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 Learning of the cryptographic and TLS's protocols basis

1.1 Handshake Protocol

1.2 Cryptographic parts in the Handshake Protocol

2 Creation of the Generic Cryptographic Interface

2.1 Principe of context

2.2 Key management

2.3 Principal functions needed in the interface

2.3.1 Hash

2.3.2 Signature

2.3.3 Generate key pairs

2.3.4 Diffie-Hellmann

2.3.5 Cipher

2.3.6 Pseudo-random number generator

3 Implementation of the new interface in embetterTLS's project

3.1 old embetterTLS VS new embetterTLS

3.2 CryptoWrap Interface to Generic Crypto Interface

4 Implementation of LibTomCrypt in the new interface for embetterTLS

4.1 embetterTLS as client

4.2 embetterTLS as server

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.

[2] Ph.D. Rolf, Oppliger. *SSL and TLS: Theory and Practice*. Artech House, eSECURITY Technologies; Beethovenstrasse 10; CH-3073; Gümligen; Switzerland, 2009.