

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

30. Juni 2014

Inhaltsverzeichnis

I. Einleitung	3
1. Motivation	4
2. Zielsetzung	5
3. Verwandte Arbeiten	6
4. Diese Arbeit	7
4.1. Inhaltlicher Aufbau	7
4.2. Veränderung ggü. Anforderung	7
II. Grundlagen	8
5. Android	9
5.1. Zusammenhang Kryptographie	9
6. Kryptographie	10
6.1. Grundlagen	10
6.2. Verschlüsselung	10
6.2.1. Symetrische Verfahren	10
6.2.2. Asymetrische Verfahren	10
6.3. Hash-Funktionen	10
6.4. Digitale Signature	10
6.4.1. Public Key Infrastruktur	10
6.5. Schlüsselvereinbarung	10
6.5.1. Diffie Hellmann	10
6.5.2. ElGamal	10
6.6. Schlüsselgenerierung	10
III. Validierung	11
6.7. Verschlüsselungsverfahren	12
6.8. Hashfunktionen	12

IV. Implementierung	13
6.9. Entwurf	14
V. Test	15
6.10. Validierung	16
6.11. Testverfahren	16
VI. Zusammenfassung und Ausblick	17
6.12. Zusammenfassung	18
6.13. Ausblick	18

Teil I.

Einleitung

1. Motivation

2. Zielsetzung

TODO: Dieser Block ist eventuell mit in Motivation enthalten

3. Verwandte Arbeiten

4. Diese Arbeit

4.1. Inhaltlicher Aufbau

4.2. Veränderung ggü. Anforderung

Teil II.

Grundlagen

5. Android

5.1. Zusammenhang Kryptographie

6. Kryptographie

6.1. Grundlagen

6.2. Verschlüsselung

6.2.1. Symmetrische Verfahren

6.2.2. Asymmetrische Verfahren

6.3. Hash-Funktionen

6.4. Digitale Signature

6.4.1. Public Key Infrastruktur

6.5. Schlüsselvereinbarung

6.5.1. Diffie Hellmann

6.5.2. ElGamal

6.6. Schlüsselgenerierung

Teil III.

Validierung

6.7. Verschlüsselungsverfahren

6.8. Hashfunktionen

Teil IV.

Implementierung

6.9. Entwurf

Teil V.

Test

6.10. Validierung

6.11. Testverfahren

Teil VI.

Zusammenfassung und Ausblick

6.12. Zusammenfassung

6.13. Ausblick