Implementierung einer Smartphone-Anwendung zum Austausch verschlüsselter Daten mit einer Cloud

1. Juli 2014

Inhaltsverzeichnis

Teil I.

Einleitung

0.1. Motivation

Am Deutschen Elektronen Synchrotron, im folgenden DESY, werden bisher wichtige und sensible Dokumente über ein Programm Namens Dropbox gesichert und verwaltet. Dropbox bietet eine Plattformunabhänginge Möglichkeit Dokuente Online abzuspeichern und von jedem anderen Standort über ein internetfähiges Gerät die Daten wieder zu öffnen [https://www.dropbox.com/]. Auch wenn Dropbox nach eigenen Angaben den Advanced Encryption Standard (AES) verwendet, bevor die Daten gespeichert werden, liegen die dafür notwendigen Schlüssel in Händen der Betreiber selbst, die somit vollen Klartextzugriff auf die Nutzerdateien haben.

Das DESY in Hamburg ist sehr daran bestrebt die erhobenen Daten in Ihrer eigenen Cloud abzusichern und gegen Fremdzugriff zu schüten. Da das DESY über eine eigene Cloud-Infrastruktur verfügt, sollen in Zukunft alle wichtigen Daten nicht nur in dieser Cloud gespeichert werden, sondern auch zusätzlich durch eine Verschlüsselung gesichert werden.

0.2. Zielsetzung

Ziel dieser Arbeit ist es aus diesem Grund einen Prototyp zu entwickeln, der einerseits mit dem Cloud-System des DESY Kommunizieren kann um dort Dateien hoch- und herunter zu laden, andererseits diese Daten auch in angemessener Form (siehe Kapitel Validierung) zu Verschlüsseln.

In der ersten Version dieser Arbeit wird ein Programm ausschließlich für das Betriebssystem Android entwickelt.

1. Verwandte Arbeiten

2. Verwandte Programme

3. Diese Arbeit

3.1. Inhaltlicher Aufbau

3.2. Veränderung ggü. Anforderung

Teil II.

Grundlagen

4. Android

4.1. Zusammenhang Kryptographie

4.1.1. OpenSSL

5. Kryptographie

5.1. Grundlagen

5.2. Verschlüsselung

5.2.1. Symetrische Verfahren

5.2.2. Asymetrische Verfahren

5.3. Hash-Funktionen

5.4. Digitale Signature

5.4.1. Public Key Infrastruktur

5.5. Schlüsselvereinbarung

5.5.1. Diffie Hellmann

5.5.2. ElGamal

5.6. Schlüsselgenerierung

5.7. Authentifizierung

5.7.1. Zwei-Faktor-Authentifizierung

Teil III.

Validierung

6. Verschlüsselungsverfahren

7. Hashfunktionen

Teil IV.

Implementierung

8. Entwurf

Teil V.

Test

9. Validierung

10. Testverfahren

Teil VI.

Zusammenfassung und Ausblick

11. Zusammenfassung

12. Ausblick