

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

30. Juni 2014

# Inhaltsverzeichnis

<b>I. Einleitung</b>	<b>4</b>
1. Motivation	5
2. Zielsetzung	6
3. Verwandte Arbeiten	7
4. Diese Arbeit	8
4.1. Inhaltlicher Aufbau . . . . .	8
4.2. Veränderung ggü. Anforderung . . . . .	8
<b>II. Grundlagen</b>	<b>9</b>
5. Android	10
5.1. Zusammenhang Kryptographie . . . . .	10
6. Kryptographie	11
6.1. Grundlagen . . . . .	11
6.2. Verschlüsselung . . . . .	11
6.2.1. Symetrische Verfahren . . . . .	11
6.2.2. Asymetrische Verfahren . . . . .	11
6.3. Hash-Funktionen . . . . .	11
6.4. Digitale Signature . . . . .	11
6.4.1. Public Key Infrastruktur . . . . .	11
6.5. Schlüsselvereinbarung . . . . .	11
6.5.1. Diffie Hellmann . . . . .	11
6.5.2. ElGamal . . . . .	11
6.6. Schlüsselgenerierung . . . . .	11
<b>III. Validierung</b>	<b>12</b>
6.7. Verschlüsselungsverfahren . . . . .	13
6.8. Hashfunktionen . . . . .	13

<b>IV. Implementierung</b>	<b>14</b>
6.9. Entwurf . . . . .	15
<b>V. Test</b>	<b>16</b>
6.10. Validierung . . . . .	17
6.11. Testverfahren . . . . .	17
<b>VI. Zusammenfassung und Ausblick</b>	<b>18</b>
6.12. Zusammenfassung . . . . .	19
6.13. Ausblick . . . . .	19

Teil I.

Einleitung

# 1. Motivation

## 2. Zielsetzung

### 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

## 7. Verschlüsselungsverfahren

## 8. Hashfunktionen

# Teil IV.

## Implementierung

## 9. Entwurf



Teil V.

Test

## 10. Validierung

## 11. Testverfahren

## Teil VI.

# Zusammenfassung und Ausblick

## 12. Zusammenfassung

## 13. Ausblick