Hochschule Offenburg
offenburg.university

E+I Elektrotechnik und Informationstechnik

Generic Cryptographic Interface

Documentation Steve Wagner

December 17, 2015

Laboratory for Embedded Systems and Communication Electronics
Hochschule Offenburg
Prof. Axel Sikora
Andreas Walz

Statutory declaration

I declare that I have authored this thesis independently, that I have not used other than the declared sources / resources, and that I have explicitly marked all material which has been quoted either literally or by content from the used sources.

Offenburg, _____ _____

Date Signature

Abstract

Contents

1 Introduction

2 Motivation

3 Design

4 Initialisation of the interface

5 Context management

5.1 Creation of a context

5.1.1 Hash context

5.1.2 Signature (for generating) context

5.1.3 Signature (for verifying) context

5.1.4 Cipher context

5.1.5 Diffie-Hellmann context

5.2 Clonin of an existing context

5.2.1 Hash context

5.2.2 Both signature context

5.3 Deletin of an existing context

6 Hash functions

6.1 Algorithm of hash

6.2 Steps to hash

7 Signature algorithms

7.1 Signature configuration

7.1.1 RSA

7.1.2 Digital Signature Algorithm (DSA)

7.1.3 Elliptic Curve Digital Signature Algorithm (ECDSA)

7.1.4 Block-Cipher-Based Message Authentication Code (CBC-MAC / CMAC)

7.1.5 keyed-Hash Message Authentication Code (HMAC)

7.2 Steps to sign

8 Generation of key pair

8.1 Configuration of a key pair

8.1.1 RSA

8.1.2 Digital Signature Algorithm (DSA)

8.1.3 Elliptic Curve Digital Signature Algorithm (ECDSA)

8.2 Steps to generate a key pair

9 Cipher algorithms

9.1 Configuration of a symmetric cipher

9.2 Configuration of an asymmetric cipher

9.3 Encrypt a plaintext

9.4 Decrypt a ciphertext

10 Generation of Diffie-Hellmann key pair

10.1 Configuration of a Diffie-Hellmann key pair

10.1.1 Diffie-Hellmann (DH)

10.1.2 Elliptic Curve Diffie Hellmann (ECDH)

10.2 Steps to generate a Diffie-Hellmann key pair

11 Calculation of a Diffie-Hellmann shared secret

11.1 Steps to calculate a shared secret

12 Pseudo-Random Number Generator

12.1 Generation of a pseudo-random number

12.2 Seed a pseudo-random number

13 Key management

13.1 Saving of a key as a big number and get an ID

13.2 Getting of a saved key with his ID

13.3 Deleting a key

Bibliography

[1] Christof Paar and Jan Pelzl. *Understanding cryptography: a textbook for students and practitioners*. Springer Berlin Heidelberg, Berlin; Heidelberg [u.a.], 2. corr. printing edition, 2010.