netidee PROJEKTE

SIKOSI

Endbericht | Call 14 | Projekt ID 4533

Inhalt

1 Einleitung

Ziel des Projektes ist es Client und Server Bibliotheken für Entwickler zur Verfügung zu stellen, die dazu verwendet werden können sichere Systeme zu schaffen. Die Konzeptionsphase wurde erfolgreich abgeschlossen und darauf aufbauend wurden die ersten Prototypen entwickelt. Diese Prototypen befanden sich mehrere Monate in der Evaluierung und wurde auf Schwachstellen überprüft. Der geplante Workshop, bei dem die Prototypen intensiv getestet und Feedback eingeholt wurde, musste Covid-19 bedingt nach hinten verschoben werden und fand dadurch erst Anfang September 2020 statt. Das Feedback und die gefundenen Schwachstellen flossen anschließend in das nächste Arbeitspaket ein, in dem die Software-Module finalisiert und Demo-Projekte erstellt wurden.

2 Projektbeschreibung

Das Ziel von SIKOSI ist die Schaffung von SDKs die von Softwareentwicklern leicht eingebunden werden können. Konkret heißt das, dass SIKOSI als Bibliothek in ein bestehendes Projekt eingebunden werden kann. Sobald dies erfolgt ist, kann SIKOSI beim Datentransport und bei der Datensicherung „zwischengeschaltet“ werden.
Wenn der Datenverkehr in einer Applikation ohne die Berücksichtigung von Sicherheit abläuft bedeutet dies, dass Daten direkt und unverschlüsselt empfangen und versandt werden (siehe Abbildung 1: Ablauf ohne Berücksichtigung von Sicherheit). Potenzielle Angreifer können somit sensible Daten abhorchen, Daten stehlen und diese sogar modifizieren. Ziel ist es, Daten zu schützen und diese nur für befugte Personen zugänglich zu machen. Der Schutz der Daten betrifft folgende Punkte

- Schutz der Daten am Smartphone/PC, damit diese nicht von einer Schad-Software ausgelesen werden können
- Schutz der Daten während der Datenübertragung, damit diese nicht abgehorcht werden können
- Schutz der Daten am Server, damit diese nicht gestohlen und manipuliert werden können

Aus diesem Grund entstand das Projekt SIKOSI, dass Software-Bibliotheken (SDKs) zur Verfügung stellt und somit eine Sicherheits-Schicht bietet, um Daten zu schützen (siehe Abbildung 2: Vergleich des Ablaufs mit SIKOSI).

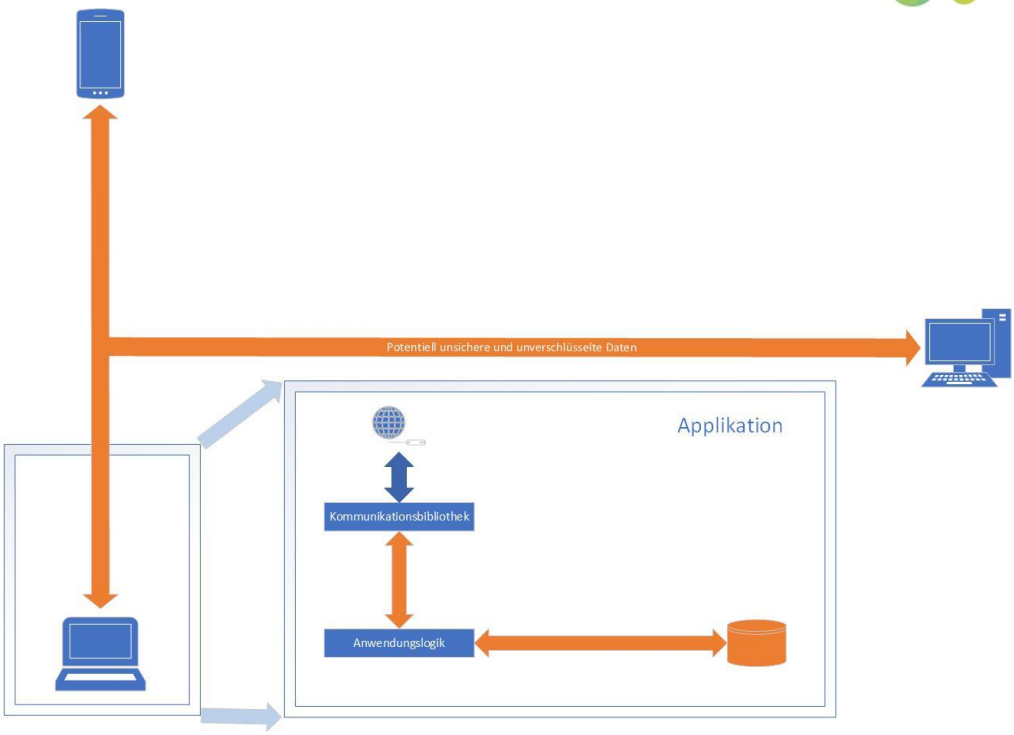

Abbildung 1: Ablauf ohne Berücksichtigung von Sicherheit

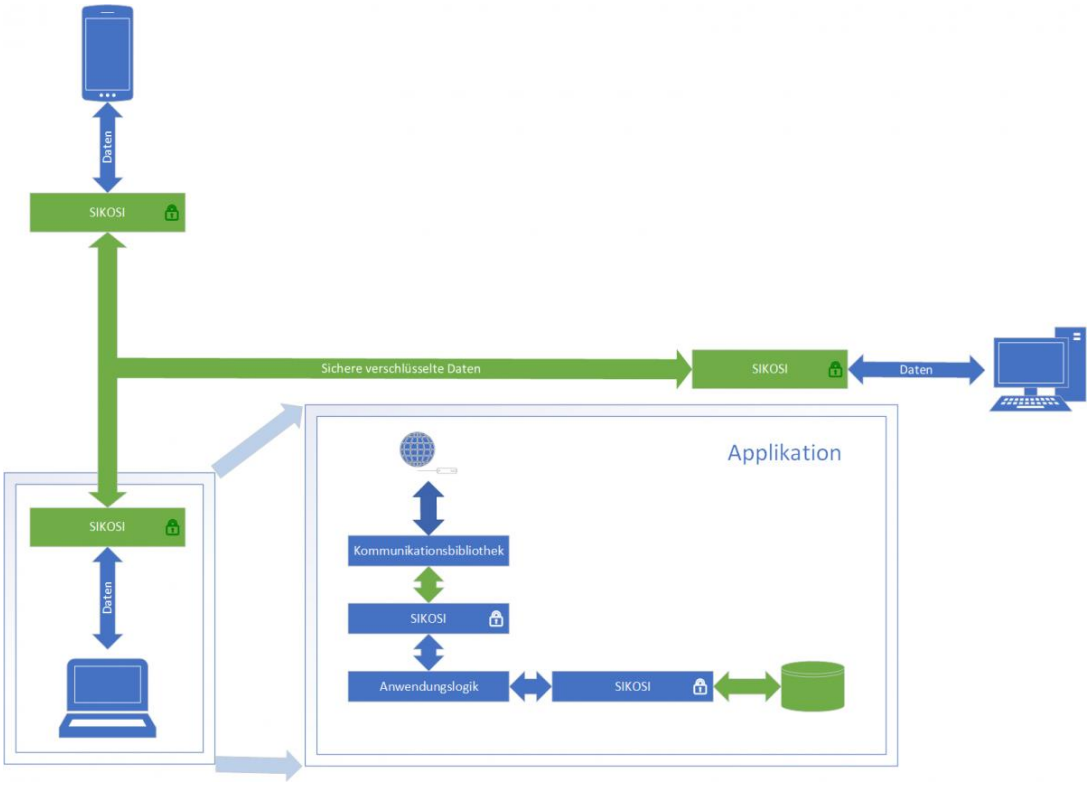

Abbildung 2: Vergleich des Ablaufs mit SIKOSI

Die Wirkung des Projektes für KMUs wäre, dass bewusst auf Sicherheit gesetzt wird und somit sichere Systeme geschaffen werden. Der Schutz der Daten steht im Vordergrund und wirkt somit präventiv für einen Datenmissbrauch. Im Bereich der DSGVO kann ein Nachweis der Sicherheitscheckliste und der angewandten Sicherheitstechnologien im Extremfall von Nutzen sein.

Entwickler bekommen SDKs zur Verfügung gestellt, die einfach in bestehende oder neue Systeme integriert werden können. Diese SDKs sind mit State-of-the-Art Technologie ausgestattet, die transparent überprüft werden können. Eine weitere positive Wirkung ist, dass von Beginn an nach dem Motto „Security First“ auf Sicherheit in Systemen gesetzt werden kann.

Der Open-Source Community ist die Transparenz des Systems nach dem Motto "YKWYG - You know what you get" überaus wichtig. Da das Projekt Open-Source ist, können sämtliche Verfahren aufgerufen und auch verbessert oder angepasst werden. Durch die Einsparung an Zeit, die zum Thema Sicherheit enorm sein kann, kann der Fokus gezielt auf andere Arbeitsschritte gelegt werden.

Folgende Projektergebnisse wurden realisiert:

- Client Bibliothek
- Server Bibliothek
- Demo-Projekt Client Software
- Demo-Projekt Server Software
- Checkliste für die Erstellung sicherer Systeme

Die erstellten Bibliotheken sollen einfach in neue oder bestehende Systeme integriert werden können. Die Demo-Projekte dienen in erster Linie Evaluierungszwecken und bieten Entwicklern eine gute Vorlage wie die SDKs eingebunden und verwendet werden können.

Das System stellt somit einen Mehrwert für Entwickler dar, da diese ohne viel Aufwand nach dem Ansatz „Security First“ vorgehen können. Dadurch profitieren auch die Benutzer von mit SIKOSI entwickelten Applikationen, da sie sich in Bezug auf Datensicherheit auf das System verlassen können.

SDKs Client

Hier sind Software Bibliotheken zu finden, die Daten sicher ver- und entschlüsseln können. Des Weiteren stehen SW-Bibliotheken zur Verfügung, um sich gegen einen Server zu authentifizieren um anschließend Schnittstellen (Funktionen) vom Server aufrufen zu können, die eine Autorisierung verlangen.

SDKs Server

Hier sind Software Bibliotheken zu finden, die Daten sicher ver- und entschlüsseln können. Des Weiteren befinden sich in den Bibliotheken Funktionen um Daten verschlüsselt in einem Speicher (wie z.B. eine Datenbank) abzuspeichern und diese nur für Personen zugänglich und lesbar zu machen, die dazu autorisiert sind. Auch stehen in den Bibliotheken Verfahren zur Verfügung, um Benutzer zu registrieren, zu authentifizieren und Schnittstellen zu schützen.

Demo Projekte Client & Demo Projekte Server

Hier befinden sich eine Vielzahl an Demoprojekten, die eine sinnvolle Verwendung der Bibliotheken zeigen und nachvollziehbar macht. Diese dienen entweder als Ausgangsbasis für neue Entwicklungen oder dienen als Nachschlagewerk um die Bibliotheken in eigenen Projekten einbinden zu können.

Exchange

Hier befinden sich Bibliotheken, die gemeinsam von Server und Client verwendet werden. Überwiegend sind dies Datenaustausch-Klassen, in denen Strukturen definiert sind, die für den Datenaustausch zwischen Client und Server benötigt werden.

Code-Dokumentation und Code-Qualität

Ein wichtiger Punkt ist es, dass der entwickelte Code eine sehr gute Qualität aufweist. Wir achten hier darauf, dass jede Klasse, jede Methode und komplexe Codestellen bereits im Quellcode dokumentiert und kommentiert sind. Sämtliche Lösungsansätze können somit einfach nachvollzogen werden. Wir verwenden hier zusätzliche externe Tools, um den Code auf Qualität zu überprüfen.

3 Verlauf der Arbeitspakete

3.1 Arbeitspaket 1 - *Detailplanung und Formales am Projektstart*

Diese Arbeitspaket wurde erfolgreich abgeschlossen.

3.2 Arbeitspaket 2 - *Konzeptphase und Recherche*

Dieses Arbeitspaket wurde erfolgreich abgeschlossen.

Dieses Arbeitspaket war insofern wichtig, um sich einen guten Überblich über bestehende Technologien zu verschaffen und Ziele konzeptionell abstecken zu können. Da EntwicklerInnen im Fokus stehen, wurden Interviews durchgeführt, um genauer auf die Bedürfnisse dieser Zielgruppe eingehen zu können.

Folgende Hauptpunkte wurden in diesem Arbeitspaket behandelt:

- Detaillierte Interviews mit Entwicklern
- Definition der Sicherheitsniveau-Matrix
- Definition der Clientfunktionalität im Hinblick auf eine große Reichweite
- Sammlung von Informationen und Technologien von sicherer End-Zu-End Kommunikation und Speicherung von Daten

- Ermittlung verwendbarer Technologien im Hinblick eins Krypto-Systems
- Evaluierung der zu verwendenden Open Source Algorithmen und Bibliotheken
- Erstellung einer Systemarchitektur

Folgende Ergebnisse wurde in diesem Arbeitspaket erreicht

- Technisches Konzept für Softwaremodule
- Systemarchitektur
- Sicherheitsniveau-Matrix

Eine große Herausforderung bei diesem Arbeitspaket war die Menge an Informationen, die in diversen Büchern und Online zur Verfügung stehen. Diese Informationen mussten auf Aktualität und dem Stand der Technik entsprechend gefiltert werden.

3.3 Arbeitspaket 3 - *Prototypische Entwicklung der Software-Module*

Dieses Arbeitspaket wurde erfolgreich abgeschlossen.

Aufbauend auf dem Konzept wurden server- und clientseitige Prototypen entwickelt. Wichtig bei SW-Projekten ist es, von Beginn an eine geeignete Struktur zu definieren, um den Überblick zu behalten und Softwareteile anschließend richtig abzulegen. Diese Struktur wurde definiert und hat sich bewährt.

Folgende Hauptpunkte wurden in diesem Arbeitspaket behandelt

- Projektanlage, Software Projekt aufsetzen
- Implementierung SW-Modul Client
- Implementierung SW-Modul Server
- Implementierung SW-Client
- Implementierung SW-Server

Folgende Ergebnisse wurden in diesem Arbeitspaket erreicht

- SW-Modul für Client in einer Erstversion vorhanden
- SW-Modul für Server in einer Erstversion vorhanden
- SW-Client für Evaluierungszwecke vorhanden
- SW-Server für Evaluierungszwecke vorhanden

Abweichungen zum Plan gab es bezüglich des Enddatums des Arbeitspaket, welches sich Covid-19 bedingt nach hinten verschoben hat.

Erfolgserlebnisse gab es hier, da nach der langen Konzept- und Coding-Phase erste greifbare Ergebnisse sichtbar wurden. Dies stellt insofern einen Erfolg dar, da sich die monatelange Arbeit bezahlt macht.

3.4 Arbeitspaket 4 - *Validierung, Workshop, Schwachstellenanalyse, Erstellung von Checklisten*

Dieses Arbeitspaket wurde erfolgreich abgeschlossen.

Der Workshop musste wie bereits erwähnt verschoben werden und fand Anfang September statt.

Folgende Arbeiten wurden durchgeführt

- Evaluierung der Prototypen
- Evaluierung der finalen Software
- Überprüfung der SW-Module, SW-Client und SW-Server auf Schwachstellen
- Workshop
- Erstellung von Checklisten für die Entwicklung sicherer Systeme

Durch die regelmäßigen Evaluierungen wurde auch die Software sukzessive verbessert.

3.5 Arbeitspaket 5 - *Finalisierung der Software-Module, Erstellung von Templates*

Dieses Arbeitspaket wurde erfolgreich abgeschlossen.

Folgende Arbeiten wurden durchgeführt

- Einarbeitung der Erkenntnisse aus den Evaluierungen und dem Workshop
- Beheben der Schwachstellen
- Verbesserung und Finalisierung der SW-Module (Client und Server)
- Verbesserung und Finalisierung des SW-Client und des SW-Server

3.6 Arbeitspaket 6 - *Fortlaufende Dokumentation und Projektmanagement*

Dieses Arbeitspaket wurde erfolgreich abgeschlossen

- Entwicklerdokumentation wurde erstellt
- Anwenderdokumentation wurde erstellt
- Einseitiges Dokument für Veröffentlichungen wurde erstellt
- "Lessions Learned" - Externe Kommunikation wurde erstellt
- Blogeinträge wurden erstellt

Seitens Projektmanagement wurden alle Punkte abgeschlossen.

3.7 Arbeitspaket 7 - *Dokumentation und Formales am Projektende*

Dieses Arbeitspaket wurde erfolgreich abgeschlossen

4 Umsetzung Förderauflagen

Nicht zutreffend.

5 Liste Projektendergebnisse

1	*Projektzwischenbericht*	*CC-BY Sharelike-3.0 AT*	*https://www.netidee.at/sikosi*
2	*Projektendbericht*	*CC-BY Sharelike-3.0 AT*	*https://www.netidee.at/sikosi*
3	*Entwickler_innen-DOKUMENTATION*	*CC-BY Sharelike-3.0 AT*	*https://www.netidee.at/sikosi*
4	*Anwender_innen-DOKUMENTATION*	*CC-BY Sharelike-3.0 AT*	*https://www.netidee.at/sikosi*
5	*Veröffentlichungsfähiger Einseiter*	*CC-BY Sharelike-3.0 AT*	*https://www.netidee.at/sikosi*
6	*Externendokumentation*	*CC-BY Sharelike-3.0 AT*	*https://www.netidee.at/sikosi*
7	*SW-Modul Client* *.NET Standard Bibliothek und Templates (plattformunabhängig)* *o) Bibliothek die in Clients integriert werden kann* *o) Verschlüsselung und Entschlüsselung von Daten*	*GPL V3*	*https://github.com/FotecGmbH/SIKOSI*
8	*SW-Modul Server* *.NET Standard Bibliothek (plattformunabhängig)* *o) Bibliothek kann in Serverapplikationen integriert werden* *o) Standardisierte APIs* *o) Sichere Speicherung von Daten*	*GPL V3*	*https://github.com/FotecGmbH/SIKOSI*

9	*SW-Client* *Demoprojekt* *o) Beispielhafte Einbindung der Bibliotheken* *o) Kann für Evaluierungen verwendet werden*	*GPL V3*	*https://github.com/FotecGmbH/SIKOSI*
10	*SW-Cloud* *Demoprojekt* *o) Beispielhafte Einbindung der Bibliotheken* *o) Kann für Evaluierungen verwendet werden*	*GPL V3*	*https://github.com/FotecGmbH/SIKOSI*
11	*Konzept* *o) Systemarchitektur* *o) Verwendbare Technologien im Hinblick auf ein Krypto-System* *o) Serverfunktionalität im Hinblick auf Zukunftsträchtig und Plattformunabhängigkeit* *o) Clientfunktionalität im Hinblick auf eine große Reichweite* *o) Sichere Speicherung von Daten* *o) Sichere End-zu-End Kommunikation* *o) Sicherheitsniveaumatrix*	*CC-BY Sharelike-3.0 AT*	*https://www.netidee.at/sikosi*
12	*Checkliste für die Entwicklung sicherer Systems* *Erleichtert die Entwicklung und soll Hilfe dabei verschaffen nichts zu vergessen*	*CC-BY Sharelike-3.0 AT*	*https://www.netidee.at/sikosi*

6 Verwertung der Projektergebnisse in der Praxis

Die Checkliste erweist sich als außerordentlich praktisch und wurde bereits an Interessenten weitergegeben. Durch den Fokus auf das Thema Sicherheit wurde das Grundgerüst für eine Applikation geschaffen, die sich aktuell noch in der Entwicklung befindet und sich mit dem Thema „Hilfe bei psychischen Problemen“ auseinandersetzt. Diese Applikation bietet eine Plattform für Betroffene, die sich gegenseitig austauschen und Hilfe erhalten wollen. Dies ist ein plakatives Beispiel, da sich Betroffene sicher fühlen wollen, wenn sie vertraute Nachrichten über das Internet senden, die nur für einen bestimmten Empfänger bestimmt sind. Mit den entwickelten SDKs wird diese Sicherheit ermöglicht.

7 Öffentlichkeitsarbeit/ Vernetzung

Das Projekt wurde bei öffentlichen Veranstaltungen folgender Kooperationen vorgestellt

- DIH-OST – Digital Innovation Hub OST
- HDD – Haus der Digitalisierung

8 Eigene Projektwebsite

Nicht zutreffen.

9 Geplante Aktivitäten nach netidee-Projektende

Die Software wird auf „GitHub“ publiziert und kann somit durch eine Open Source Community weiterentwickelt werden. Die entwickelten Software Bibliotheken werden in verschiedenen Systemen integriert und getestet. Feedback von Forschungsunternehmen und Entwicklern, die Interesse an der Verwendung eines solchen Systems zeigen, wird gesammelt und nach Projektende einer erneuten Förderung zugeführt. An dieser Stelle ist anzumerken, dass erst die erwarteten Projektergebnisse wirtschaftsnahe Förderschienen, wie FTI, CDP, ABC ermöglichen. Konkret würde sich für FOTEC als Partner beim Austrian Blockchain Center ist, ein ABC Projekt mit einem österreichischen Unternehmen anbieten. Unabhängig davon werden die Projektergebnisse in jedem Fall über folgende Schienen disseminiert:

- Dataskop
- Open^3 Toolbox
- HDD – Haus der Digitalisierung
- ABC – Austrian Blockchain Center
- CDP – Center for Digital Production
- Improve! – Interreg Digitalisierungsprojekt AT/HU Pannonian Business Network, Sopron Uni, am-Lab, Pannon Uni, Campus02, Profactor, FOTEC
- DihOST – Digital Innovation Hub Ostösterreich FH St. Pölten, IMC FH Krems, FOTEC, Forschung Burgenland

Des Weiteren werden die entwickelten Software-Bibliotheken in realen Anwendungen, die seitens FOTEC entwickelt werden, eingebunden und somit Erfahrungen in einer realen Umgebung gesammelt.

Insbesondere werden sich nach Projektende weitere Anforderungen und Arbeitsschwerpunkte ergeben, da es zum Thema Sicherheit immer wieder neue Lücken auftauchen, die geschlossen werden müssen.

10 Anregungen für Weiterentwicklungen durch Dritte

Ein großer erster Schritt wurde bereits getätigt und die Bibliotheken bietet eine gute Ausgangsbasis für zukünftige Entwicklungen. Aus aktueller Sicht ist man für zukünftige Entwicklungen gut aufgestellt. Das Thema Sicherheit muss immer im Auge behalten werden, dadurch sollte man auch nicht immer auf Dritt-Komponenten verlassen, sondern diese stets kritisch hinterfragen.