

Generic Cryptographic Interface

Documentation Steve Wagner

December 16, 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,

Datum

Unterschrift

Abstract

Contents

1	Initialisation of the interface	1
2	Context management	2
2.1	Creation of a context	2
2.1.1	Hash context	2
2.1.2	Signature (for generating) context	2
2.1.3	Signature (for verifying) context	2
2.1.4	Cipher context	2
2.1.5	Diffie-Hellmann context	2
2.2	Clone an existing context	2
2.2.1	Hash context	2
2.2.2	Both signature context	2
2.3	Delete an existing context	2
3	Hash	3
3.1	Algorithm of hash	3
3.2	Steps to hash	3
4	Signature	4
4.1	Signature configuration	4
4.1.1	RSA	4
4.1.2	Digital Signature Algorithm (DSA)	4
4.1.3	Elliptic Curve Digital Signature Algorithm (ECDSA)	4
4.1.4	Block-Cipher-Based Message Authentication Code (CBC-MAC / CMAC)	4
4.1.5	keyed-Hash Message Authentication Code (HMAC)	4
4.2	Steps to sign	4
5	Generate key pair	5
5.1	Configuration of a key pair	5
5.1.1	RSA	5
5.1.2	Digital Signature Algorithm (DSA)	5
5.1.3	Elliptic Curve Digital Signature Algorithm (ECDSA)	5
5.2	Steps to generate a key pair	5
6	Cipher	6
6.1	Configuration of a symmetric cipher	6
6.2	Configuration of an asymmetric cipher	6
6.3	Encrypt a plaintext	6
6.4	Decrypt a ciphertext	6

7	Generate Diffie-Hellmann key pair	7
7.1	Configuration of a Diffie-Hellmann key pair	7
7.1.1	Diffie-Hellmann (DH)	7
7.1.2	Elliptic Curve Diffie Hellmann (ECDH)	7
7.2	Steps to generate a Diffie-Hellmann key pair	7
8	Calculate a Diffie-Hellmann shared secret	8
8.1	Steps to calculate a shared secret	8
9	Pseudo-Random Number Generator	9
9.1	Generate a pseudo-random number	9
9.2	Seed a pseudo-random number	9
10	Key management	10
10.1	Save a key as big number and get an ID	10
10.2	Get a saved key with his ID	10
10.3	Delete a key	10

1 Initialisation of the interface

2 Context management

2.1 Creation of a context

2.1.1 Hash context

2.1.2 Signature (for generating) context

2.1.3 Signature (for verifying) context

2.1.4 Cipher context

2.1.5 Diffie-Hellmann context

2.2 Clone an existing context

2.2.1 Hash context

2.2.2 Both signature context

2.3 Delete an existing context

3 Hash

3.1 Algorithm of hash

3.2 Steps to hash

4 Signature

4.1 Signature configuration

4.1.1 RSA

4.1.2 Digital Signature Algorithm (DSA)

4.1.3 Elliptic Curve Digital Signature Algorithm (ECDSA)

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

4.1.5 keyed-Hash Message Authentication Code (HMAC)

4.2 Steps to sign

5 Generate key pair

5.1 Configuration of a key pair

5.1.1 RSA

5.1.2 Digital Signature Algorithm (DSA)

5.1.3 Elliptic Curve Digital Signature Algorithm (ECDSA)

5.2 Steps to generate a key pair

6 Cipher

6.1 Configuration of a symmetric cipher

6.2 Configuration of an asymmetric cipher

6.3 Encrypt a plaintext

6.4 Decrypt a ciphertext

7 Generate Diffie-Hellmann key pair

7.1 Configuration of a Diffie-Hellmann key pair

7.1.1 Diffie-Hellmann (DH)

7.1.2 Elliptic Curve Diffie Hellmann (ECDH)

7.2 Steps to generate a Diffie-Hellmann key pair

8 Calculate a Diffie-Hellmann shared secret

8.1 Steps to calculate a shared secret

9 Pseudo-Random Number Generator

9.1 Generate a pseudo-random number

9.2 Seed a pseudo-random number

10 Key management

10.1 Save a key as big number and get an ID

10.2 Get a saved key with his ID

10.3 Delete a key