Gesicherte Datenablage Server Client Anwendung

Einleitung

Eine gesicherte Datenablage für den Sicheren Austausch von Dateien.

Dabei wird die Privatsphäre der User und ein besonderes Augenmerk auf die Sicherheit gelegt. Die Anwendung soll Client und Serveranwendung basiert sein.

Ein besonderes Augenmerk soll auf die Verschlüsselung gelegt werden. Zum einen werden die Daten Symmetrisch verschlüsselt, aber auch asymmetrische Verschlüsslung ist im Einsatz.

Jede Client Anwendung generiert einen symmetrischen Schlüssel bei der erst Initiation der Applikation.

Jeder User bekommt auch auf dem Server einen eigenen symmetrischen Schlüssel auf dem Server, welcher Die Daten ein zweites Mal verschlüsselt.

Die Authentifikation erfolgt über eine zwei Stufen Identifikation.

Der Token wird verwendet um den wechsel der SSL-keys zu initieren bei der übertragung der Dateien.

Bei der Arbeit wird nach IPERKA vorgegangen.

Information

Dokumente zu diesem Auftrag:

Praktische Prüfung Aspekte einer Business Anwendung (1).pdf

Aspekte einer Business Anwendung Auftrag 1.pdf

Wie kann man Dateien Aufsplitten in Java?

Read line funktioniert bei grösseren Dateien. Jedoch bei Dateien die kleiner sind wird es Probleme geben.

Bei kürzeren Files könnte man einen String Split benutzen (Weniger als 8 Zeilen)

"Randomisierte" Übertragung der Pakete und wieder Zusammensetzung von diesen?

Könnte über Token vermischt werden.

Wie können multiple SSL-Schlüssel verwendet werden?

Der Token wird zusammen mit der Zeit Gehasht und dabei kann man eine Unterteilung generieren.

Der Token wurde vom Server generiert und ist daher auf beiden Seiten vorhanden.

Technische Rahmenbedingungen

Es soll eine Datenübertragung Applikation entstehen, welche die Kunden Daten Sicher überträgt und verwahrt.

Der Serverbetreiber hat keinen direkten Zugriff auf die Daten.

Sicherheitslücken

Kunden können sich registrieren und einen Account eröffnen. (Es wird ein Aktivierungs-Key verwendet für die erst Serververbindung)

Die Daten des Benutzers werden Symmetrisch verschlüsselt hierbei wird das Passwort, der Username so wie der Aktivierung Key verwendet.

Die Daten können vom Kunden eingesehen, uploadet und gedownloadet werden.

Der Computer mit der Server Applikation soll regelmässig update erfahren und Virengescannt werden.

Bereits bei der Entwicklung sollen Test zur Sicherheit implementiert werden.

Libraries sind aktuell und bei dem Aufwand der Weiterentwicklung mit einzuberechnen.

Zur nach Vollziehbarkeit der Zugriffe wird ein Log implementiert.

Die Passwörter der User werden nur gehasht abgelegt.

Die Passwörter müssen mindestens 15 Stellen lang sein, Ein Kleinbuchstaben, einem Grossbuchstaben enthalten, mindestens eine Zahl so wie ein Sonderzeichen enthalten.

Risiken

Bei Verlust des User Passworts wird ein Recovery implementiert.

Der User soll nur eine sehr begrenztes GUI zur Anzeige der Uploadeten Daten und zum Uploaden der Daten haben.

Des Weiteren hat er eine Login- so wie eine Logout-Funktion haben.

Bei Technischem Versagen soll die Applikation nach einem Neustart wieder einsetzbar sein.

Zum Schutz gegen höhere Gewalt sollen Regelmässige Backups des Systems erstellt werden.

Arbeitsjournal 15.03.2022

Die Plannung hat weitaus mehr Zeit eingenommen als erwartet.

Es konnte jedoch schon eine Kleiner Teil der Realisierung umgesetzt werden.

Es wurden die Klasse für die SSH Key Generation erstellt, so wie der Generation.

Die Apsekte und der Ausbau von element so wie die Formen der Verschlüsselung sind leicht Problematisch.

Arbeitsjournal 22.03.2022

Ausarbeitung der Datenübertragung für die Wahl der