Certification Report

Buheita Fujiwara, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	2006-08-30 (ITC-6096)
Certification No.	C0107
Sponsor	Stiftung Secure Information and Communication Technologies SIC
Name of TOE	IAIK-JCE CC Core
Version of TOE	3.15
PP Conformance	None
Conformed Claim	EAL3
Developer	Stiftung Secure Information and Communication Technologies SIC
Evaluation Facility	TÜV Informationstechnik GmbH, Evaluation Body for IT-Security

This is to report that the evaluation result for the above TOE is certified as follows.
2007-06-27

Haruki Tabuchi, Technical Manager
Information Security Certification Office
IT Security Center

Evaluation Criteria, etc.: This TOE is evaluated in accordance with the following criteria prescribed in the "IT Security Evaluation and Certification Scheme".

- Common Criteria for Information Technology Security Evaluation Version 2.3 (ISO/IEC 15408:2005)
- Common Methodology for Information Technology Security Evaluation Version 2.3 (ISO/IEC 18045:2005)

Evaluation Result: Pass

"IAIK-JCE CC Core" has been evaluated in accordance with the provision of the "IT Security Certification Procedure" by Information-technology Promotion Agency, Japan, and has met the specified assurance requirements.

Notice:
This document is the English translation version of the Certification Report published by the Certification Body of Japan Information Technology Security Evaluation and Certification Scheme.

Table of Contents

1. Executive Summary

1.1 Introduction

This Certification Report describes the content of certification result in relation to IT Security Evaluation of "IAIK-JCE CC Core" (hereinafter referred to as "the TOE") conducted by TÜV Informationstechnik GmbH, Evaluation Body for IT-Security (hereinafter referred to as "Evaluation Facility"), and it reports to the sponsor, Stiftung Secure Information and Communication Technologies SIC.

The reader of the Certification Report is advised to read the corresponding ST and manuals (please refer to "1.5.9 Documents Attached to Product" for further details) attached to the TOE together with this report. The assumed environment, corresponding security objectives, security functional and assurance requirements needed for its implementation and their summary specifications are specifically described in ST. The operational conditions and functional specifications are also described in the document attached to the TOE.

Note that the Certification Report presents the certification result based on assurance requirements conformed to the TOE, and does not certify individual IT product itself.

Note: In this Certification Report, IT Security Evaluation Criteria and IT Security Evaluation Method prescribed by IT Security Evaluation and Certification Scheme are named CC and CEM, respectively.

1.2 Evaluated Product

1.2.1 Name of Product

The target product by this Certificate is as follows:

Name of Product:	IAIK-JCE CC Core
Version:	3.15
Developer:	Stiftung Secure Information and Communication Technologies SIC

1.2.2 Product Overview

The TOE, the library IAIK-JCE CC Core, version 3.15, is a pure Java™ software delivered to users as part of a toolkit. This toolkit consists of a Java library in form of JAR (Java Archive) files, documentation and demo code. The TOE provides components usable to develop applications including functionality to create and verify digital signatures, to encrypt and to decrypt data, and to generate random numbers.

The IAIK-JCE CC Core is a set of APIs and implementations of cryptographic functionality, including:

- hash functions
- signature schemes
- block ciphers
- stream ciphers
- asymmetric ciphers
- message authentication codes

• random number generators

1.2.3 Scope of TOE and Overview of Operation

The TOE is software which is conformant to the Java Cryptographic Architecture (JCA) and Java Cryptographic Extensions (JCE) frameworks, implements a Cryptographic Service Provider as defined in the JCA and JCE. The boundary of the TOE is "IAIK Cryptography Provider" shown in Figure 1 below, and cryptographic functions (SHA-1、SHA-256、SHA-384、SHA-512、RIPEMD-160、HMAC、RSA Signature、RSA Cipher、AES、Triple-DES、RC2、ARCFOUR、Secure Random) directly under that.

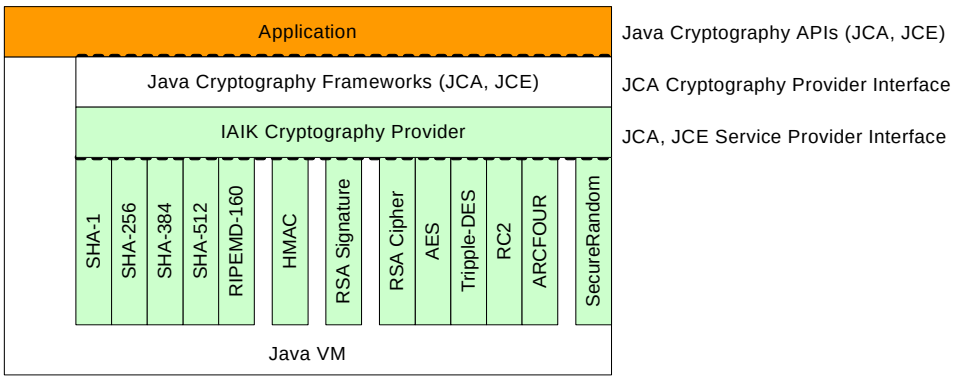

Figure 1-1 The TOE and its environment

Applications access the TOE through JCA/JCE framework and the TOE supplies them cryptographic functions as mentioned and figured above like SHA-1, AES, etc. Details of functions offered by the TOE are explained in the next chapter.

1.2.4 TOE Functionality

The TOE supplies functions mentioned above in 1.2.3 Figure 1, which are defined as TOE security functions.

a) Hash related functionality
The TOE implements following hash algorithms:

- SHA-1 [FIPS PUB 180-1]
- Ripemd-160 [ISO/IEC 10118-3]
- SHA-256 [FIPS PUB 180-2]
- SHA-384 [FIPS PUB 180-2]
- SHA-512 [FIPS PUB 180-2]

b) MAC related functionality
The TOE creates message authentication code according to HMAC algorithm. HMAC uses following algorithms:

- SHA-1 [FIPS PUB 180-1]
- Ripemd-160 [ISO/IEC 10118-3]
- SHA-256 [FIPS PUB 180-2]
- SHA-384 [FIPS PUB 180-2]
- SHA-512 [FIPS PUB 180-2]

Applications must supply secret keys which conform {(128 + k * 8) bit ≤ blocksize of the

used hash function, with [k=0,1,2,...]}. The TOE supports smaller keys, too, but they are not suitable to be used under "SOF-High" environment claimed by the TOE.

c) Digital Signature related functionality
The TOE performs the creation and authentication of electronic signatures according to following electronic signature scheme:

- RSA with SHA-1, SHA-256, SHA-384, SHA-512 or RIPEMD-160 according to [PKCS#1v1.5], with key lengths of 1024 + k * 64 [k=0,1,2,...] bit. The maximum key size is 8192 bit.
- RSA-PSS with SHA-1, SHA-256, SHA-384, SHA-512 or RIPEMD-160 according to [PKCS#1v2.1], with key lengths of 1024 + k * 64 [k=0,1,2,...] bit. The maximum key size is 8192 bit.

The TOE supports smaller keys, too, but they are not suitable to be used under "SOF-High" environment claimed by the TOE.

d) Encryption functionality
The TOE implements following block cipher:
- AES 128, 192, 256 bit [FIPS PUB 197]
- Triple-DES 112, 168 bit [FIPS 46-3]
- RC2 128-1024 bit [RFC 2268]

These block ciphers are available under following operation modes:
- ECB
- CBC
- OFB
- CFB

In case of AES, CTR is also supported.

The TOE implements following stream cipher:
- ARCFOUR 128 – 2048 bit according to [IETF-Draft-Kaukonen]. This algorithm is assumed to be compatible with RC4TM from RSA Security Inc.

The TOE implements following asymmetric cryptography:
- RSA 1024 + k * 64 [k=0,1,2,...] bit according to [PKCS#1v1.5]. The maximum key size is 8192 bit.
- RSA-OAEP 1024 + k * 64 [k=0,1,2,...] bit according to [PKCS#1v2.1]. The maximum key size is 8192 bit.

The TOE supports smaller keys, too, but they are not suitable to be used under "SOF-High" environment claimed by the TOE.

e) Random Number Generator related functionality
The TOE implements two (2) random number generators based on the following hash algorithms:
- SHA-1 [FIPS PUB 180-1]
- Ripemd-160 [ISO/IEC 10118-3]
- SHA-256 [FIPS PUB 180-2]
- SHA-384 [FIPS PUB 180-2]
- SHA-512 [FIPS PUB 180-2]

When random number is generated, the functionality must be initialized by seeds which have suitable entropies.

1.3 Conduct of Evaluation

Based on the IT Security Evaluation/Certification Program operated by the Certification Body, TOE functionality and its assurance requirements are being evaluated by evaluation facility in accordance with those publicized documents such as "IT Security Evaluation and Certification Scheme"[2], "IT Security Certification Procedure"[3] and "Evaluation Facility Approval Procedure"[4].

Scope of the evaluation is as follow.

- Security design of the TOE shall be adequate;
- Security functions of the TOE shall be satisfied with security functional requirements described in the security design;
- This TOE shall be developed in accordance with the basic security design;
- Above mentioned three items shall be evaluated in accordance with the CC Part 3 and CEM.

More specific, the evaluation facility examined "IAIK-JCE CC Core Security Target" as the basis design of security functions for the TOE (hereinafter referred to as "the ST")[1], the evaluation deliverables in relation to development of the TOE and the development, manufacturing and shipping sites of the TOE. The evaluation facility evaluated if the TOE is satisfied both Annex B of CC Part 1 (either of [5], [8] or [11]) and Functional Requirements of CC Part 2 (either of [6], [9] or [12]) and also evaluated if the development, manufacturing and shipping environments for the TOE is also satisfied with Assurance Requirements of CC Part 3 (either of [7], [10] or [13]) as its rationale. Such evaluation procedure and its result are presented in "EVALUATION TECHNICAL REPORT (ETR)" (hereinafter referred to as "the Evaluation Technical Report") [17]. Further, evaluation methodology should comply with the CEM (either of [14], [15] or [16]).

1.4 Certification

The Certification Body verifies the Evaluation Technical Report prepared by the evaluation facility and evaluation evidence materials, and confirmed that the TOE evaluation is conducted in accordance with the prescribed procedure. Certification review is also prepared for those concerns found in the certification process. Evaluation is completed with the Evaluation Technical Report dated 2007-06 submitted by the evaluation facility and those problems pointed out by the Certification Body are fully resolved and confirmed that the TOE evaluation is appropriately conducted in accordance with CC and CEM. The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by the evaluation facility and concluded fully certification activities.

1.5 Overview of Report

1.5.1 PP Conformance

There is no PP to be conformed.

1.5.2 EAL

Evaluation Assurance Level of TOE defined by this ST is EAL3 conformance.

1.5.3 SOF

This ST claims “SOF-High” as its minimum strength of function.

The security policy of the TOE is aimed to provide secure encrypting function. It is, therefore, necessary for the TOE to claim “SOF-High”.

1.5.4 Security Functions

All functions supplied by the TOE are security functions which are described in 1.2.4 TOE Functionality.

1.5.5 Threat

The TOE assumes following threats presented in Table 1-1 below, and provides functions for countermeasure against them.

Table 1-1 Assumed Threats

Identifier	Threats
T.SignatureForgery	S.Attacker could forge O.Signature or recover O.PrivateKey From O.Signature.
T.DeduceData	S.Attacker could deduce O.Data from O.CipherText.
T.DeduceKey	S.Attacker could deduce O.SecretKey from O.CipherText.
T.DeduceRandomSeed	S.Attacker could deduce O.RandomSeed.
T.PredictRandomNumber	S.Attacker could predict the next generated O.RandomNumber.
T.MACForgery	S.Attacker could forge O.MAC or recover O.SecretKey.
T.HashForgery	S.Attacker could find collisions to O.Hash.

Definitions of Subject (S.Attacker, etc) and Object (O.Signature, etc) are listed below in Table 1-2-1 and Table 1-2-2 respectively.

Table 1-2-1 Definitions of Subject

Subject	Definition
S.Admin	User who is in charge to perform the TOE installation and TOE configuration.
S.Developer	User who is in charge to use the TOE for developing his Application (S.Application).
S.Application	The surrounding application which is using the TOE.
S.JavaVM	Java™ Virtual Machine.

S.Attacker	A human or a process outside the TOE whose main goal is to access Application sensitive information. For functions with SOF-high claim the attacker has a high attack potential and no time limit. For all other functions the TOE has no obvious vulnerabilities that are exploitable by attackers possessing low attack potential.

Table 1-2-2 Definitions of Object

Object	Definition
O.Data	Private data obtained from the S.Application (e.g. Data to be signed).
O.MAC	MAC generated by the TOE.
O.Hash	Hash generated by the TOE.
O.Signature	Signature generated by the TOE.
O.CipherText	The cipher text generated by the TOE.
O.PrivateKey	Private Key Data which the TOE uses to generate O.Signature (e.g. RSA Private key).
O.SecretKey	Secret Key Data which the TOE uses to encrypt O.Data and/or decrypt O.CipherText (e.g. AES key).
O.RandomSeed	The seed (initial state) used by the DRNG
O.RandomNumber	The random number generated by the TOE

1.5.6 Organizational Security Policy

No organizational security policies to comply with are required by the TOE.

1.5.7 Configuration Requirements

The TOE runs under following environments:

- JVM Specification 1.0.2 with the Java Platform 1.1 API and JCE 1.2.x
- JVM Specification 1.2 with one of the following APIs:
  - o J2SE 5.0
  - o J2SE 1.4.x
  - o J2SE 1.3.x and JCE 1.2.x
  - o J2SE 1.2.x and JCE 1.2.x

1.5.8 Assumptions for Operational Environment

Assumptions of required environment using this TOE are presented in the Table 1-3.

The effective performance of the TOE security functions are not assured unless these preconditions are satisfied.

Table 1-3 Assumption of TOE usage

Identifier	Assumption
A.Protection	The TOE and its environment are protected in such a way that it is impossible for S.Attacker to read or modify any data managed by the TOE, i.e. objects defined in chapter 3.4.2.
A.Train	Administrators (S.Admin) are assumed to be suitably qualified to set up the system and to verify the TOE integrity.
A.Manual	S.Developer uses the TOE in the right way as described in the manual. In order to reach SOF high, the S.Developer must use the key sizes recommend in the manual.
A.SeedManagement	The IT-Environment must provide a suitable seed for the RandomNumberGenerator. Furthermore it must ensure that the seed is kept secret.
A.KeyManagement	The IT-Environment is responsible for key management. Key management is out of scope of the TOE. O.PrivateKey and O.SecretKey, needed for computation of O.CipherText, O.MAC and O.Signature, must be provided by S.Application. The TOE does not generate or destruct keys. Given key material won't be modified or stored by the TOE.
A.Java_Spec	The S.Admin or S.Developer has to install a Java™ VM that works according the JVM Specification V 1.0.2 [JVMSpec1] with the API of Java™ 1.1 [JavaAPI1.1] or JVM 1.2 [JVMSpec2] with one of the following APIs: ・J2SE 5.x [JavaAPI5] ・J2SE 1.4.x [JavaAPI1.4] ・J2SE 1.3.x [JavaAPI1.3] ・J2SE 1.2.x [JavaAPI1.2]

A.JCE_Spec	If the Java™ API in use is older than version 1.4 [JavaAPI1.4] (1.1.x [JavaAPI1.1], 1.2.x [JavaAPI1.2] or 1.3.x [JavaAPI1.3]) the S.Admin/S.Developer has to install a JCE framework that works according to the JCE 1.2 [JCE1.2-REF], JCE 1.2.1 [JCE1.2.1-REF] or JCE 1.2.2 [JCE1.2.2-REF] specification.

Definition of Subject (like S.Attacker, etc) and Object (like O.PrivateKey, etc) on the above Table 1-3 is explained in Table 1-2-1 and Table 1-2-2 of 1.5.5 Threat.

1.5.9 Documents Attached to Product

Documents attached to the TOE are listed below.

(1) HTML guidance documentation included in the ZIP file iaikjce315cc.zip.
(2) API documentation included in the ZIP file iaikjce315cc.zip.

2. Conduct and Results of Evaluation by Evaluation Facility

2.1 Evaluation Methods

Evaluation was conducted by using the evaluation methods prescribed in CEM in accordance with the assurance requirements in CC Part 3. Details for evaluation activities are report in the Evaluation Technical Report. It described the description of overview of the TOE, and the contents and verdict evaluated by each work unit prescribed in CEM.

2.2 Overview of Evaluation Conducted

The history of evaluation conducted was present in the Evaluation Technical Report as follows.

Evaluation has started on 2006-09 and concluded by completion the Evaluation Technical Report dated 2007-06. The evaluation facility received a full set of evaluation deliverables necessary for evaluation provided by developer, and examined the evidences in relation to a series of evaluation conducted. Additionally, the evaluation facility directly visited the development and manufacturing sites on 2007-02 and examined procedural status conducted in relation to each work unit for configuration management, delivery and operation and lifecycle by investigating records and staff hearing. Further, the evaluation facility executed sampling check of conducted testing by developer and evaluator testing by using developer testing environment at developer site on 2007-01 and 2007-02.

Concerns found in evaluation activities for each work unit were all issued as Observation Report and were reported to developer. These concerns were reviewed by developer and all problems were solved eventually.

As for concerns indicated during evaluation process by the Certification Body, the certification review was sent to the evaluation facility. These were reflected to evaluation after investigation conducted by the evaluation facility and the developer.

2.3 Product Testing

Followings are overview of developer testing evaluated by evaluator and evaluator testing conducted by evaluator.

2.3.1 Developer Testing

1) Developer Test Environment
The test configuration of the developer testing is shown below:

- SUN JRE 1.1.8_010 serves as Java version 1.1.8,
- SUN JRE 1.2.2_017 serves as Java version 1.2.2,
- SUN JRE 1.3.1_19 serves as Java version 1.3.1,
- SUN JRE 1.4.0_04 serves as Java version 1.4.0,
- SUN JRE 1.4.1_06 serves as Java version 1.4.1,
- SUN JRE 1.4.2_12 serves as Java version 1.4.2,
- SUN JRE 1.5.0_09 (32-bit) serves as Java version 1.5.0

2) Outlining of Developer Testing
Followings are outline of the testing performed by the developer.

a. Test configuration
The test configuration of the developer testing is shown in the above 2.3.1, 1) Developer Test Environment. The developer's test was performed in a testing environment of hardware and software configuration equivalent to the TOE configuration specified in the ST.

b. Testing Approach
For the testing, following 2 (two) approaches were performed:

1. Type1: known-answer-tests
This is to verify TOE according to "test-vector" either provided by NIST or developed by the developer, except Random Number Generator. These "test-vector" used by the developer are from third party and keeping their legitimacy. In the test operation, parameters and key-lengths are changed and/or extended including the maximum/minimum to verify the TOE.

As for Random Number Generator, tests are performed according to "test suite" shown in {AIS20}.

2. Type2: API tests
This is to ensure that the TOE behaves according to the API specification of JCA/JCE.

c. Scope of Testing Performed
56 items of testing were performed by the developer.

The coverage analysis was conducted and it was verified that the testing covered all of the security functions as well as the external interfaces described in the functional specification. The depth analysis was also conducted and it was examined that the testing covered all the subsystems and the subsystem interfaces described in the high-level design.

d. Result
The evaluator confirmed consistencies between the expected test results and the actual test results provided by the developer. The evaluator confirmed the developer testing approach, legitimacy of testing items, and consistencies between actual testing approach as well as their results and the test plan.

2.3.2 Evaluator Testing

1) Evaluator Test Environment
Test configuration performed by the evaluator is same as the developer testing.

2) Outlining of Evaluator Testing
Followings are outline of testing performed by the evaluator.

a. Test configuration
Test configuration performed by the evaluator is same as the developer testing. The evaluator testing was performed in a testing environment of hardware and software configuration equivalent to the TOE configuration specified in the ST.

b. Testing Approach
For the evaluator testing, following 2 (two) approaches were performed:

1.Augmentation of developer testing for the TSF
The evaluator generates its original “test vector” which are different from the developer’s ones in contents as well as size, and verifies the TOE with them.

2.Supplementation of developer testing strategy
The evaluator devises their original tests (such as stress testing) which are not conducted by the developer, and verifies the TOE with them.

c. Scope of Testing Performed
The evaluator performed 24 original tests. The evaluator performed sampling tests in all of items which were performed by the developer, except testing of “code coverage” and “AIS20”. The selection policy of test items of the evaluator is as follows:

1. to perform all of tests which were carried out by the developer, except some tests that are impossible for the evaluator because of time restriction

2. to perform independent testing using different “test vector” from the developer’s

3. to perform additional testing like “stress test” from different viewpoints to the developer

d. Result
All evaluator testing were completed correctly. The evaluator confirmed the behavior of the TOE. The evaluator also confirmed that all the test results were consistent with the expected behavior.

2.4 Evaluation Result

The evaluator had the conclusion that the TOE satisfies all work units prescribed in CEM by submitting the Evaluation Technical Report.

3. Conduct of Certification

The following certification was conducted based on each materials submitted by evaluation facility during evaluation process.

1. Contents pointed out in the Observation Report shall be adequate.
2. Contents pointed out in the Observation Report shall properly be reflected.
3. Evidential materials submitted were sampled, its contents were examined, and related work units shall be evaluated as presented in the Evaluation Technical Report.

4. Conclusion

4.1 Certification Result

The Certification Body verified the Evaluation Technical Report, the Observation Report and the related evaluation evidential materials submitted and confirmed that all evaluator action elements required in CC Part 3 are conducted appropriately to the TOE. The Certification Body verified the TOE is satisfied the EAL3 assurance requirements prescribed in CC Part 3.

4.2 Recommendations

None

5. Glossary

The abbreviations used in this report are listed below.

CC:	Common Criteria for Information Technology Security Evaluation
CEM:	Common Methodology for Information Technology Security Evaluation
EAL:	Evaluation Assurance Level
PP:	Protection Profile
SOF:	Strength of Function
ST:	Security Target
TOE:	Target of Evaluation
TSF:	TOE Security Functions

6. Bibliography

[1] IAIK-JCE CC Core Security Target Version 1.8 16 March 2007

[2] IT Security Evaluation and Certification Scheme, May 2007, Information-technology Promotion Agency, Japan CCS-01

[3] IT Security Certification Procedure, May 2007, Information-technology Promotion Agency, Japan CCM-02

[4] Evaluation Facility Approval Procedure, May 2007, Information-technology Promotion Agency, Japan CCM-03

[5] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 2.3 August 2005 CCMB-2005-08-001

[6] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002

[7] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003

[8] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 2.3 August 2005 CCMB-2005-08-001 (Translation Version 1.0 December 2005)

[9] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002 (Translation Version 1.0 December 2005)

[10] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003 (Translation Version 1.0 December 2005)

[11] ISO/IEC 15408-1:2005 - Information Technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model

[12] ISO/IEC 15408-2:2005 - Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements

[13] ISO/IEC 15408-3:2005 - Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements

[14] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 2.3 August 2005 CCMB-2005-08-004

[15] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 2.3 August 2005 CCMB-2005-08-004 (Translation Version 1.0 December 2005)

[16] ISO/IEC 18045:2005 Information technology - Security techniques - Methodology for IT security evaluation

[17] EVALUATION TECHNICAL REPORT (ETR) Version 3 2007-06-25

[AIS20] Application Notes and Interpretation of the Scheme (AIS) AIS 20, Version 1, Date: 2 December,1999, Status: Mandatory, Subject: Functionality classes and evaluation methodology for, deterministic random number generators, Publisher: Certification body of the BSI, Section II 2, as part of the certification scheme

[FIPS 46-3] U.S. Department Of Commerce, Federal Information Processing Standards Publication: Data Encryption Standard (DES), FIPS PUB 46-3, U.S. Department Of Commerce, 199925 October 251999 (http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf).

[FIPS PUB 180-1] U.S. Department Of Commerce, Federal Information Processing Standards Publication: Secure Hash Standard, FIPS PUB 180-1, U.S. Department Of Commerce, 171995 April 1995 17 (http://csrc.nist.gov/publications/fips/fips180-1/fip180-1.pdf).

[FIPS PUB 180-2] U.S. Department Of Commerce, Federal Information Processing Standards Publication: Secure Hash Standard, FIPS PUB 180-2, U.S. Department Of Commerce, 262001 November 2001 26 (http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf).

[FIPS PUB 197] U.S. Department Of Commerce, Federal Information Processing Standards Publication: Advanced Encryption Standard, FIPS PUB 197, U.S. Department Of Commerce, 26 November 2001 (http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf).

[IETF-Draft-Kaukonen] K.Kaukonen, R.Thayer: A Stream Cipher Encryption Algorithm "Arcfour", IETF draft (Internet Draft: draft-kaukonen-cipher-arcfour-03.txt), 14 July 1999.

[ISO/IEC 10118-3]
ISO/IEC 10118-3:2003, Information technology -- Security techniques -- Hash-functions -- Part 3: Dedicated hash-functions, ISO/IEC, JTC 1/SC27, 14 November 2003.

[JavaAPI1.1] Java™ Platform 1.1 Core API Specification, SUN Microsystems, Inc., Palo Alto, California, 1995-1999, (http://java.sun.com/products/archive/jdk/1.1/index.html)

[JavaAPI1.2] Java™ 2 Platform, Standard Edition, v1.2.2 API Specification, SUN Microsystems, Inc., 1999, (http://java.sun.com/products/jdk/1.2/docs/api/index.html)

[JavaAPI1.3] Java™ 2 Platform, Standard Edition, v 1.3.1 API Specification, SUN Microsystems, Inc., 2001, (http://java.sun.com/j2se/1.3/docs/api/index.html)

[JavaAPI1.4] Java™ 2 Platform, Standard Edition, v 1.4.2 API Specification, SUN Microsystems, Inc., 2003, (http://java.sun.com/j2se/1.4.2/docs/api/)

[JavaAPI5] Java™ 2 Platform, Standard Edition, v 5.0 API Specification, SUN Microsystems, Inc., 2004, (http://java.sun.com/j2se/1.5.0/docs/api/)

[JCE1.2-REF] Java™ Cryptography Extension (JCE) API Specification & Reference, version 1.2, SUN Microsystems, Inc. (http://java.sun.com/products/jce/).

[JCE1.2.1-REF] Java™ Cryptography Extension (JCE) API Specification & Reference, version 1.2.1, SUN Microsystems, Inc. (http://java.sun.com/products/jce/).

[JCE1.2.2-REF] Java™ Cryptography Extension (JCE) API Specification & Reference, version 1.2.2, SUN Microsystems, Inc. (http://java.sun.com/products/jce/).

[JVMSpec1] Tim Lindholm, Frank Yellin: Tim Lindholm, Frank Yellin: The JavaTM Virtual Machine Specification, Addison-Wesley Pub Co, September 1996, ASIN: 020163452X (http://java.sun.com/docs/books/vmspec/index.html).

[JVMSpec2] Tim Lindholm, Frank Yellin: Tim Lindholm, Frank Yellin: The JavaTM Virtual Machine Specification (2nd Edition), Addison-Wesley Pub Co, 2nd edition, April 1999, ISBN: 0201432943 (http://java.sun.com/docs/books/vmspec/index.html).

[PKCS#1v1.5] PKCS#1 v1.5: RSA Encryption Standard RSA Laboratories; 1 November 1, 1993 (http://www.rsasecurity.com/rsalabs/pkcs/pkcs-1/).

[PKCS#1v2.1] PKCS#1 v2.1: RSA Cryptography Standard RSA Laboratories; June 14, 2002 (http://www.rsasecurity.com/rsalabs/pkcs/pkcs-1/).

[RFC 2268] R. Rivest: A Description of the RC2(r) Encryption Algorithm, Network Working Group, March 1998 (http://www.ietf.org/rfc/rfc2268.txt).