- [21] Maurício David. *Encryption - LiteDB :: A .NET embedded NoSQL database*. URL: <https://www.litedb.org/docs/encryption/> (besucht am 22.06.2022).
 - [22] Maurício David. *LiteDB :: A .NET embedded NoSQL database*. URL: <https://www.litedb.org/> (besucht am 22.06.2022).
 - [23] Maurício David. *mbdavid/LiteDB: LiteDB - A .NET NoSQL Document Store in a single data file - https://www.litedb.org*. URL: <https://github.com/mbdavid/litedb> (besucht am 22.06.2022).
 - [24] Maurício David. *Object Mapping - LiteDB :: A .NET embedded NoSQL database*. URL: <http://www.litedb.org/docs/object-mapping/> (besucht am 06.07.2022).
 - [25] Maurício David. *Overview - LiteDB :: A .NET embedded NoSQL database*. URL: <http://www.litedb.org/docs/> (besucht am 24.06.2022).
 - [26] Claudia Eckert. *IT-Sicherheit: Konzepte – Verfahren – Protokolle*. Oldenbourg Verlag, 2012. ISBN: 978-3-486-70687-1.
 - [27] Max-Planck-Institut für ethnologische Forschung. *Institut / Max Planck Institut für ethnologische Forschung*. URL: <https://www.eth.mpg.de/2899313/institute> (besucht am 30.06.2022).
 - [28] MariaDB Foundation. *Data-at-Rest Encryption Overview - MariaDB Knowledge Base*. URL: <https://mariadb.com/kb/en/data-at-rest-encryption-overview/> (besucht am 22.06.2022).
 - [29] MariaDB Foundation. *File Key Management Encryption Plugin - MariaDB Knowledge Base*. URL: <https://mariadb.com/kb/en/file-key-management-encryption-plugin/> (besucht am 22.06.2022).
 - [30] MariaDB Foundation. *MariaDB*. URL: <https://github.com/MariaDB/> (besucht am 22.06.2022).
 - [31] MariaDB Foundation. *MariaDB Foundation - MariaDB.org*. URL: <https://mariadb.org/> (besucht am 22.06.2022).
 - [32] SQLite Consortium und Frank A. Krueger. *praeclarum/sqlite-net: Simple, powerful, cross-platform SQLite client and ORM for .NET*. URL: <https://github.com/praeclarum/sqlite-net> (besucht am 22.06.2022).
 - [33] Nitrokey GmbH. *Nitrokey FIDO2 | www.nitrokey.com*. URL: https://shop.nitrokey.com/de_DE/shop/product/nkfi2-nitrokey-fido2-55 (besucht am 02.07.2022).
 - [34] Ritvik Gupta. *Rust Is the Most Loved Language, Beats Python and TypeScript*. URL: <https://www.turing.com/blog/rust-is-the-most-popular-programming-language/> (besucht am 05.07.2022).
 - [35] GitHub Inc. *Search - language:C#*. URL: <https://github.com/search?q=language%3AC%23&type=Repositories&ref=advsearch&l=C%23&l=> (besucht am 05.07.2022).
 - [36] MongoDB Incorporated. *BSON (Binary JSON): Specification*. URL: <https://bsonspec.org/spec.html> (besucht am 24.06.2022).
 - [37] MongoDB Incorporated. *MongoDB Data Encryption | MongoDB*. URL: <https://www.mongodb.com/basics/mongodb-encryption> (besucht am 22.06.2022).
 - [38] MongoDB Incorporated. *MongoDB: Die Plattform Für Anwendungsdaten | MongoDB*. URL: <https://www.mongodb.com/de-de> (besucht am 22.06.2022).
 - [39] MongoDB Incorporated. *mongodb/mongo: The MongoDB Database*. URL: <https://github.com/mongodb/mongo> (besucht am 22.06.2022).
 - [40] MongoDB Incorporated. *Server Side Public License - MongoDB*. URL: <https://github.com/mongodb/mongo/blob/master/LICENSE-Community.txt> (besucht am 22.06.2022).

-
- [41] Europäische Kommission. *Ethics and data protection*. 2021. URL: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-and-data-protection_he_en.pdf (besucht am 23.06.2022).
 - [42] Eike Kühl. *Reisen: So schützen Sie Ihre Daten an der Grenze* / ZEIT ONLINE. URL: <https://www.zeit.de/digital/datenschutz/2019-06/reisen-datenschutz-grenzbeamte-kontrolle-usa/komplettansicht> (besucht am 30.06.2022).
 - [43] K. Brunner und L. Deuber und F. Ebert und F. Obermaier und N. Richter und V. Wormer. *Wie eine Polizei-App Touristen in China ausspäht - Politik - SZ.de*. URL: <https://www.sueddeutsche.de/politik/china-app-ueberwachung-touristen-1.4508470> (besucht am 30.06.2022).
 - [44] Wallabit Media LLC. *U2F, Fido2, USB & Webauthn Authentication Supported Sites*. URL: <https://www.buybitcoinworldwide.com/dongle-auth/> (besucht am 02.07.2022).
 - [45] Wojciech Muła. *Sample skip list; max level is 4*. URL: https://en.wikipedia.org/wiki/File:Skip_list.svg (besucht am 30.06.2022).
 - [46] Oracle. *MySQL*. URL: <https://www.mysql.com/de/> (besucht am 22.06.2022).
 - [47] Oracle. *MySQL :: Commercial License for OEMs, ISVs and VARs*. URL: <https://www.mysql.com/about/legal/licensing/oem/> (besucht am 22.06.2022).
 - [48] Oracle. *MySQL :: MySQL Enterprise Transparent Data Encryption (TDE)*. URL: <https://www.mysql.com/products/enterprise/tde.html> (besucht am 22.06.2022).
 - [49] Oracle. *mysql/mysql-server: MySQL Server, the world's most popular open source database, and MySQL Cluster, a real-time, open source transactional database*. URL: <https://github.com/mysql/mysql-server> (besucht am 22.06.2022).
 - [50] William Pugh. *Concurrent Maintenance of Skip Lists*. Institute for Advanced Computer Studies, Department of Computer Science, University of Maryland, College Park. Apr. 1989. URL: <http://hdl.handle.net/1903/542> (besucht am 30.06.2022).
 - [51] I. Puja, P. Posic und D. Jaksic. "Overview and Comparison of Several relational Database Modelling Metodologies and Notations". In: *2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. 2019, S. 1641–1646. DOI: 10.23919/MIPRO.2019.8756667.
 - [52] Bundesamt für Sicherheit in der Informationstechnik (BSI). *IT-Grundschutz-Kompendium (Edition 2021)*. 2021. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2021.pdf?__blob=publicationFile&v=6 (besucht am 23.06.2022).
 - [53] Bundesamt für Sicherheit in der Informationstechnik (BSI). *Zwei-Faktor-Authentisierung*. 2018. URL: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/zwei-faktor-authentisierung_node.html (besucht am 23.06.2022).
 - [54] Universe Today. *How Many Atoms Are There in the Universe?* - Universe Today. URL: <https://www.universetoday.com/36302/atoms-in-the-universe/> (besucht am 24.06.2022).
 - [55] Wikipedia. *Martin-Notation*. URL: <https://de.wikipedia.org/wiki/Martin-Notation> (besucht am 05.07.2022).

Abbildungsverzeichnis

1	FIDO2 USB Key von NitroKey	28
2	Überblick über das technische System	31
3	Der Anmeldefluss mit Nutzernamen, Passwort und FIDO.	33
4	Erstellung neuer Datenbankzugangsdaten	35
5	Skip-Listen	36
6	Entity Relationship Diagram	38
7	Rollenschema für das Projekt	41

Tabellenverzeichnis

1	Übersicht Programmiersprachen	12
2	Übersicht Programmiersprachen	14
3	Übersicht der DBMS	16
4	Lokale Verschlüsselung der DBMS	17
5	Autorisierung der DBMS	18
6	Editortypen	40
7	Größe der Testdatenbank	53

Anhang

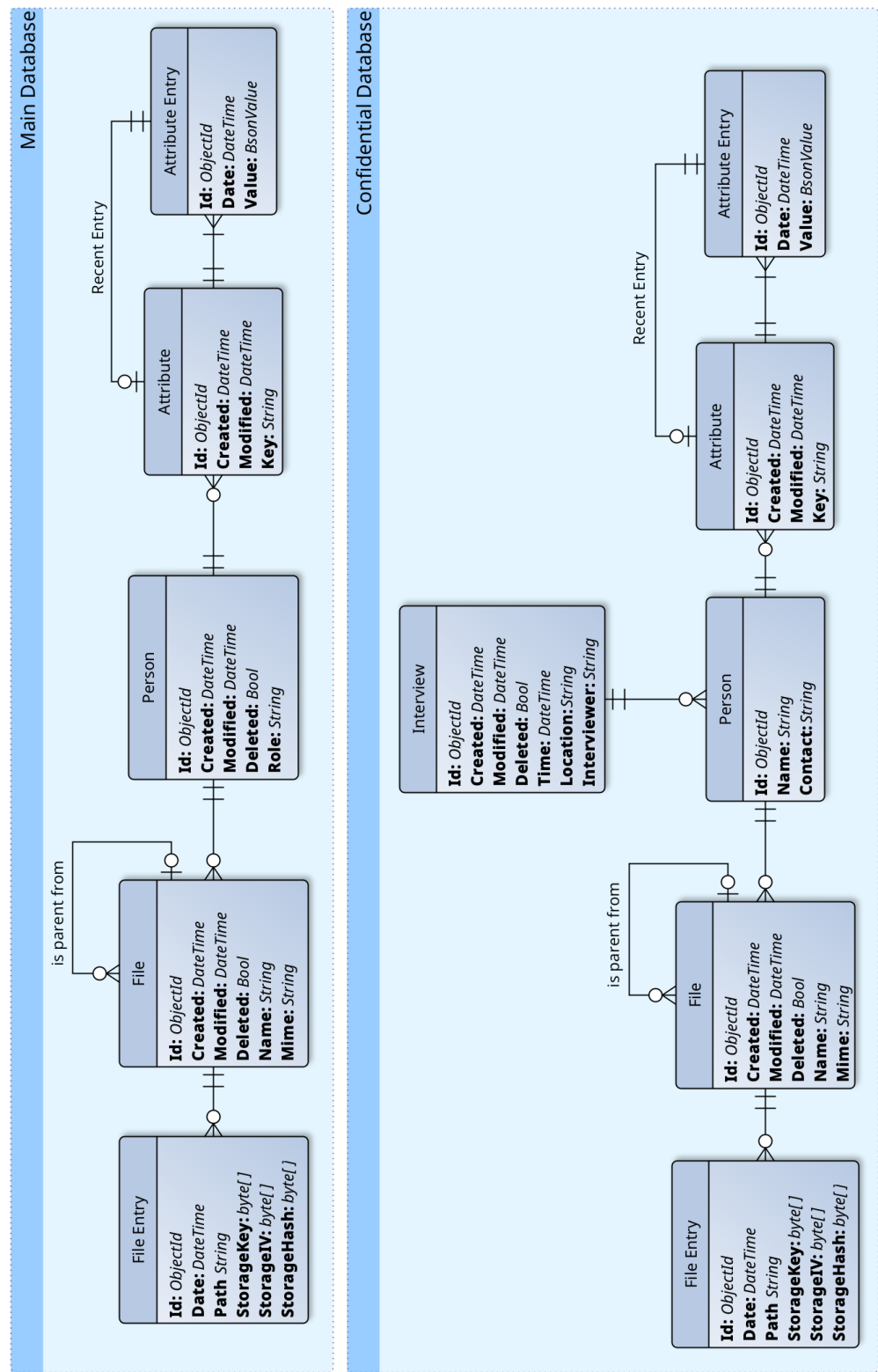
Der Anhang sind weitere Dokumentationen zum Projekt und zur Arbeit enthalten. Quellcode ist nur auf der beiliegenden CD verfügbar.

Die Dokumentationen sind teilweise auf Englisch, weil das Programm selbst auf Englisch dokumentiert wurde. Es wurden nicht alle Dokumentationen auf Deutsch übersetzt.

Die Kapitel D und E sind die gerenderte Version des Schemas. Das originale Schema befindet sich als Json-Schema bzw. AsyncApi-Schema auf der Beiliegenden CD. Diese Schemas wurden mit dem beiliegenden Tool `/tools/AsyncApiRenderer` in die dargestellte Repräsentation umgewandelt.

Bei der AsyncApi wird eine Liste an Response-Nachrichten angezeigt. Dies sind Nachrichten, die der Server als Antwort auf die Anfrage senden kann. Die Nachrichten können zeitlich wiederholt oder mehrere Unterschiedliche hintereinander gesendet werden. Dies obliegt der Aufgabe, die der Server mit der Anfrage bearbeitet.

A Entity Relationship Diagramm v0.6



Erklärung siehe Abbildung 6.

B Projektsteckbrief

Projekttitel	Planung und Entwicklung einer Datenbankanwendung für das Forschungsdatenmanagement		
Projektnummer	2022-SWD-19526		
Projektleitung	Max Brauer		
Auftraggeber	Sebastian Ehser, Max-Planck-Institut für ethnologische Forschung		
Projektnutzen	Verwaltung von Forschungsdaten		
Projektumfeld			
Projekthalt / -ziele	<p>Erstellen eine Datenbankanwendung zur Aufnahme von Forschungsdaten für Forschende eines ethnologischen Instituts. Diese Anwendung soll den Forschenden auf seinen Reisen begleiten und die Arbeit mit seinen Daten erleichtern. Dabei soll ein besonderes Augenmerk auf die Sicherheit gelegt werden.</p> <p>Als Nichtziel wurden zusätzliche Relationen zwischen den Interviewten (außer den vorgeschriebenen) festgelegt.</p> <p>(prototypisch Start mit Raza und das Ziel das auf das gesamte Institut umzusetzen)</p>		
Projektnutzen	<ul style="list-style-type: none"> • Vereinfachung in der Arbeitsweise der Forschenden durch zentrale und strukturierte Speicherung und Darstellung von Daten • Sicherung der Daten durch Backups und Zugriffskontrollen • Weniger Papierverbrauch bei der Arbeit mit den Daten 		
Klärungs-/ Unterstützungsbedarf	<ul style="list-style-type: none"> • Genaues Modell der zu speichernden Daten • Aktuelle Arbeitsweise der Forschenden 		
Start / Ende	Januar 2022 - Juni 2022		
Zwischentermine	<ul style="list-style-type: none"> • Anmeldung der Bachelorarbeit: offen • Vorstellen der Zwischenergebnisse: im 2-4 Wochen Rythmus • Verteidigung der Arbeit: 5-6 Monate nach Anmeldung der Arbeit • Alphaversion: • Betaversion: • Releaseversion: ähnlich zur Verteidigung 		
Aufwand	Software: 112-150 Stunden	Schriftliche Arbeit: 300 Stunden	Gesamt: 450 Stunden
Beteiligte	<ul style="list-style-type: none"> • Max Brauer (Entwickler und Verfasser der Arbeit) • Sebastian Ehser (Auftraggeber, Projektberater MPI) • Christian Kieser (technischer Berater MPI) • Farah Raza (Bedarfsträgerin) 		
Risiken	<ul style="list-style-type: none"> • Krankheit oder sonstige Ausfälle • Software wird nicht rechtzeitig fertig • Software entspricht nicht oder nicht komplett den Wünschen der Kunden 		

C config.json Schema

Informationen und Erklärungen sind im Kapitel 4.4.4. Für den Vergleich gibt es hier zwei Repräsentationen:

1. Das originale Schema, welches so aufgebaut ist, wie es nach json-schema.org spezifiziert

ist. Dies wurde manuell vom Autor erstellt.

2. Eine eigene Darstellung des oben gezeigten Schemas, welches das Schema als generierte Tabelle und generiertes Beispiel anzeigt. Der Generator befindet sich mit auf der CD als Quellcode unter `/tools/AsyncApiRenderer` und wurde für dieses Projekt speziell angefertigt.

Alle weiteren Darstellungen und Beispiel im Anhang nutzen die 2. Repräsentation. Die 1. Repräsentation aller Anhänge befindet sich auf der CD im Ordner `/schemas`.

1. Darstellung:

```
{
  "$schema": "http://json-schema.org/draft-07/schema",
  "type": "object",
  "properties": {
    "name": {
      "type": "string",
      "description": "Der Name der Datenbank. Muss der gleiche wie
der Ordner sein.",
      "examples": [ "test-db" ]
    },
    "recovery-key-hash": {
      "type": "string",
      "description": "Der Base64 codierte SHA512 Hash des
Master-Keys.",
      "examples": [ "abdef01234567890..." ]
    },
    "role-schema": {
      "type": "string",
      "description": "Der Pfad zum Rollenschema innerhalb des
Schemaordners. Dieses Schema gilt für die gesamte Datenbank."
    },
    "access": {
      "type": "array",
      "description": "Eine Liste von Zugangsdaten, die Zugriff auf
diese Datenbank haben",
      "items": {
        "type": "object",
        "description": "Die Einstellungen zu einen speziellen
Zugriff",
        "properties": {
          "user": {
            "type": "string",
            "description": "Der Nutzernamen des Nutzers, der
Zugriff hat. Dieser darf mehrfach verwendet werden.",
            "examples": [ "mustermann" ]
          },
          "user-id": {
            "type": "string",
            "format": "guid",
            "description": "Eine GUID für diesen Nutzerzugang."
          }
        }
      }
    }
  }
}
```

```

Wird für die Fido-Authentifizierung genutzt.",
    "examples":
        [ "d19482e9-e5df-4826-a824-235b5119dafc" ]
},
"password-salt": {
    "type": "string",
    "description": "Base64 codierte zufällige
Byte-Folge, die zusammen mit dem Passwort verarbeitet wird.",
    "examples": [ "abdef01234567890..." ]
},
"password-hash": {
    "type": "string",
    "description": "Base64 codierter Hash aus
Passwort und Salt",
    "examples": [ "abdef01234567890..." ]
},
"fido-descriptor": {
    "type": [ "null", "object" ],
    "description": "Gespeicherte Informationen zum
Fido USB Stick. Format ist durch die Bibliothek bestimmt.",
    "examples": [
        {
            "Type": 0,
            "Id": "ABDEFabcdef5678",
            "Transports": null
        }
    ]
},
"fido-public-key": {
    "type": [ "null", "string" ],
    "description": "Base64 codierter Public Key vom
Fido USB Stick",
    "examples": [ "abdef01234567890..." ]
},
"fido-user-handle": {
    "type": [ "null", "string" ],
    "description": "Base64 codierter User Handle vom
Fido USB Stick",
    "examples": [ "abdef01234567890..." ]
},
"fido-counter": {
    "type": [ "null", "integer" ],
    "description": "Der Counter Wert bei der letzten
Anmeldung.",
    "examples": [ 1024 ]
},
"enc-salt": {
    "type": "string",
    "description": "Base64 codierte zufällige

```

```

Bytefolge, die mit dem Passwort gehasht wird.",
    "examples": [ "abdef01234567890..." ]
  },
  "enc-key": {
    "type": "string",
    "description": "Base64 codierte, mit AES
verschlüsselte Datenbankschlüssel. Um diesen zu entschlüsseln ist der Hash
aus enc-salt und Passwort nötig.",
    "examples": [ "abdef01234567890..." ]
  },
  "created": {
    "type": "string",
    "format": "date-time",
    "description": "Der Zeitstempel an dem dieser
Zugriff angelegt wurde."
  }
},
"required": [
  "user",
  "user-id",
  "password-salt",
  "password-hash",
  "fido-descriptor",
  "fido-public-key",
  "fido-user-handle",
  "fido-counter",
  "enc-salt",
  "enc-key",
  "created"
]
},
"contains-index": {
  "type": "boolean",
  "description": "Gibt an, ob ein Index für diese Datenbank
existiert. Wird nicht mehr verwendet.",
  "examples": [ "true" ]
}
},
"required": [
  "name",
  "recovery-key-hash",
  "role-schema",
  "access",
  "contains-index"
]
}

```

2. Darstellung:

Path	Flags	Type/Value	Description
<code>name</code>	R	<i>string</i>	Der Name der Datenbank. Muss der gleiche wie der Ordner sein.
<code>recovery-key-hash</code>	R	<i>string</i>	Der Base64 codierte SHA512 Hash des Master-Keys.
<code>role-schema</code>	R	<i>string</i>	Der Pfad zum Rollenschema innerhalb des Schemaordners. Dieses Schema gilt für die gesamte Datenbank.
<code>access</code>	R	<i>array</i>	Eine Liste von Zugangsdaten, die Zugriff auf diese Datenbank haben
<code>access[]</code>	R	<i>object</i>	Die Einstellungen zu einen speziellen Zugriff
<code>access[].user</code>	R	<i>string</i>	Der Nutzernamen des Nutzers, der Zugriff hat. Dieser darf mehrfach verwendet werden.
<code>access[].user-id</code>	R	<i>string</i> , <guid>	Eine GUID für diesen Nutzerzugang. Wird für die Fido-Authentifizierung genutzt.
<code>access[].password-salt</code>	R	<i>string</i>	Base64 codierte zufällige Byte-Folge, die zusammen mit dem Passwort verarbeitet wird.
<code>access[].password-hash</code>	R	<i>string</i>	Base64 codierter Hash aus Passwort und Salt
<code>access[].fido-descriptor</code>	RN	<i>object</i>	Gespeicherte Informationen zum Fido USB Stick. Format ist durch die Bibliothek bestimmt.
<code>access[].fido-public-key</code>	RN	<i>string</i>	Base64 codierter Public Key vom Fido USB Stick
<code>access[].fido-user-handle</code>	RN	<i>string</i>	Base64 codierter User Handle vom Fido USB Stick
<code>access[].fido-counter</code>	RN	<i>int</i>	Der Counter Wert bei der letzten Anmeldung.
<code>access[].enc-salt</code>	R	<i>string</i>	Base64 codierte zufällige Bytefolge, die mit dem Passwort gehasht wird.
<code>access[].enc-key</code>	R	<i>string</i>	Base64 codierte, mit AES verschlüsselte Datenbankschlüssel. Um diesen zu entschlüsseln ist der Hash aus enc-salt und Passwort nötig.
<code>access[].created</code>	R	<i>string</i> , <date-time>	Der Zeitstempel an dem dieser Zugriff angelegt wurde.
<code>contains-index</code>	R	<i>bool</i>	Gibt an, ob ein Index für diese Datenbank existiert. Wird nicht mehr verwendet.

Flags:

- *R*: This field is required. This path must always exist.
- *N*: The value of this field can be `null`.

```
{
  "name": "test-db",
  "recovery-key-hash": "abdef01234567890...",
  "role-schema": "abc",
  "access": [
    {
      "user": "mustermann",
      "user-id": "d19482e9-e5df-4826-a824-235b5119dafc",
      "password-salt": "abdef01234567890...",
      "password-hash": "abdef01234567890...",
      "fido-descriptor": {
        "Type": 0,
        "Id": "ABDEFabcdef5678",
        "Transports": null
      },
      "fido-public-key": "abdef01234567890...",
      "fido-user-handle": "abdef01234567890...",
      "fido-counter": 1024,
      "enc-salt": "abdef01234567890...",
      "enc-key": "abdef01234567890...",
      "created": "2001-01-01T15:17:19.001"
    }
  ],
  "contains-index": "true"
}
```

D Rollenschema

Genaue Erklärung dazu siehe Kapitel 4.4.3.

Path	Flags	Type/Value	Description
<code>name</code>	R	<i>string</i>	Der komplette Name inklusive lokalen Pfad des Schemas.
<code>online</code>	RN	<i>string</i> , <code><url></code>	Die online URL, wo das Schema abgerufen werden könnte. Wenn das nur ein lokales Schema ist, dann ist dieser Wert null.
<code>roles</code>	R	<i>array</i>	Alle einzelnen Rollen zu diesem Schema
<code>roles[]</code>	R	<i>object</i>	
<code>roles[].name</code>	R	<i>string</i>	Der Name der Rolle
<code>roles[].abstract</code>	R	<i>bool</i>	Bestimmt ob diese Rolle als abstrakt deklariert wurde. Abstrakte Rollen können nicht instantiiert werden.
<code>roles[].parent</code>	RN	<i>string</i>	Der optionale Name der Elternrolle von dem alle Eigenschaften geerbt werden sollen.
<code>roles[].attributes</code>	R	<i>object</i>	Alle Attribute dieser Rolle. Die Namen der Attribute sind frei wählbar, dürfen aber nicht doppelt vorkommen.
<code>roles[].attributes.*</code>	A	<i>object</i>	Ein einzelnes Attribut für die Rolle
<code>roles[].attributes.*.type</code>	R	"DateTime", "SingleLine", "MultiLine", "Number", "Int", "Bool"	Die Art und somit auch der Typ des Eingabefeldes
<code>roles[].attributes.*.protected</code>	R	<i>bool</i>	Gibt an, ob das Attribut geschützt (confidential) ist.
<code>roles[].attributes.*.history</code>	R	<i>bool</i>	Gibt an, ob eine Historie zu diesem Attribut angelegt werden soll.

Flags:

- *R*: This field is required. This path must always exist.
- *N*: The value of this field can be [null](#).
- *A*: This is an additional property. You can insert any not previously defined name to add your own properties. The schema of this property is predefined and has to be used as above.

```
{
  "name": "/test/schemas/v0.json",
  "online": "http://schemas.example.com/test/schemas/v0.json",
  "roles": [
    {
      "name": "Patient",
      "abstract": false,
      "parent": null,
      "attributes": {
        "gender": {
          "type": "SingleLine",
          "protected": true,
          "history": false
        },
        "personal experience": {
          "type": "MultiLine",
          "protected": false,
          "history": true
        }
      }
    },
    {
      "name": "Family",
      "abstract": false,
      "parent": null,
      "attributes": {
        "religion": {
          "type": "SingleLine",
          "protected": true,
          "history": false
        },
        "personal experience": {
          "type": "MultiLine",
          "protected": false,
          "history": true
        }
      }
    }
  ]
}
```

E Dacryptero - Internal WebSocket API

Version: 1.0.0

This is the internal api used by the ui and the main webserver. See in the development notes for more details.

E.1 PUB /ws/ Operation

The messages that are sent from the UI to the server

Accepts **one of** the following messages:

E.1.1 AccountLogin *Login with the provided credentials*

The UI sends the server the username and password combination. This will result in a `FidoResult` or `AccountFidoRequest` message.

Path	Flags	Type/Value	Description
<code>\$type</code>	R	"AccountLogin"	
<code>username</code>	R	<i>string</i>	
<code>password</code>	R	<i>string</i>	

Flags:

- *R*: This field is required. This path must always exists.

Responses:

- `FidoResult`
- `SendNotification`
- `AccountFidoRequest`

Examples:

```
{
  "$type": "AccountLogin",
  "username": "abc",
  "password": "abc"
}
```

E.1.2 AccountRegister *Register with new credentials*

The UI sends the server the username and password combination for a new account.

Path	Flags	Type/Value	Description
<code>\$type</code>	R	"AccountRegister"	
<code>database</code>	R	<i>string</i>	
<code>key</code>	RN	<i>string</i>	The key that is used for creating new databases. For existing databases this key is not used and null.
<code>username</code>	R	<i>string</i>	
<code>password</code>	R	<i>string</i>	

Flags:

- *R*: This field is required. This path must always exists.
- *N*: The value of this field can be `null`.

Responses:

- SendNotification
- AccountFidoRequest

Examples:

```
{
  "$type": "AccountRegister",
  "database": "db-main",
  "key": null,
  "username": "abc",
  "password": "abc"
}
```

```
{
  "$type": "AccountRegister",
  "database": "db-main",
  "key": "abc",
  "username": "abc",
  "password": "abc"
}
```

E.1.3 DatabaseAddFinish *Finalize the DB creation*

Finalize the DB creation and sends every user the new database

Path	Flags	Type/Value	Description
<code>\$type</code>	R	"DatabaseAddFinish"	
<code>id</code>	R	<i>string</i>	The key that was used for the db creation process

Flags:

- *R*: This field is required. This path must always exists.

Responses:

- SendNotification
- InfoSend
- DatabaseCreated

Examples:

```
{
  "$type": "DatabaseAddFinish",
  "id": "#id-0123456789abcdef"
}
```

E.1.4 DatabaseAddRequest *Starts the process of the db creation*

Starts the process of the db creation

Path	Flags	Type/Value	Description
\$type	R	"DatabaseAddRequest"	
database	R	<i>string</i>	The new database name. The format has to match the pattern <code>^[\w-]+\$</code>
schema	R	<i>string</i>	

Flags:

- *R*: This field is required. This path must always exists.

Responses:

- SendNotification
- DatabaseAddRequestInfo

Examples:

```
{
  "$type": "DatabaseAddRequest",
  "database": "new-db-name",
  "schema": "abc"
}
```

E.1.5 DatabaseCancelCreation *Cancel DB Creation Process*

Cancel the DB creation process and discard all collected data.

Path	Flags	Type/Value	Description
\$type	R	"DatabaseCancelCreation"	
key	R	<i>string</i>	The key that is used to identify the db creation process

Flags:

- *R*: This field is required. This path must always exists.

Examples:

```
{
  "$type": "DatabaseCancelCreation",
  "key": "abc"
}
```

E.1.6 DatabaseConnect *Connect to Database*

Starts the connection process to an existing database. If required it will ask for user login.

Path	Flags	Type/Value	Description
<code>\$type</code>	R	"DatabaseConnect"	
<code>name</code>	R	<i>string</i>	The database name

Flags:

- *R*: This field is required. This path must always exists.

Responses:

- SendNotification
- LoginRequest

Examples:

```
{
  "$type": "DatabaseConnect",
  "name": "abc"
}
```

E.1.7 DatabaseRemoveUser *Removes User from Database*

Tells the server to remove a user from the database configuration. This process is not revertible.

Path	Flags	Type/Value	Description
<code>\$type</code>	R	"DatabaseRemoveUser"	
<code>database</code>	R	<i>string</i>	
<code>user-id</code>	R	<i>string</i> , <guid>	

Flags:

- *R*: This field is required. This path must always exists.

Responses:

- SendNotification
- InfoSend

Examples:

```
{
  "$type": "DatabaseRemoveUser",
  "database": "db-main",
  "user-id": "guid"
}
```

E.1.8 DatabaseUnlock *Unlocks Database*

Unlocks the database to be able to add new access. This can be done using the provided master key. Otherwise the server will start an authentication process.

Path	Flags	Type/Value	Description
\$type	R	"DatabaseUnlock"	
database	R	<i>string</i>	
master-key	RN	<i>string</i>	

Flags:

- *R*: This field is required. This path must always exist.
- *N*: The value of this field can be `null`.

Responses:

- SendNotification
- InfoSend

Examples:

```
{
  "$type": "DatabaseUnlock",
  "database": "db-main",
  "master-key": null
}
```

```
{
  "$type": "DatabaseUnlock",
  "database": "db-main",
  "master-key": "abc"
}
```

E.1.9 DataInterviewAddRequest *Add Interview Request*

Creates a new interview entry at the server and fill with empty data. The server will respond with the created interview entry

Path	Flags	Type/Value	Description
\$type	R	"DataInterviewAddRequest"	
database	R	<i>string</i>	

Flags:

- *R*: This field is required. This path must always exist.

Responses:

- DataInterviewAddSend

Examples:

```
{
  "$type": "DataInterviewAddRequest",
  "database": "db-main"
}
```

E.1.10 DataInterviewGet *Request the data of a single interview*

Get the full data of a single interview

Path	Flags	Type/Value	Description
\$type	R	"DataInterviewGet"	
id	R	<i>string</i>	

Flags:

- *R*: This field is required. This path must always exist.

Responses:

- DataInterviewSend

Examples:

```
{
  "$type": "DataInterviewGet",
  "id": "#id"
}
```

E.1.11 DataInterviewListPersonRequest *Request the list of persons in an interview*

Request the full list of all persons that are assigned to an interview.

Path	Flags	Type/Value	Description
\$type	R	"DataInterviewListPersonRequest"	
id	R	<i>string</i>	

Flags:

- *R*: This field is required. This path must always exist.

Responses:

- DataInterviewListPersonSend

Examples:

```
{
  "$type": "DataInterviewListPersonRequest",
  "id": "#id"
}
```

E.1.12 DataPersonAddRequest *Add Person Request*

Creates a new person entry at the server and fill with empty data. The server will respond with the created interview entry.

Path	Flags	Type/Value	Description
\$type	R	"DataPersonAddRequest"	
database	R	<i>string</i>	
interview	R	<i>string</i>	
role	R	<i>string</i>	

Flags:

- *R*: This field is required. This path must always exists.

Responses:

- EditDenied
- DataPersonAddSend

Examples:

```
{
  "$type": "DataPersonAddRequest",
  "database": "db-main",
  "interview": "#id",
  "role": "abc"
}
```

E.1.13 DataPersonGet *Request the data of a single person*

Get the full data of a single person with history of attributes

Path	Flags	Type/Value	Description
\$type	R	"DataPersonGet"	
id	R	<i>string</i>	

Flags:

- *R*: This field is required. This path must always exists.

Responses:

- DataPersonSend

Examples:

```
{
  "$type": "DataPersonGet",
  "id": "#id"
}
```

E.1.14 DatabaseUnlock *Locks unlocked Database*

With **DatabaseUnlock** the Database transition in the unlocked state (if no master key was provided after the login process). The transition the database back to the safe locked state this message can be sent. To add new access again you have to send **DatabaseUnlock**.

Path	Flags	Type/Value	Description
\$type	R	"DatabaseUnlock"	
database	R	<i>string</i>	

Flags:

- *R*: This field is required. This path must always exists.

Responses:

- InfoSend

Examples:

```
{
  "$type": "DatabaseUnlock",
  "database": "db-main"
}
```

E.1.15 EditAttributeSend *Send the edit of an attribute of an person.*

This sends the the edit of an attribute. If the attribute doesn't exists before it will be creates as long the schema of the user allows it.

Path	Flags	Type/Value	Description
\$type	R	"EditAttributeSend"	
id	R	<i>string</i>	
key	R	<i>string</i>	
value	R	<i>string, number, bool</i>	

Flags:

- *R*: This field is required. This path must always exists.

Responses:

- EditDenied
- EditAccept

Examples:

```
{
  "$type": "EditAttributeSend",
  "id": "#id",
  "key": "abc",
  "value": "abc"
}
```

```
{
  "$type": "EditAttributeSend",
  "id": "#id",
  "key": "abc",
  "value": 3.14
}
```

```
{
  "$type": "EditAttributeSend",
  "id": "#id",
  "key": "abc",
  "value": false
}
```

E.1.16 EditPersonSend *Send the edit of the person*

This sends the the edit of an person. The editable fields are optional. They are only updated if they are set.

Path	Flags	Type/Value	Description
\$type	R	"EditPersonSend"	
id	R	<i>string</i>	
delete		<i>bool</i>	If set to true this will delete this person
name	N	<i>string</i>	
contact	N	<i>string</i>	

Flags:

- *R*: This field is required. This path must always exists.
- *N*: The value of this field can be `null`.

Responses:

- EditDenied
- EditAccept
- SendNotification

Examples:

```
{
  "$type": "EditPersonSend",
  "id": "#id"
}
```

E.1.17 FidoReceive *Receives Information from FIDO USB Token*

Sends the Information from the FIDO USB Token to the server

Path	Flags	Type/Value	Description
\$type	R	"FidoReceive"	
method	R	<i>string</i>	The method that was used for the fido request
value	R		Arbitrary JSON data that was provided from the FIDO USB token

Flags:

- *R*: This field is required. This path must always exists.

Responses:

- FidoResult
- SendNotification

Examples:

```
{
  "$type": "FidoReceive",
  "method": "abc",
  "value": {
    "arbitrary": "data"
  }
}
```

E.1.18 FileChangeConfidential *Change the confidential setting of a single file*

Change the confidential setting of a file or folder. If a file is moved to non-confidential all confidential parent directories are also moved to non-confidential to allow further access to this file after the the confidential database is removed. No other files are touched.

If a folder is moved to confidential all containing files and folders are also moved to confidential.

Path	Flags	Type/Value	Description
\$type	R	"FileChangeConfidential"	
id	R	<i>string</i>	
confidential	R	<i>bool</i>	

Flags:

- *R*: This field is required. This path must always exists.

Responses:

- SendNotification
- FileUpdated

Examples:

```
{
  "$type": "FileChangeConfidential",
```

```

    "id": "#id",
    "confidential": false
  }

```

E.1.19 FileDelete *Deletes file or folder*

Deletes a file or a folder with all containing files. This will mark the files as deleted and they are not really removed from disk.

Path	Flags	Type/Value	Description
\$type	R	"FileDelete"	
id	R	<i>string</i>	

Flags:

- *R*: This field is required. This path must always exists.

Responses:

- SendNotification
- FileUpdated

Examples:

```

{
  "$type": "FileDelete",
  "id": "#id"
}

```

E.1.20 FileFetch *Fetch a single file*

This will fetch a single file by its id

Path	Flags	Type/Value	Description
\$type	R	"FileFetch"	
id	R	<i>string</i>	

Flags:

- *R*: This field is required. This path must always exists.

Responses:

- FileSend

Examples:

```

{
  "$type": "FileFetch",
  "id": "#id"
}

```

E.1.21 FileMove *Move one file to another folder*

Changes the parent directory of one file or folder to a different one. Both the file/folder and the new target has to be attached to the same resource. No circular references are allowed.

Path	Flags	Type/Value	Description
<code>\$type</code>	R	"FileMove"	
<code>id</code>	R	<i>string</i>	
<code>parent</code>	RN	<i>string</i>	

Flags:

- *R*: This field is required. This path must always exists.
- *N*: The value of this field can be [null](#).

Responses:

- SendNotification
- FileMoved

Examples:

```
{
  "$type": "FileMove",
  "id": "#id",
  "parent": "#id"
}
```

E.1.22 FilePersonFetch *Fetch a list of files from an person*

This will send the list of all files attached to an person. If the `root` field is not set it will send all files attached to the root (they have no parent files). Otherwise it will send the direct decendends of this root

Path	Flags	Type/Value	Description
<code>\$type</code>	R	"FilePersonFetch"	
<code>person</code>	R	<i>string</i>	
<code>root</code>	N	<i>string</i>	

Flags:

- *R*: This field is required. This path must always exists.
- *N*: The value of this field can be [null](#).

Responses:

- FilePersonSend

Examples:

```
{
  "$type": "FilePersonFetch",
  "person": "#id"
}
```

E.1.23 FileRename *Rename a file*

Renames an existing file. If the provided name is empty or already used this request is silently ignored. If its succeeds a `file-updated` message will be sent.

Path	Flags	Type/Value	Description
<code>\$type</code>	R	"FileRename"	
<code>id</code>	R	<i>string</i>	
<code>name</code>	R	<i>string</i>	

Flags:

- *R*: This field is required. This path must always exists.

Responses:

- FileUpdated

Examples:

```
{
  "$type": "FileRename",
  "id": "#id",
  "name": "abc"
}
```

E.1.24 InfoRequest *Request the current info from the server*

After the login the ui can request the current information from the server

Path	Flags	Type/Value	Description
<code>\$type</code>	R	"InfoRequest"	

Flags:

- *R*: This field is required. This path must always exists.

Responses:

- InfoSend

Examples:

```
{
  "$type": "InfoRequest"
}
```

E.1.25 PerformReindex *Do a re-index of the database*

Tells the server to start a whole new re-index of all entries in the specified database. This will take a while.

Path	Flags	Type/Value	Description
<code>\$type</code>	R	"PerformReindex"	

Path	Flags	Type/Value	Description
database	R	<i>string</i>	

Flags:

- *R*: This field is required. This path must always exist.

Responses:

- SendNotification

Examples:

```
{
  "$type": "PerformReindex",
  "database": "db-main"
}
```

E.1.26 SchemaRequest *Requests the data of a schema*

The schema needs to be registered at the server before. It is recommended to cache the result because it is unlikely that it will change.

Path	Flags	Type/Value	Description
\$type	R	"SchemaRequest"	
name	R	<i>string</i>	

Flags:

- *R*: This field is required. This path must always exist.

Responses:

- SchemaResponse

Examples:

```
{
  "$type": "SchemaRequest",
  "name": "abc"
}
```

E.1.27 SearchCancel *Cancel a search request*

If the user changes its query or leaves the page the search should be canceled. This is not necessary if the results are already finished.

The server will send a last **SearchResponse** message to notify the cancellation

Path	Flags	Type/Value	Description
\$type	R	"SearchCancel"	
query	R	<i>string</i>	

Path	Flags	Type/Value	Description
uiId	N	<i>string</i>	This is a field that can be set by the UI to identify the messages later.

Flags:

- *R*: This field is required. This path must always exist.
- *N*: The value of this field can be `null`.

Examples:

```
{
  "$type": "SearchCancel",
  "query": "abc"
}
```

E.1.28 SearchSend *Send a new search request to the server*

The search query is a complex string that allows detailed sorting and filtering

Path	Flags	Type/Value	Description
\$type	R	"SearchSend"	
query	R	<i>string</i>	
uiId	N	<i>string</i>	This is a field that can be set by the UI to identify the messages later.

Flags:

- *R*: This field is required. This path must always exist.
- *N*: The value of this field can be `null`.

Responses:

- SearchResponse

Examples:

```
{
  "$type": "SearchSend",
  "query": "abc"
}
```

E.2 SUB /ws/ Operation

The messages that are sent from the server to the UI

Accepts **one of** the following messages:

E.2.1 AccountFidoRequest *Sends a request for the FIDO token*

The UI starts the interaction with a FIDO USB Token using the provided data.

Path	Flags	Type/Value	Description
\$type	R	"AccountFidoRequest"	
command	R	<i>string</i>	
database	R	<i>string</i>	
value	R		The arbitrary data that is forwarded to the fido library

Flags:

- *R*: This field is required. This path must always exists.

Examples:

```
{
  "$type": "AccountFidoRequest",
  "command": "abc",
  "database": "db-main",
  "value": {
    "arbitrary": "data"
  }
}
```

E.2.2 DatabaseAddRequestInfo *Sends info for db creation process*

This message sends the current state of the database creation step.

Path	Flags	Type/Value	Description
\$type	R	"DatabaseAddRequestInfo"	
info	R	<i>object</i>	
info.key	R	<i>string</i>	The key to identify this creation process (the can be multiple ones at the same time).
info.database	R	<i>string</i>	
info.schema	R	<i>string</i>	
info.access	R	<i>array</i>	
info.access[]	R	<i>object</i>	
info.access[] .user	R	<i>string</i>	
info.access[] .user-id	R	<i>string</i> , <guid>	
info.access[] .fido	R	<i>bool</i>	Tells if an FIDO authentication is used for this.
info.access[] .created	R	<i>string</i> , <date-time>	

Flags:

- *R*: This field is required. This path must always exists.

Examples:

```
{
  "$type": "DatabaseAddRequestInfo",
  "info": {
    "key": "abc",
    "database": "db-main",
    "schema": "abc",
    "access": [
      {
        "user": "abc",
        "user-id": "guid",
        "fido": false,
        "created": "2001-01-01T15:17:19.001"
      }
    ]
  }
}
```

E.2.3 DataInterviewAddSend *Add Interview send*

The answer of the server with the created interview

Path	Flags	Type/Value	Description
\$type	R	"DataInterviewAddSend"	
id	R	<i>string</i>	

Flags:

- *R*: This field is required. This path must always exists.

Examples:

```
{
  "$type": "DataInterviewAddSend",
  "id": "#id"
}
```

E.2.4 DataInterviewListPersonSend *Send the list of persons in an interview*

This is the response to the `DataInterviewListPersonRequest` message. This will only contain a partial list. The ui has to merge the results.

There is no last message field. It is possible that responses are sent twice if two requests are sent at the same time.

Path	Flags	Type/Value	Description
\$type	R	"DataInterviewListPersonSend"	
id	R	<i>string</i>	
persons	R	<i>array</i>	
persons[]	R	<i>object</i>	
persons[].id	R	<i>string</i>	
persons[].role	R	<i>string</i>	

Flags:

- *R*: This field is required. This path must always exists.

Examples:

```
{
  "$type": "DataInterviewListPersonSend",
  "id": "#id",
  "persons": [
    {
      "id": "#id",
      "role": "abc"
    }
  ]
}
```

E.2.5 DataInterviewSend *Sends the data of an interview*

This message is a response of `data-interview-get` and will provide the full interview. If no interview was found the `data` field will be null.

Path	Flags	Type/Value	Description
\$type	R	"DataInterviewSend"	
id	R	<i>string</i>	
data	RN	<i>object</i>	
data.id	R	<i>string</i>	
data.database	R	<i>string</i>	
data.created	R	<i>string</i> , <date-time>	
data.modified	R	<i>string</i> , <date-time>	
data.deleted	R	<i>bool</i>	
data.time	R	<i>string</i> , <date-time>	
data.location	R	<i>string</i>	
data.interviewer	R	<i>string</i>	

Flags:

- *R*: This field is required. This path must always exist.
- *N*: The value of this field can be `null`.

Examples:

```
{
  "$type": "DataInterviewSend",
  "id": "#id",
  "data": null
}
```

```
{
  "$type": "DataInterviewSend",
  "id": "#id",
  "data": {
    "id": "#id",
    "database": "db-main",
    "created": "2001-01-01T15:17:19.001",
    "modified": "2001-01-01T15:17:19.001",
    "deleted": false,
    "time": "2001-01-01T15:17:19.001",
    "location": "abc",
    "interviewer": "abc"
  }
}
```

E.2.6 DataPersonAddSend *Add Person send*

The answer of the server with the created person

Path	Flags	Type/Value	Description
\$type	R	"DataPersonAddSend"	
id	R	<i>string</i>	
data	RN	<i>object</i>	
data.id	R	<i>string</i>	
data.database	R	<i>string</i>	
data.created	R	<i>string</i> , <date-time>	
data.modified	R	<i>string</i> , <date-time>	
data.deleted	R	<i>bool</i>	
data.interview	N	<i>string</i>	
data.name	N	<i>string</i>	
data.altName	R	<i>string</i>	

Path	Flags	Type/Value	Description
data.contact	N	<i>string</i>	
data.role	R	<i>string</i>	
data.attributes	R	<i>array</i>	
data.attributes[]	R	<i>object</i>	
data.attributes[].key	R	<i>string</i>	
data.attributes[].created	R	<i>string</i> , <date-time>	
data.attributes[].modified	R	<i>string</i> , <date-time>	
data.attributes[].entries	R	<i>array</i>	the complete history of this attribute
data.attributes[].entries[]	R	<i>object</i>	
data.attributes[].entries[].date	R	<i>string</i> , <date-time>	
data.attributes[].entries[].value	R	<i>string</i> , <i>int</i> , <i>number</i> , <i>bool</i>	
data.attributes[].entry	R	<i>object</i>	
data.attributes[].entry.date	R	<i>string</i> , <date-time>	
data.attributes[].entry.value	R	<i>string</i> , <i>int</i> , <i>number</i> , <i>bool</i>	

Flags:

- *R*: This field is required. This path must always exists.
- *N*: The value of this field can be `null`.

Examples:

```
{
  "$type": "DataPersonAddSend",
  "id": "#id",
  "data": null
}
```

```
{
  "$type": "DataPersonAddSend",
  "id": "#id",
  "data": {
    "id": "#id",
    "database": "db-main",
    "created": "2001-01-01T15:17:19.001",
    "modified": "2001-01-01T15:17:19.001",
    "deleted": false,
    "altName": "abc",
  }
}
```

```

    "role": "abc",
    "attributes": [
      {
        "key": "abc",
        "created": "2001-01-01T15:17:19.001",
        "modified": "2001-01-01T15:17:19.001",
        "entries": [
          {
            "date": "2001-01-01T15:17:19.001",
            "value": "Lorem Ipsum"
          }
        ],
        "entry": {
          "date": "2001-01-01T15:17:19.001",
          "value": "Lorem Ipsum"
        }
      }
    ]
  }
}

```

E.2.7 DataPersonSend *Sends the data of an person*

This message is a response of `data-person-get` and will provide the full person. If no person was found the `data` field will be `null`.

Path	Flags	Type/Value	Description
<code>\$type</code>	R	"DataPersonSend"	
<code>id</code>	R	<i>string</i>	
<code>data</code>	RN	<i>object</i>	
<code>data.id</code>	R	<i>string</i>	
<code>data.database</code>	R	<i>string</i>	
<code>data.created</code>	R	<i>string</i> , <date-time>	
<code>data.modified</code>	R	<i>string</i> , <date-time>	
<code>data.deleted</code>	R	<i>bool</i>	
<code>data.interview</code>	N	<i>string</i>	
<code>data.name</code>	N	<i>string</i>	
<code>data.altName</code>	R	<i>string</i>	
<code>data.contact</code>	N	<i>string</i>	
<code>data.role</code>	R	<i>string</i>	
<code>data.attributes</code>	R	<i>array</i>	
<code>data.attributes[]</code>	R	<i>object</i>	
<code>data.attributes[]</code> <code>.key</code>	R	<i>string</i>	
<code>data.attributes[]</code> <code>.created</code>	R	<i>string</i> , <date-time>	

Path	Flags	Type/Value	Description
data.attributes[].modified	R	<i>string</i> , <date-time>	
data.attributes[].entries	R	<i>array</i>	the complete history of this attribute
data.attributes[].entries[]	R	<i>object</i>	
data.attributes[].entries[].date	R	<i>string</i> , <date-time>	
data.attributes[].entries[].value	R	<i>string</i> , <i>int</i> , <i>number</i> , <i>bool</i>	
data.attributes[].entry	R	<i>object</i>	
data.attributes[].entry.date	R	<i>string</i> , <date-time>	
data.attributes[].entry.value	R	<i>string</i> , <i>int</i> , <i>number</i> , <i>bool</i>	

Flags:

- *R*: This field is required. This path must always exists.
- *N*: The value of this field can be [null](#).

Examples:

```
{
  "$type": "DataPersonSend",
  "id": "#id",
  "data": null
}
```

```
{
  "$type": "DataPersonSend",
  "id": "#id",
  "data": {
    "id": "#id",
    "database": "db-main",
    "created": "2001-01-01T15:17:19.001",
    "modified": "2001-01-01T15:17:19.001",
    "deleted": false,
    "altName": "abc",
    "role": "abc",
    "attributes": [
      {
        "key": "abc",
        "created": "2001-01-01T15:17:19.001",
        "modified": "2001-01-01T15:17:19.001",
        "entries": [
          {
```

```

        "date": "2001-01-01T15:17:19.001",
        "value": "Lorem Ipsum"
    }
],
"entry": {
    "date": "2001-01-01T15:17:19.001",
    "value": "Lorem Ipsum"
}
}
]
}
}

```

E.2.8 DatabaseCreated *Database was created*

Sends that a single database creation process is finished and the database was created.

Path	Flags	Type/Value	Description
\$type	R	"DatabaseCreated"	
id	R	<i>string</i>	The key of the database creation process

Flags:

- *R*: This field is required. This path must always exists.

Examples:

```

{
  "$type": "DatabaseCreated",
  "id": "#id-0123456789abcdef"
}

```

E.2.9 EditAccept *The successful answer of the server of an edit request*

After the client has sent an edit request this will be the answer if the edit was successful

Path	Flags	Type/Value	Description
\$type	R	"EditAccept"	
id	R	<i>string</i>	
key	N	<i>string</i>	Is null if deleted
target	R	<i>string</i> , "Interview", "Person", "Attribute"	

Flags:

- *R*: This field is required. This path must always exists.
- *N*: The value of this field can be [null](#).

Examples:

```
{
  "$type": "EditAccept",
  "id": "#id",
  "target": "Interview"
}
```

```
{
  "$type": "EditAccept",
  "id": "#id",
  "target": "Person"
}
```

```
{
  "$type": "EditAccept",
  "id": "#id",
  "target": "Attribute"
}
```

E.2.10 EditDenied *The edit cannot be done after an edit request*

After the client has sent an edit request which cant be fulfilled this will be the answer.

Path	Flags	Type/Value	Description
\$type	R	"EditDenied"	
id	R	<i>string</i>	
key	N	<i>string</i>	Is null if deleted
target	R	<i>string</i> , "Interview", "Person", "Attribute"	
reasonCode	R	"IdNotFound", "SchemaNotFound", "AttributeNot Available", "Attribute Forbidden", "InvalidValue Type", "Generic"	
reason	R	<i>string</i>	A simple description of this error in english.

Flags:

- *R*: This field is required. This path must always exists.
- *N*: The value of this field can be [null](#).

Examples:

```
{
  "$type": "EditDenied",
  "id": "#id",
  "target": "Interview",
  "reasonCode": "IdNotFound",
  "reason": "abc"
}
```

```
{
  "$type": "EditDenied",
  "id": "#id",
  "target": "Person",
  "reasonCode": "IdNotFound",
  "reason": "abc"
}
```

```
{
  "$type": "EditDenied",
  "id": "#id",
  "target": "Attribute",
  "reasonCode": "IdNotFound",
  "reason": "abc"
}
```

E.2.11 FidoResult *Result of the FIDO request*

Sends the result of the FIDO request to the user

Path	Flags	Type/Value	Description
<code>\$type</code>	R	"FidoResult"	
<code>is-success</code>	R	<i>bool</i>	
<code>error</code>	RN	<i>string</i>	The error message if success is false

Flags:

- *R*: This field is required. This path must always exist.
- *N*: The value of this field can be `null`.

Examples:

```
{
  "$type": "FidoResult",
  "is-success": false,
  "error": null
}
```



```
{
  "$type": "FidoResult",
  "is-success": false,
  "error": "abc"
}
```

E.2.12 FileMoved *Notify about moved files*

Notifies the UI about a moved file or folder.

Path	Flags	Type/Value	Description
\$type	R	"FileMoved"	
id	R	<i>string</i>	
database	R	<i>string</i>	
created	R	<i>string</i> , <date-time>	
modified	R	<i>string</i> , <date-time>	
deleted	R	<i>bool</i>	
person	R	<i>string</i>	
parent	N	<i>string</i>	
name	R	<i>string</i>	
mime	R	<i>string</i>	The MIME type of this file. If this file is a folder the string folder is used instead.
confidential	R	<i>bool</i>	
entries	R	<i>array</i>	the complete history of this file. This is empty if its a folder
entries[]	R	<i>object</i>	
entries[].date	R	<i>string</i> , <date-time>	
entries[].hash	R	<i>string</i>	The Base64 encoded SHA512 Hash of the encrypted file
entries[].exists	R	<i>bool</i>	This flag describes if this file version is on the local disk available and ready for download.
entry	RN	<i>object</i>	the most reason file entry. This is empty for folders
entry.date	R	<i>string</i> , <date-time>	
entry.hash	R	<i>string</i>	The Base64 encoded SHA512 Hash of the encrypted file
entry.exists	R	<i>bool</i>	This flag describes if this file version is on the local disk available and ready for download.

Flags:

- *R*: This field is required. This path must always exist.
- *N*: The value of this field can be `null`.

Examples:

```
{
  "$type": "FileMoved",
  "id": "#id",
  "database": "db-main",
  "created": "2001-01-01T15:17:19.001",
  "modified": "2001-01-01T15:17:19.001",
  "deleted": false,
  "person": "#id",
  "name": "abc",
  "mime": "text/plain",
  "confidential": false,
  "entries": [
    {
      "date": "2001-01-01T15:17:19.001",
      "hash": "abc",
      "exists": false
    }
  ],
  "entry": null
}
```

```
{
  "$type": "FileMoved",
  "id": "#id",
  "database": "db-main",
  "created": "2001-01-01T15:17:19.001",
  "modified": "2001-01-01T15:17:19.001",
  "deleted": false,
  "person": "#id",
  "name": "abc",
  "mime": "text/plain",
  "confidential": false,
  "entries": [
    {
      "date": "2001-01-01T15:17:19.001",
      "hash": "abc",
      "exists": false
    }
  ],
  "entry": {
    "date": "2001-01-01T15:17:19.001",
    "hash": "abc",
    "exists": false
  }
}
```

```

    }
  }

```

E.2.13 FilePersonSend *Send the requested list of file of an person*

Send the list of files that the user has with `file-person-fetch` requested. If no files are found, the root or the person doesn't exists the list will be empty.

Path	Flags	Type/Value	Description
<code>\$type</code>	R	"FilePersonSend"	
<code>person</code>	R	<i>string</i>	
<code>root</code>	RN	<i>string</i>	
<code>data</code>	R	<i>array</i>	
<code>data[]</code>	R	<i>object</i>	
<code>data[].id</code>	R	<i>string</i>	
<code>data[].database</code>	R	<i>string</i>	
<code>data[].created</code>	R	<i>string</i> , <date-time>	
<code>data[].modified</code>	R	<i>string</i> , <date-time>	
<code>data[].deleted</code>	R	<i>bool</i>	
<code>data[].person</code>	R	<i>string</i>	
<code>data[].parent</code>	N	<i>string</i>	
<code>data[].name</code>	R	<i>string</i>	
<code>data[].mime</code>	R	<i>string</i>	The MIME type of this file. If this file is a folder the string <code>folder</code> is used instead.
<code>data[].confidential</code>	R	<i>bool</i>	
<code>data[].entries</code>	R	<i>array</i>	the complete history of this file. This is empty if its a folder
<code>data[].entries[]</code>	R	<i>object</i>	
<code>data[].entries[].date</code>	R	<i>string</i> , <date-time>	
<code>data[].entries[].hash</code>	R	<i>string</i>	The Base64 encoded SHA512 Hash of the encrypted file
<code>data[].entries[].exists</code>	R	<i>bool</i>	This flag describes if this file version is on the local disk available and ready for download.
<code>data[].entry</code>	RN	<i>object</i>	the most reason file entry. This is empty for folders
<code>data[].entry.date</code>	R	<i>string</i> , <date-time>	
<code>data[].entry.hash</code>	R	<i>string</i>	The Base64 encoded SHA512 Hash of the encrypted file
<code>data[].entry.exists</code>	R	<i>bool</i>	This flag describes if this file version is on the local disk available and ready for download.

Flags:

- *R*: This field is required. This path must always exist.
- *N*: The value of this field can be `null`.

Examples:

```
{
  "$type": "FilePersonSend",
  "person": "#id",
  "root": "#id",
  "data": [
    {
      "id": "#id",
      "database": "db-main",
      "created": "2001-01-01T15:17:19.001",
      "modified": "2001-01-01T15:17:19.001",
      "deleted": false,
      "person": "#id",
      "name": "abc",
      "mime": "text/plain",
      "confidential": false,
      "entries": [
        {
          "date": "2001-01-01T15:17:19.001",
          "hash": "abc",
          "exists": false
        }
      ],
      "entry": null
    },
    {
      "id": "#id",
      "database": "db-main",
      "created": "2001-01-01T15:17:19.001",
      "modified": "2001-01-01T15:17:19.001",
      "deleted": false,
      "person": "#id",
      "name": "abc",
      "mime": "text/plain",
      "confidential": false,
      "entries": [
        {
          "date": "2001-01-01T15:17:19.001",
          "hash": "abc",
          "exists": false
        }
      ],
      "entry": {
```

```

    "date": "2001-01-01T15:17:19.001",
    "hash": "abc",
    "exists": false
  }
}
]
}

```

E.2.14 FileSend *Send the requested info of a single file*

Sends the info of a single file if it was requested by an `file-fetch`. If this entry doesn't exists the data field will be null.

Path	Flags	Type/Value	Description
<code>\$type</code>	R	"FileSend"	
<code>id</code>	R	<i>string</i>	
<code>data</code>	RN	<i>object</i>	
<code>data.id</code>	R	<i>string</i>	
<code>data.database</code>	R	<i>string</i>	
<code>data.created</code>	R	<i>string</i> , <date-time>	
<code>data.modified</code>	R	<i>string</i> , <date-time>	
<code>data.deleted</code>	R	<i>bool</i>	
<code>data.person</code>	R	<i>string</i>	
<code>data.parent</code>	N	<i>string</i>	
<code>data.name</code>	R	<i>string</i>	
<code>data.mime</code>	R	<i>string</i>	The MIME type of this file. If this file is a folder the string folder is used instead.
<code>data.confidential</code>	R	<i>bool</i>	
<code>data.entries</code>	R	<i>array</i>	the complete history of this file. This is empty if its a folder
<code>data.entries[]</code>	R	<i>object</i>	
<code>data.entries[] .date</code>	R	<i>string</i> , <date-time>	
<code>data.entries[] .hash</code>	R	<i>string</i>	The Base64 encoded SHA512 Hash of the encrypted file
<code>data.entries[] .exists</code>	R	<i>bool</i>	This flag describes if this file version is on the local disk available and ready for download.
<code>data.entry</code>	RN	<i>object</i>	the most reason file entry. This is empty for folders
<code>data.entry.date</code>	R	<i>string</i> , <date-time>	
<code>data.entry.hash</code>	R	<i>string</i>	The Base64 encoded SHA512 Hash of the encrypted file

Path	Flags	Type/Value	Description
<code>data.entry.exists</code>	R	<i>bool</i>	This flag describes if this file version is on the local disk available and ready for download.

Flags:

- *R*: This field is required. This path must always exists.
- *N*: The value of this field can be `null`.

Examples:

```
{
  "$type": "FileSend",
  "id": "#id",
  "data": null
}
```

```
{
  "$type": "FileSend",
  "id": "#id",
  "data": {
    "id": "#id",
    "database": "db-main",
    "created": "2001-01-01T15:17:19.001",
    "modified": "2001-01-01T15:17:19.001",
    "deleted": false,
    "person": "#id",
    "name": "abc",
    "mime": "text/plain",
    "confidential": false,
    "entries": [
      {
        "date": "2001-01-01T15:17:19.001",
        "hash": "abc",
        "exists": false
      }
    ],
    "entry": null
  }
}
```

```
{
  "$type": "FileSend",
  "id": "#id",
  "data": {
    "id": "#id",
    "database": "db-main",
```

```

    "created": "2001-01-01T15:17:19.001",
    "modified": "2001-01-01T15:17:19.001",
    "deleted": false,
    "person": "#id",
    "name": "abc",
    "mime": "text/plain",
    "confidential": false,
    "entries": [
      {
        "date": "2001-01-01T15:17:19.001",
        "hash": "abc",
        "exists": false
      }
    ],
    "entry": {
      "date": "2001-01-01T15:17:19.001",
      "hash": "abc",
      "exists": false
    }
  }
}

```

E.2.15 FileUpdated *File was updated on the server*

If the user has updated a file with the REST Api the server will send this message after successfull upload.

Path	Flags	Type/Value	Description
\$type	R	"FileUpdated"	
id	R	<i>string</i>	
database	R	<i>string</i>	
created	R	<i>string</i> , <date-time>	
modified	R	<i>string</i> , <date-time>	
deleted	R	<i>bool</i>	
person	R	<i>string</i>	
parent	N	<i>string</i>	
name	R	<i>string</i>	
mime	R	<i>string</i>	The MIME type of this file. If this file is a folder the string folder is used instead.
confidential	R	<i>bool</i>	
entries	R	<i>array</i>	the complete history of this file. This is empty if its a folder
entries[]	R	<i>object</i>	
entries[].date	R	<i>string</i> , <date-time>	

Path	Flags	Type/Value	Description
<code>entries[].hash</code>	R	<i>string</i>	The Base64 encoded SHA512 Hash of the encrypted file
<code>entries[].exists</code>	R	<i>bool</i>	This flag describes if this file version is on the local disk available and ready for download.
<code>entry</code>	RN	<i>object</i>	the most reason file entry. This is empty for folders
<code>entry.date</code>	R	<i>string</i> , <date-time>	
<code>entry.hash</code>	R	<i>string</i>	The Base64 encoded SHA512 Hash of the encrypted file
<code>entry.exists</code>	R	<i>bool</i>	This flag describes if this file version is on the local disk available and ready for download.

Flags:

- *R*: This field is required. This path must always exists.
- *N*: The value of this field can be `null`.

Examples:

```
{
  "$type": "FileUpdated",
  "id": "#id",
  "database": "db-main",
  "created": "2001-01-01T15:17:19.001",
  "modified": "2001-01-01T15:17:19.001",
  "deleted": false,
  "person": "#id",
  "name": "abc",
  "mime": "text/plain",
  "confidential": false,
  "entries": [
    {
      "date": "2001-01-01T15:17:19.001",
      "hash": "abc",
      "exists": false
    }
  ],
  "entry": null
}
```

```
{
  "$type": "FileUpdated",
  "id": "#id",
  "database": "db-main",
  "created": "2001-01-01T15:17:19.001",
```



```

    "modified": "2001-01-01T15:17:19.001",
    "deleted": false,
    "person": "#id",
    "name": "abc",
    "mime": "text/plain",
    "confidential": false,
    "entries": [
      {
        "date": "2001-01-01T15:17:19.001",
        "hash": "abc",
        "exists": false
      }
    ],
    "entry": {
      "date": "2001-01-01T15:17:19.001",
      "hash": "abc",
      "exists": false
    }
  }
}

```

E.2.16 InfoSend *Send the current server info from the server to the ui*

This is send after the `info-request` message

Path	Flags	Type/Value	Description
<code>\$type</code>	R	"InfoSend"	
<code>user</code>	R	<i>string</i>	
<code>database</code>	R	<i>array</i>	
<code>database[]</code>	R	<i>object</i>	
<code>database[].name</code>	R	<i>string</i>	
<code>database[].connected</code>	R	<i>bool</i>	
<code>database[].hasConfidential</code>	R	<i>bool</i>	This flag is only true if the database is connected and the confidential data is available
<code>database[].roleSchema</code>	R	<i>string</i>	
<code>database[].access</code>	R	<i>array</i>	
<code>database[].access[]</code>	R	<i>object</i>	
<code>database[].access[].user</code>	R	<i>string</i>	
<code>database[].access[].user-id</code>	R	<i>string</i> , <guid>	
<code>database[].access[].fido</code>	R	<i>bool</i>	Tells if an FIDO authentication is used for this.
<code>database[].access[].created</code>	R	<i>string</i> , <date-time>	

Path	Flags	Type/Value	Description
database[] .unlocked	RN	<i>string</i> , <date-time>	The timestamp when this access was unlocked.
schemas	R	<i>array</i>	
schemas[]	R	<i>string</i>	
uploadToken	R	<i>string</i>	This upload token is used to verify the author of an upload to the REST Api. This token can be used for the following things: - upload new file - update file - download file

Flags:

- *R*: This field is required. This path must always exists.
- *N*: The value of this field can be [null](#).

Examples:

```
{
  "user": "alice",
  "database": [
    {
      "name": "main",
      "connected": true
    },
    {
      "name": "bob",
      "connected": false
    }
  ],
  "uploadToken": "\u003Cinsert your token here\u003E"
}
```

E.2.17 LoginRequest *Request the UI to show the login box*

The server needs credentials and the user has to login

Path	Flags	Type/Value	Description
\$type	R	"LoginRequest"	
database	R	<i>string</i>	

Flags:

- *R*: This field is required. This path must always exists.

Examples:

```
{
  "$type": "LoginRequest",
  "database": "db-main"
}
```

E.2.18 SchemaResponse *Sends the data of a schema*

This contains the data of the requested schema. If the name was invalid an empty schema will be returned.

Path	Flags	Type/Value	Description
<code>\$type</code>	R	"SchemaResponse"	
<code>name</code>	R	<i>string</i>	
<code>schema</code>	R	<i>array</i>	
<code>schema[]</code>	R	<i>object</i>	
<code>schema[].name</code>	R	<i>string</i>	
<code>schema[].abstract</code>	R	<i>bool</i>	
<code>schema[].parent</code>	RN	<i>string</i>	
<code>schema[].attributes</code>	R	<i>object</i>	
<code>schema[].attributes.*</code>	A	<i>object</i>	
<code>schema[].attributes.*.type</code>	R	<i>string</i>	
<code>schema[].attributes.*.protected</code>	R	<i>bool</i>	
<code>schema[].attributes.*.history</code>	R	<i>bool</i>	

Flags:

- *R*: This field is required. This path must always exist.
- *N*: The value of this field can be [null](#).
- *A*: This is an additional property. You can insert any not previously defined name to add your own properties. The schema of this property is predefined has to be used as above.

Examples:

```
{
  "$type": "SchemaResponse",
  "name": "abc",
  "schema": [
    {
      "name": "abc",
      "abstract": false,
      "parent": null,
      "attributes": {
        "*foo-bar-baz*": {
          "type": "abc",
          "protected": false,
          "history": false
        }
      }
    }
  ]
}
```

```

    }
  },
  {
    "name": "abc",
    "abstract": false,
    "parent": "abc",
    "attributes": {
      "*foo-bar-baz*": {
        "type": "abc",
        "protected": false,
        "history": false
      }
    }
  }
}
]
}

```

E.2.19 SearchResponse *Respond with the search result*

Response with a partial result. The server will continuously send more of these frames if it has more data.

Path	Flags	Type/Value	Description
\$type	R	"SearchResponse"	
query	R	<i>string</i>	
uiId		<i>string</i>	This is an exact copy of the uiId field of SearchSend and only set if it was set in the request.
isLast	R	<i>bool</i>	If this was the last message to this search query this field will be set true .
order	R	<i>int</i>	The internal message order of the server.
elapsed-seconds	R	<i>number</i>	The number of seconds since the start of the execution of the query
sorting	R	<i>array</i>	This object contains the necessary information for the ui to sort all incoming result entries. The entries are listed in their priority. Always sort according the first entry, if that matches according the second entry and so on. This array will never be empty.
sorting[]	R	<i>object</i>	
sorting[].target	R	"None", "Score", "Attribute", "Field"	The kind of target that was sorted here
sorting[].name	RN	<i>string</i>	The name of the target

Path	Flags	Type/Value	Description
sorting[] .direction	R	"Ascending", "Descending"	The direction that should be sorted for
result	R	<i>array</i>	
result[]	R	<i>object</i>	
result[].id	R	<i>string</i>	
result[].database	R	<i>string</i>	
result[].type	R	"Interview", "Person", "File"	
result[].role	RN	<i>string</i>	Only used if type is Person
result[].title	R	<i>string</i>	
result[].sorting	R	<i>array</i>	Contains the values for sorting in the same order as the provided search configuration.
result[] .sorting[]	RN	<i>string, number</i>	Contains the single value for the sortig. This supports the types string and number. If this field doesn't exists for this search result the value is null.
result[].info	R	<i>array</i>	
result[].info[]	R	<i>object</i>	
result[].info[] .name	R	<i>string</i>	
result[].info[] .value	R	<i>string</i>	
result[].found		<i>array</i>	
result[].found[]	R	<i>object</i>	
result[].found[] .field	R	<i>string</i>	
result[].found[] .type	R	"Field", "Attribute"	
result[].found[] .value	R	<i>array</i>	
result[].found[] .value[]	R		
result[].found[] .value[].<0>	C	<i>object</i>	
result[].found[] .value[].<0>.type	R	"Ellipsis"	
result[].found[] .value[].<1>	C	<i>object</i>	
result[].found[] .value[].<1>.type	R	"Context", "Term"	
result[].found[] .value[].<1> .value	R	<i>string</i>	

Flags:

- *R*: This field is required. This path must always exist.
- *N*: The value of this field can be `null`.
- *C*: This is one of multiple choices. You have to select one of the choices.

Examples:

```
{
  "$type": "SearchResponse",
  "query": "abc",
  "isLast": false,
  "order": 42,
  "elapsed-seconds": 3.14,
  "sorting": [
    {
      "target": "Field",
      "name": "Name",
      "direction": "Ascending"
    },
    {
      "target": "Score",
      "name": null,
      "direction": "Descending"
    }
  ],
  "result": [
    {
      "id": "#id",
      "database": "db-main",
      "type": "Person",
      "role": "Doctor",
      "title": "abc",
      "sorting": [
        null,
        "abc",
        3.14
      ],
      "info": [
        {
          "name": "abc",
          "value": "abc"
        }
      ]
    }
  ]
}
```

E.2.20 SendNotification *Sends a user notification*

A mechanism for the server to tell the user about a progress of a state, some information

or errors.

Path	Flags	Type/Value	Description
<code>\$type</code>	R	"Send Notification"	
<code>id</code>	RN	<i>string</i>	The notification id. That is only used if the server intent to update this notification in the future.
<code>img</code>	RN	<i>string</i>	The url of the icon that should be shown. <code>null</code> if no icon should be shown.
<code>title</code>	R	<i>string</i>	
<code>description</code>	R	<i>string</i>	
<code>progress</code>	R	<i>array</i>	
<code>progress.<0></code>	C		Do not show progress at all
<code>progress.<0>[0]</code>	R	"null"	
<code>progress.<1></code>	C		Show a progress but the state is undefined
<code>progress.<1>[0]</code>	R	"undefined"	
<code>progress.<2></code>	C		Show a specific progress state. The value is a number between 0 and 1
<code>progress.<2>[0]</code>	R	"progress"	
<code>progress.<2>[1]</code>	R	<i>number</i>	
<code>close</code>	RN	<i>string</i> , <date-time>	The UTC timestamp when this notification should be closed. <code>null</code> if the notification should be persistent. The server will send an update later to remove it.

Flags:

- *R*: This field is required. This path must always exists.
- *N*: The value of this field can be `null`.
- *C*: This is one of multiple choices. You have to select one of the choices.

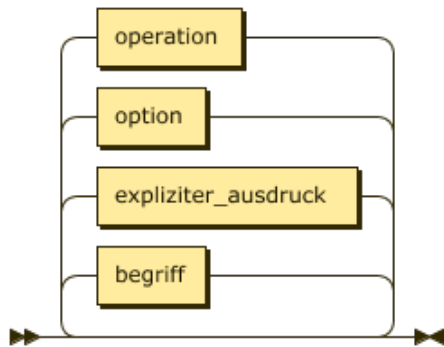
Examples:

```
{
  "$type": "SendNotification",
  "id": null,
  "img": null,
  "title": "Hello World",
  "description": "Have a nice day",
  "progress": [
    "null"
  ],
  "close": "2000-01-01T10:11:12"
}
```

```
{
  "$type": "SendNotification",
  "id": "download-1",
  "img": "/path/to/download/icon.png",
  "title": "Download",
  "description": "cat videos (50%)",
  "progress": [
    "progress",
    0.5
  ],
  "close": null
}
```

```
{
  "$type": "SendNotification",
  "id": "42",
  "img": null,
  "title": "Searching for the Answer of the ...",
  "description": "ultimate Question of Live, the Universe and Everything",
  "progress": [
    "undefined"
  ],
  "close": null
}
```


F Suchquery



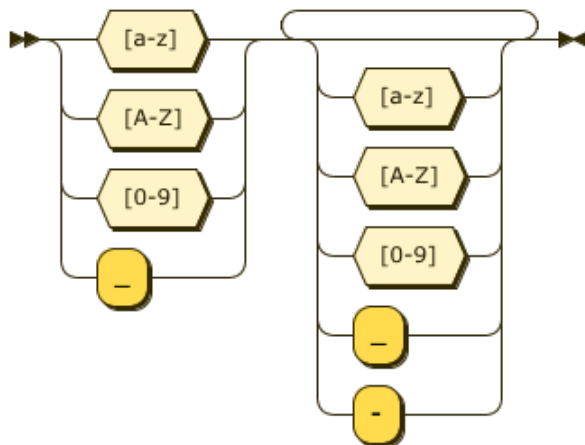
Die Anwendung erlaubt das Eingeben von speziell formatierten Suchanfragen. Diese werden in textueller Form von der Oberfläche aufgenommen, an den Server weitergeleitet, dort ausgewertet und dann die Ergebnisse zurück übermittelt. Diese textuellen Anfragen werden als Suchqueries oder auch kurz Query genannt.

Im folgenden Unterkapiteln wird auf dem Aufbau eines solchen Suchqueries genauer eingegangen.

F.1 Sonderzeichen

Sonderzeichen, sofern sie keine spezielle Syntax bilden werden ignoriert und nicht in die Suche eingeschlossen.

F.2 Begriffe



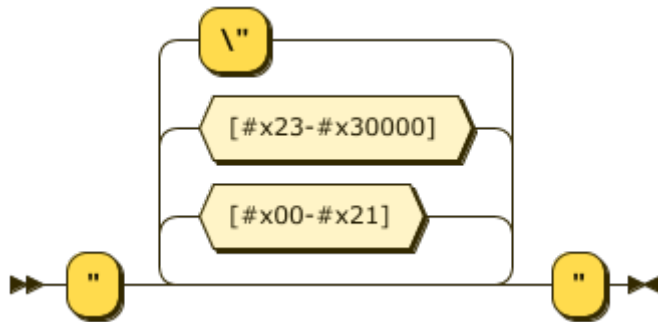
Begriffe werden mit einem Leerzeichen abgetrennt im Query definiert. Begriffe bestehen nur aus Zeichen der Zeichenklasse \w. Bindestriche dürfen zwischendrin vorkommen, aber nicht am Anfang. Groß- und Kleinschreibung wird ignoriert.

Es muss nur ein Begriff aus der Liste von Begriffen passen. Passen mehrere fällt das Ranking besser aus.

Beispiele:

- **Apfel** sucht nach allem, wo Apfel vorkommt
- **Apfel Banane** sucht nach allem, wo entweder Apfel oder Banane vorkommt. Wenn beides vorkommt, so erhält dies eine höhere Priorität

F.3 Explizite Ausdrücke

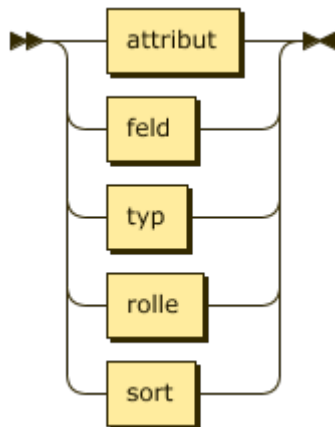


Explizite Ausdrücke werden von doppelten Anführungsstrichen " umschlossen. Alle Zeichen darin werden direkt gesucht und es wird nichts umformatiert. Anführungsstriche werden mit \ " escaped.

Beispiele:

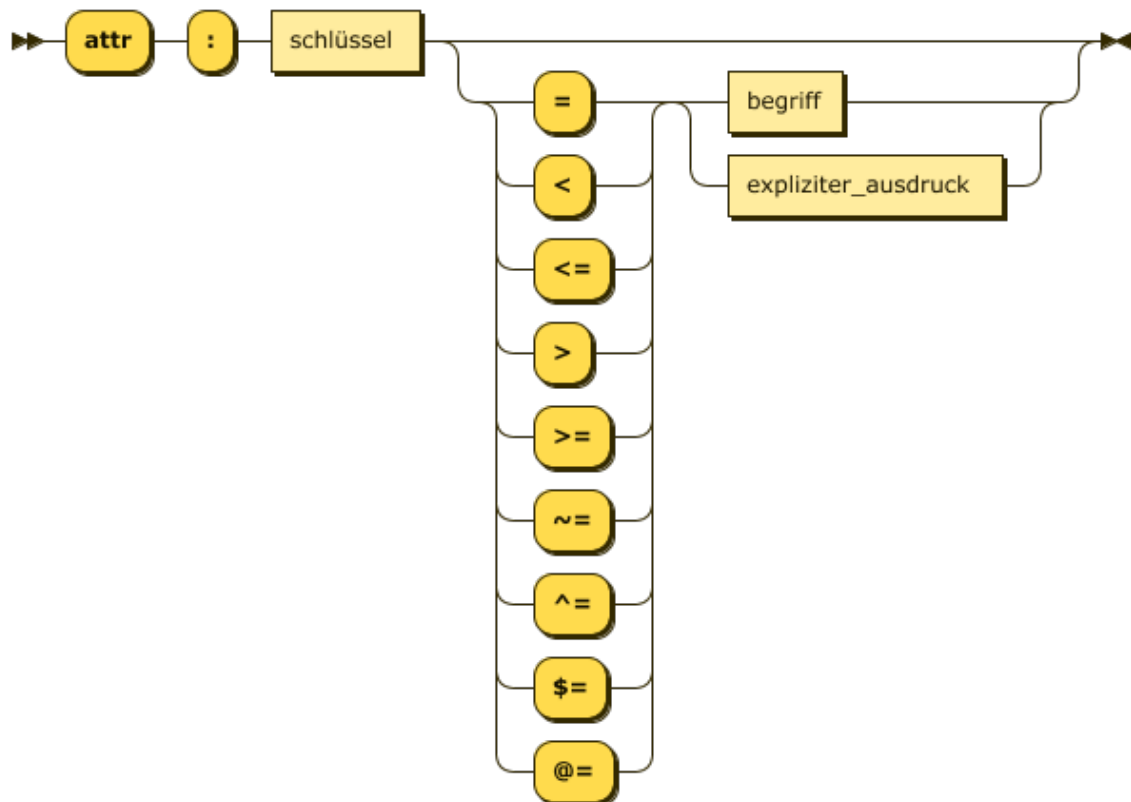
- `Äpfel, Banane"` sucht nach allem, wo der Substring "Äpfel, Banane" in genau dieser Schreibung enthalten ist.

F.4 Optionen



Es gibt verschiedene Optionen. Alle Optionen sind mit dem Schlüssel, einen Doppelpunkt und einen Wert versehen. Wenn Werte Leerzeichen enthalten, müssen diese mit doppelten Anführungsstrichen " umschlossen werden.

F.4.1 Attribute



Sucht direkt nach einem Attribut und vergleicht diesen.

Attribute erzwingen den Typ `person`. Somit sind `type:person attr:age` und `attr:age` äquivalent.

Als Schlüssel für diese Operation gilt `attr`. Danach folgt der Attributsschlüssel, ein Vergleichsoperator und ein Wert.

Folgende Vergleichsoperatoren werden unterstützt:

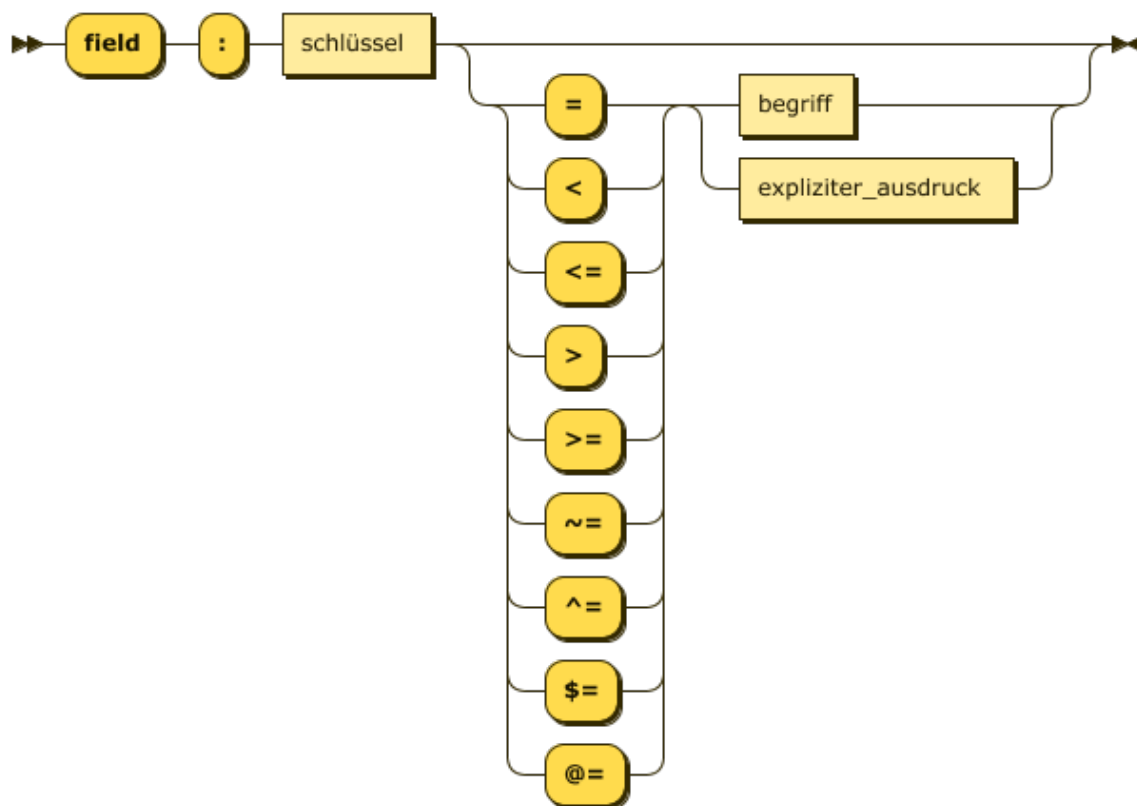
Operator	Wertetyp	Beschreibung
=	alle	Das ganze Attribut muss den Wert entsprechen
<=, <, >=, >	int, float	Mathematischer Vergleichsoperator
~=	string	Attribut muss Wert enthalten
^=	string	Attribut muss mit Wert anfangen
\$=	string	Attribut muss mit Wert aufhören
@=	string	Attribut muss einen Regulären Ausdruck genügen. Wenn dieser Anführungsstriche, Klammern oder Leerzeichen enthält, muss alles in Anführungsstriche gesetzt werden.

Es kann auch der Operator und Wert weggelassen werden, dann wird nur die Existenz des Attributs geprüft.

Beispiele:

- `attr:age>=5` Sucht nach allen Einträgen, dessen Alter gleich oder größer als 5 ist.
- `attr:opinion` Sucht nach allen Einträgen, die einen Wert für `opinion` haben
- `attr:hasConsent=true` Sucht nach allen Einträgen, die einen Consent hinterlegt haben.
- `attr:opinion@="do(es)?n't like m[ae]n"` Sucht nach allen Einträge mit einen Wert für `opinion` welcher einen bestimmten Regulären Ausdruck folgt.

Kann der Vergleichsoperator auf den Wert nicht angewandt werden, so schlägt dieser Teil immer fehl und trifft auf nichts zu. Dasselbe tritt auch ein, wenn der Reguläre Ausdruck fehlerhaft ist.

F.4.2 Felder

Sucht direkt nach einem Feld und vergleicht mit diesen.

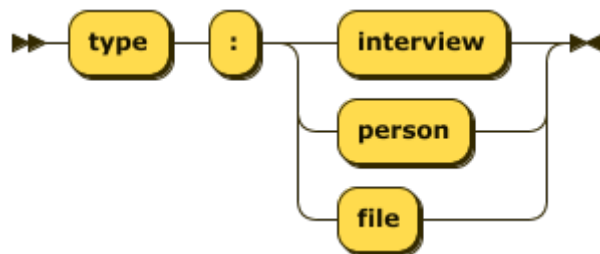
Felder sind äquivalent so aufgebaut wie Attribute und arbeiten ähnlich, bieten aber die gleichen Optionen an.

Felder können bei Interview und Person nur ausgewertet werden, wenn die Confidential Database verfügbar ist. Wenn nicht, schlägt dies immer zwingend fehl. Es können nur bestimmte Felder abgerufen werden:

- **Interview:** time, location, interviewer
- **Person:** name, contact
- **File:** name, kind

Beispiele:

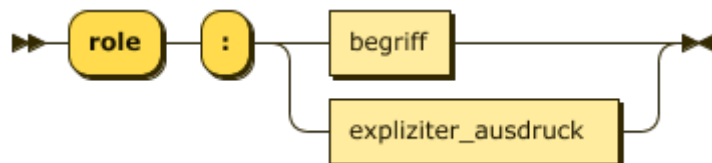
- `field:name~=Ralf` Das Namensfeld enthält "Ralf"

F.4.3 Typ

Sucht nur bestimmte Arten von Datensätzen ab.

Als Schlüssel gilt `type` und als Wert kann eins der folgenden genutzt werden:

Wert	Beispiel	Beschreibung
<code>interview</code>	<code>type:interview</code>	Sucht nur nach Interviews
<code>person</code>	<code>type:person</code>	Sucht nach einer Person
<code>file</code>	<code>type:file</code>	Sucht nach einer Datei (hier werden nur die Metadaten berücksichtigt)

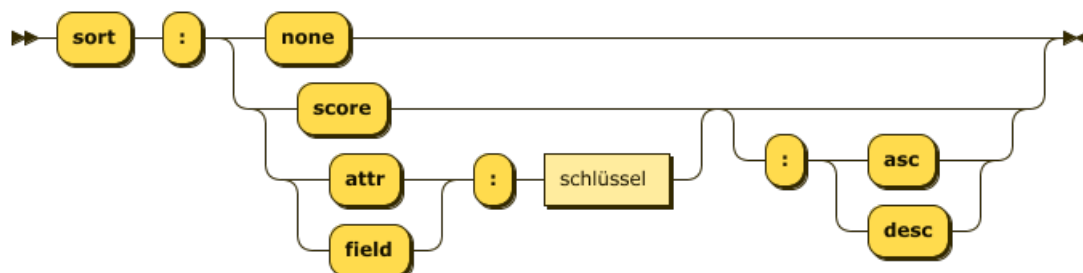
F.4.4 Rolle

Sucht nur noch Interviewten, welche eine Rolle innehaben.

Als Schlüssel gilt `role` und als Wert wird der Schlüssel für die Rolle genutzt:

Beispiel:

- `role:doctor` Sucht nach allen Doktoren
- `role:family` Sucht nach allen Familienmitgliedern

F.4.5 Sortierung

Sortiert die Ergebnisse nach einem bestimmten Feld oder Score:

Sortierungen dürfen nur in der obersten Ebene definiert werden! Andernfalls werden diese ignoriert.

Als Schlüssel gilt hier **sort**. Der Wert ist in mehrere Teile geteilt, welche mit einem Doppelpunkt **:** abgetrennt sind.

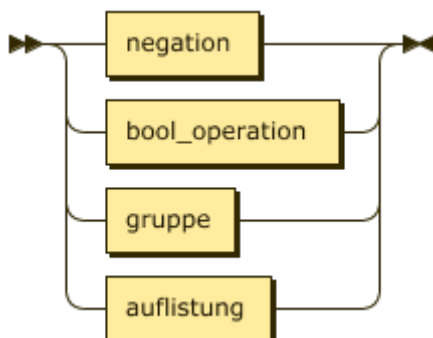
Als erstes kommt hier die Sorte, dann abhängig von der Sorte noch zusätzliche Optionen und zuletzt die Richtung.

Sorte	Extra Feld	Richtung	Beispiel	Beschreibung
score	<i>keins</i>	desc	sort:score:desc	Sortiert anhand des resultierenden Scores.
attr	Schlüssel	asc	sort:attr:age:asc	Sortiert anhand eines Attributes.
field	Schlüssel	asc	sort:field:name:asc	Sortiert anhand eines Standardfelds.
none	<i>keins</i>	<i>egal</i>	sort:none	Sortiert das Ergebnis nicht und gibt sofort alles aus. Dies ist relevant, wenn es schnelle Ergebnisse geht und keine großen Datenmengen erwartet werden.

Falls eine Richtung nicht angegeben wird, so wird die standardmäßige Sortierung für die Sorte genommen.

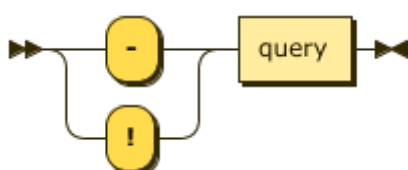
Hinweis: **field** ist bei Interview und Person sind nur verfügbar, wenn die Confidential Database verfügbar ist. Andernfalls wird diese Sortierung immer ignoriert.

F.5 Operatoren



Listen von Wörtern können mit Operatoren versehen werden, wodurch diese nur unter bestimmten Bedingungen erfüllt werden.

F.5.1 Negation



Ein Minus – direkt vor einen Ausdruck (es dürfen beliebig viele Leerzeichen zwischen Minus und Ausdruck stehen) negiert diese Behauptung. Nur solange der interne Ausdruck nicht zutrifft, gilt dies als erfolgreich.

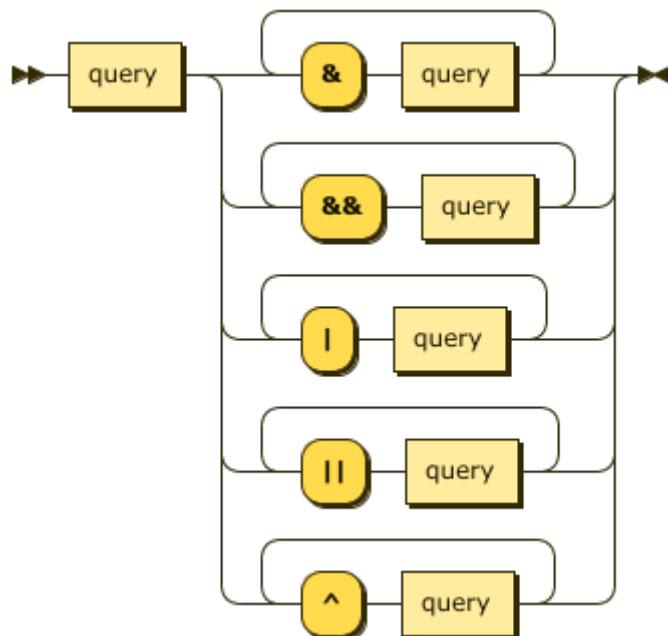
Alternativ zu einen Minus darf auch ein Ausrufezeichen ! verwendet werden.

Folgenden mehrere Negationszeichen aufeinander werden diese solange aufgelöst, bis nur noch eins oder keins mehr übrig ist.

Beispiele:

- `-Apfel` sucht nach allem, was keinen Apfel enthält
- `Apfel - Banane` sucht nach allem was Apfel, aber keine Banane enthält.
- `-!--!Apfel` entspricht `-Apfel`

F.5.2 AND, OR, XOR



Diese Operatoren erlauben komplexere Ausdrücke:

Operator	Beschreibung
<code> </code> oder <code> </code>	Der komplexe Ausdruck trifft nur zu, wenn eine von beiden Seiten zutrifft.
<code>&&</code> oder <code>&</code>	Der komplexe Ausdruck trifft nur zu, wenn beide Seiten zutreffen.
<code>^</code>	Der Ausdruck trifft nur zu, wenn entweder die linke Seite oder die rechte Seite zutrifft. Aber niemals beide gleichzeitig.

Die Operatoren dürfen gemischt werden, hierbei gilt aber folgende Priorität: Zuerst wird `^` ausgewertet, danach `&` und zum Schluss `|`. Falls eine andere Reihenfolge gewünscht ist, so sind Klammern zu verwenden.

Der Unterschied zwischen den einfachen und doppelten Operator ist beim Scoring. Beim doppelten wird nur der größte Score weitergegeben. Wobei beim einfachen die Summe genommen wird. Hierrüber lässt sich also die Priorität in den Suchergebnissen festlegen.

Beispiele:

- `Apfel && Banane` Sucht nach allem, wo Apfel **und** Banane gleichzeitig vorkommen.
- `role:doctor || Doctor` Sucht nach allen mit der Rolle Doktor oder wo das Wort Doktor irgendwo vorkommt.
- `Apfel ^ Banane` Sucht nach allem, wo entweder Apfel oder Banane vorkommt, aber niemals beides gleichzeitig.

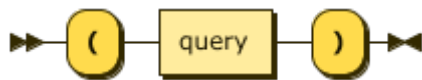
F.5.2.1 Unterschiede bei der Sortierreihenfolge Man nehme an, wir haben folgende Texte, welche in der Datenbank existieren:

- Apfel Kiwi Birne
- Apfel Kiwi
- Apfel Banane Birne Kirsche
- Apfel Kiwi Kirsche

Diese werden je nach Query in einer unterschiedlichen Reihenfolge ausgegeben:

- `(apfel kiwi) | (birne | banane | kirsche):`
 - Apfel Banane Birne Kirsche, Score: 4
 - Apfel Kiwi Birne, Score: 3
 - Apfel Kiwi Kirsche, Score: 3
 - Apfel Kiwi, Score: 2
- `(apfel kiwi) || (birne || banane || kirsche):`
 - Apfel Kiwi Birne, Score: 2
 - Apfel Kiwi, Score: 2
 - Apfel Kiwi Kirsche, Score: 2
 - Apfel Banane Birne Kirsche, Score: 1

F.5.3 Gruppen



Runde Klammern (und) können Listen Wörtern gruppieren und somit komplexere Ausdrücke erstellen.

Falls es nicht genügend schließende Klammern gibt, so wird am Ende aufgefüllt. Gibt es zu viele schließende Klammern, werden diese ignoriert.

Beispiele: - `Apfel && (Banane Kiwi)` Sucht nach allem, wo zwingend ein Apfel vorkommt und mindestens eins von Banane oder Kiwi

F.5.4 Auflistung



Wenn Ausdrücke nur von Leerzeichen begrenzt sind, so werden diese zu Listen zusammengefasst. Diese arbeiten nach speziellen Regeln:

1. Solange keine Optionen enthalten sind, so muss nur eins davon vorkommen. Dies entspräche der Logik, dass `Apfel Banane` und `Apfel | Banane` gleich arbeiten.

2. Wenn mehrere Ausdrücke in einer Auflistung zutreffen, so erhöht sich ihr Score. Bei einer einfachen Kette von `||` bleibt der Score erhalten.
3. Optionen werden in Auflistungen als zwingend angesehen. Die Auflistung kann somit nur noch erfolgreich passen, wenn diese Option erfolgreich ist. Die anderen Ausdrücke behalten ihre Logik bei.

Somit entspräche `role:doctor Doctor House role:doctor && (Doctor House)`.

4. Bei der Abarbeitung werden die Optionen immer zuerst abgearbeitet. Erst dann werden sich die anderen Ausdrücke angeschaut. Hierbei werden auch Gruppen von Klammern beachtet.

Somit entspräche `Doctor House role:doctor (attr:age) role:doctor && (Doctor House (attr:age))`.

Hinweis: Jeder Query ist in einer Auflistung eingeschlossen und auch ein leerer Query ist eine Auflistung. Eine leere Auflistung ist immer Erfolgslos.

`()` entspricht somit nichts, `-()` entspricht somit alles

F.6 Scoring

Es wird bei der Abarbeitung des Query's ein Score ermittelt. Hierbei gelten je nach Ausdruck folgende Regeln:

1. **Begriffe:** Wenn passend, dann 1.0 andernfalls 0.0
2. **Optionen:** Erzwingt das Fehlschlagen oder Erfolgreich sein von Auflistungen.
3. **Operator:**
 1. **Negation:** Wenn interne Ausdruck größer als 0, dann ist das Ergebnis 0.0, andernfalls 1.0
 2. **AND, OR, XOR:**
 - Mit `&`, `|` und `^`: Ergebnis ist Summe von linken und rechten Ausdruck, wenn Ausdruck erfolgreich. Andernfalls 0.0.
 - Mit `&&` und `||`: Ergebnis ist Maximum vom linken und rechten, wenn Ausdruck erfolgreich. Andernfalls 0.0.
 3. **Gruppen:** Der Score ist immer der Score aus der internen Auflistung
 4. **Auflistung:**
 - Wenn einer der Attribute fehlschlägt: 0.0
 - Wenn leer: 0.0
 - Ansonsten Summe der enthaltenden Scorings

F.7 Query-Optimierung

Bevor der Query ausgewertet wird, wird dieser von außen nach innen vereinfacht und somit optimiert. Die Queries werden in folgender Reihenfolge bearbeitet:

1. Wiederholte gleiche Operatoren, werden auf eine Hierarchie gebracht:
 - `apfel && (banane && kiwi)` entspricht `apfel && banane && kiwi`
2. Negation wird aufgelöst:
 - `-!-!-apfel` entspricht `-apfel`
 - `--apfel` entspricht `apfel`
3. Widersprüchliche Attribute werden aufgelöst:
 - `role:doctor role:family apfel` entspricht `()`

- `type:interview` wird zu `()` wenn die Confidential Database nicht mehr verfügbar ist.
 - `type:interview attr:age` entspricht `()`
 - `type:person attr:age` entspricht `attr:age`
4. Verundete Gruppen nur aus Attributen werden zusammengefasst:
 - `(role:doctor) && (attr:age=5)` entspricht `(role:doctor attr:age=5)`
 5. Wenn eine Auflistung nur eine Gruppe enthält, so wird der Inhalt der Gruppe in die Auflistung gezogen:
 - `((apfel banane)))` entspricht `apfel banane`
 - `((role:doctor)))` entspricht `role:doctor`
 - `role:doctor ((attr:age))` entspricht `role:doctor (attr:age)`
 6. Vorauswertung von booleschen Ausdrücken:
 - `apfel && ()` entspricht `()`
 - `apfel && -()` entspricht `apfel`
 - `apfel || ()` entspricht `apfel`

Oder hier noch einmal als übersichtliche Tabelle. `op` steht hierfür für den Operator.

Operator	<code>apfel op ()</code>	<code>apfel op -()</code>
<code>&</code>	<code>()</code>	<code>apfel & -()</code>
<code>&&</code>	<code>()</code>	<code>apfel</code>
<code> </code>	<code>apfel</code>	<code>apfel -()</code>
<code> </code>	<code>apfel</code>	<code>apfel</code>
<code>^</code>	<code>apfel</code>	<code>-apfel</code>

Der Query wird auf unterschiedliche Tabellen ausgeführt, also wird der Query je nach Tabelle noch einmal extra umgebaut:

1. Wenn Confidential Database nicht verfügbar ist, wird folgendes optimiert:
 - `type:interview` zu `()` (immer)
 - `field:name` zu `()` (bei Person Tabelle)
2. Einschränkungen des Typs werden konkretisiert:
 - `type:interview` wird zu `()` bei einer Person Tabelle und zu `-()` bei einer Interview Tabelle
 - `attr:age` wird zu `()` bei einer Interview oder File Tabelle
 - `role:doctor` wird zu `()` bei einer Interview oder File Tabelle
3. Alle oben genannten Optimierungen werden noch einmal geprüft
4. Sortieralternativen werden ausgewertet:
 - `(sort:field:name a | sort:attr:age b)` zu `sort:field:name (a | b)`
 - `(sort:field:name a || sort:attr:age b)` zu `sort:field:name (a || b)`
 - `(sort:field:name a & sort:attr:age b)` zu `sort:field:name sort:attr:age (a & b)`
 - `(sort:field:name a && sort:attr:age b)` zu `sort:field:name sort:attr:age (a && b)`
 - `(sort:field:name a ^ sort:attr:age b)` zu `a ^ b`
5. Unmögliche Sortierungen oder doppelte Sortierungen entfernt:
 - `sort:field:name:asc sort:field:name:desc a` zu `a`
 - `sort:field:name:asc sort:field:name:asc a` zu `sort:field:name:asc a`

Als nächstes werden sich die Optionen auf der obersten Ebene angeschaut. Diese können die Auswahl der Tabellen deutlich einschränken. Außerdem sind diese so strukturiert, dass

sich diese ohne weiteres problemlos auf der Datenbank ausführen lassen.

Danach werden sich die anderen Ausdrücke angeschaut. Für jeden wird separat nach folgenden Regeln entschieden, ob sich dieser auf der Datenbank ausführen lässt:

- Enthält in irgendeiner Tiefe eine Option: Nein
- Enthält in irgendeiner Tiefe eine Auflistung mit mehr als einen Ausdruck: Nein > Hier könnte es Probleme mit dem Scoring geben.
- Enthält in irgendeiner Tiefe den Operator `&` oder `|`: Nein > Auch hier gibt es ein Scoringproblem.

Alles was sich auf der Datenbank ausführen lässt, wird auch auf dieser ausgeführt. Danach geht der Server die restlichen Ausdrücke durch, überprüft diese und berechnet einen Score.

Zum Schluss wird nach den Sortierregeln sortiert. Diese werden nur aus der obersten Ebene genommen und auch in der Reihenfolge abgehandelt. Falls keine Sortierung angegeben ist, so wird nach dem Score absteigend sortiert.

F.8 Beispiele:

Eine Sammlung von komplexen Beispielen:

- `attr:age>=30 attr:age<=50 (field:name sort:field:name || sort:field:age:desc)`

Sucht sich alle Person zwischen 30 und 50 heraus. Solange die Confidential Datenbank noch verfügbar ist, wird nach Namen sortiert, andernfalls nach dem Alter absteigend.

- `(type:interview field:location~=London && field:interviewer~=Bob) || attr:location~=Londyn`

Sucht nach allen Interviews, welche von Bob in London geführt wurden, oder allen Personen, dessen `location` Attribut fälschlicherweise `Londyn` enthält.

- `sort:none We need a pretty long example with many words in it`

Sucht nach allen Datensätzen, welches eins der angegebenen Wörter enthält. Die Sortierung `none` sorgt dafür, dass einfach sofort ausgegeben und nicht gewartet werden soll.

- `"mail@example.com" "http://localhost.de"`

Sucht nach Feldern, wo eine spezifische E-Mail-Adresse oder Link vorkommt. Da diese Sonderzeichen enthalten, müssen diese in doppelten Anführungsstrichen `"` gesetzt werden.

Selbstständigkeitserklärung

Hiermit versichere ich, dass ich die vorliegende Arbeit selbständig verfasst habe, keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe und die allgemeinen Grundsätze guter wissenschaftlicher Praxis beachtet habe.

Halle, 07.07.2022

Ort, Datum

Unterschrift