188 Scheme Crypto Policy

Issue: 4.0, 2013-06-18

Authorisation: Martin Bergling, Technical Manager
Table of Contents

1 Preface 3
  1.1 Purpose 3
  1.2 Typography 3

2 Scheme Crypto Policy 5
  2.1 Background 5
  2.2 Definition of TOE boundaries 5
  2.3 Description of key management 5
  2.4 Standards for cryptographic functions 5
  2.5 Use of cryptographic primitives 6
  2.6 Standards for cryptographic primitives 6
  2.7 Implementation of cryptographic primitives 6

3 Instructions for the evaluator 7
  3.1 Scope 7
  3.2 Evaluation activities 7
  3.3 Documentation of evaluation results 8

Appendix A Allowed Cryptographic Standards 9
  A.1 Cryptographic Primitives 9
  A.2 Modes of Operation 10
  A.3 Asymmetric Schemes 11

Appendix B Questions and Answers 13

Appendix C Referenced Standard Documents 15

Appendix D Scheme Policy Addendum - Evaluations being subject for approval by the Swedish NCSA 16
  D.1 TOE invoking cryptographic functions, approved by the Swedish NCSA, and implemented in the environment 16
  D.2 How to specify confidential information in ST's 16
Preface

This document is part of the description of the Swedish Common Criteria Evaluation and Certification Scheme ("the Scheme").

The Scheme has been established by the Swedish Certification Body for IT Security (CSEC) to evaluate and certify the trustworthiness of security features in IT products and the suitability of protection profiles (PP) to define implementation-independent sets of IT security requirements.

The objectives of the Scheme are to ensure that all evaluations are performed to high and consistent standards and are seen to contribute significantly to confidence in the security of those products and protection profiles; to improve the availability of evaluated IT products and protection profiles; and to continuously improve the efficiency and cost-effectiveness of the evaluation and certification process for IT products and protection profiles.

This document is part of a series of documents that provide a description of aspects of the Scheme and procedures applied under it. This document is of value to all participants under the Scheme, i.e., to anyone concerned with the development, procurement, or accreditation of IT systems for which security is a consideration, as well as those already involved in the Scheme, i.e., Scheme employees, evaluators, current customers, contractors, and security consultants.

The Scheme documents and further information can be obtained from the Swedish Certification Body for IT Security here:

<table>
<thead>
<tr>
<th>Swedish Certification Body for IT Security</th>
<th>FMV / CSEC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Postal address: SE-115 88 Stockholm, Sweden</td>
<td>Visiting address: Banérsgatan 62</td>
</tr>
<tr>
<td>Telephone: +46-8-782 4000</td>
<td>E-mail: <a href="mailto:csec@fmv.se">csec@fmv.se</a></td>
</tr>
<tr>
<td>Web: <a href="http://www.csec.se">www.csec.se</a></td>
<td></td>
</tr>
</tbody>
</table>

1.1 Purpose

This document provides instructions for evaluations of TOEs with cryptographic functionality, including a list of cryptographic algorithms that may be subject to CC evaluation, instructions how to define the TOE boundaries, and rules for specification of SFRs in a PP or ST.

1.2 Typography

The following terms are used to specify requirements:

**SHALL** Within normative text, “SHALL” indicates “requirements strictly to be followed in order to conform to the document and from which no deviation is permitted.” (ISO/IEC).

**SHOULD** Within normative text, “SHOULD” indicates “that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required.” (ISO/IEC)

The CC interprets 'not necessarily required' to mean that the choice of another possibility requires a justification of why the preferred option was not chosen.
MAY  Within normative text, “MAY” indicates “a course of action permissible within the limits of the document.” (ISO/IEC).

CAN  Within normative text, “CAN” indicates “statements of possibility and capability, whether material, physical or causal.” (ISO/IEC).
2 **Scheme Crypto Policy**

2.1 **Background**
Criteria for the assessment of the inherent qualities of cryptographic algorithms are not covered in the Common Criteria. CC part 1 states that the evaluation scheme under which the CC is applied has to make provision for such assessments if needed. The CEM states that any specific guidance in dealing with cryptography is left up to the discretion of the schemes.

The Swedish Armed Forces' National Communications Security Authority ("Swedish NCSA") has the authority to evaluate and approve cryptographic algorithms and systems to be used for the protection of classified information and other sensitive information critical for the protection of Swedish national critical infrastructure.

The following sections define the policy for CC evaluations performed within the Swedish Scheme as required by FMV/CSEC and the Swedish NCSA.

2.2 **Definition of TOE boundaries**
The physical boundaries of the TOE SHOULD be explicitly defined as a continuous perimeter which contains all the hardware, software and/or firmware components of the TOE.

The logical scope of the TOE SHOULD contain all the cryptographic functions implemented and/or invoked by the TOE, which are necessary to satisfy the security problem in the ST/PP.

2.3 **Description of key management**
Key management operations, invoked by the TOE, which are necessary to satisfy the security problem in the ST/PP, SHOULD be instantiated through FCS_CKM.

Import/export of cryptographic keys over the TOE boundary SHOULD be specified through FDP_ITC/FDP_ETC.

The "TOE Description" section SHOULD provide any information about key management procedures being necessary to apply in order to accomplish the security objectives (including but not limited to generation, distribution, entry, storage, export, import, access and destruction).

2.4 **Standards for cryptographic functions**
Cryptographic functions (i.e. cryptographic primitives, cryptographic protocols, random number generators etc) specified in the ST/PP for evaluations that are subject for mutual recognition SHOULD be specified through SFR:s referring to well defined publicly available cryptographic standards.

Cryptographic functions specified in ST/PP for evaluations that are subject for Swedish NCSA Cryptographic Approval MAY be specified through SFR:s referring to cryptographic standards approved by Swedish NCSA.

If the TOE only implements a subset of a referenced cryptographic standard, this limitation SHALL be unambiguously stated in the reference to the standard.

The TOE Description section of the ST/PP MAY mention cryptographic functionality and implementation in the product, that is not necessary to meet the security objectives. Where such cryptographic functionality is described in the ST/PP, both the ST/PP and the CR SHALL contain clear caveat statements to this effect.
FMV/CSEC reserves the right to judge whether the use of a cryptographic standard is appropriate to use in order to meet the ST/PP security objectives.

2.5 Use of cryptographic primitives
Cryptographic primitives being used by the TOE, which are necessary to accomplish security objectives in the ST/PP SHOULD be instantiated through FCS_COP.
Cryptographic primitive operations SHALL be subject for evaluation if, and only if, it has been instantiated through FCS_COP in the ST/PP.
FMV/CSEC reserves the right to judge whether the use of a cryptographic primitive is to be instantiated through FCS_COP in order to meet the ST/PP security objectives.

2.6 Standards for cryptographic primitives
Standards for implementation of cryptographic primitives and their related parameters in FCS_COP SHOULD be chosen among:
- CSEC list of allowed cryptographic standards, as specified in Appendix A
- Swedish NCSA list of approved cryptographic standards.
Other cryptographic primitives MAY be accepted into the certification if the cryptographic primitive and its strength is well documented and a rational is provided which explains why this cryptographic primitive need to be used.

2.7 Implementation of cryptographic primitives
The implementation of cryptographic primitives and related key management (i.e. FCS_COP, FCS_CKM and random bit generation), MAY be located in the TOE environment and hence be excluded from evaluation.
In such case:
The ST/PP SHOULD specify an interface (through software, firmware, hardware and/or other mechanisms) which unambiguously separates the part of the crypto- and key management implemented as a part of the TOE, from the implementation being a part of the environment.
The TOE administrator SHOULD be able to verify that the part of the crypto- and/or key management operations being implemented in the environment is being used in the evaluated configuration. The administrative guidance documentation SHOULD provide the necessary information on how to do this.
Correctness of the implementation of cryptographic primitives and related key management implemented in the environment SHALL be attested either through
- Swedish NCSA verification and approval,
- Vendor affirmation.
The ST/PP and certification report SHALL describe who performed verification of correctness of implementation.
Vendor affirmation MAY be done through referring to attestations of correctness of implementation provided by parties outside the Scheme.
The Evaluator SHALL analyse the coverage of compliance testing made by the other party in order to confirm that there is no gap in coverage as required by the CC and the CEM.
3 Instructions for the evaluator

3.1 Scope
The case where no cryptographic SFRs are included in the ST/PP, and the case where all cryptographic primitives and related key management are implemented within the physical scope of the TOE, are covered by CC/CEM and no further guidance will be given here.

The case where cryptographic SFRs exist in the ST/PP, but some cryptographic primitives, and related key management, are implemented outside the physical scope of the TOE, on the other hand, is not covered by the CC/CEM. This chapter provides guidance for how the evaluator shall deal with this case.

3.2 Evaluation activities
The evaluator SHALL verify that the physical and the logical scope of the TOE are defined in accordance with this document, and that all necessary SFRs are present and well defined in the ST/PP.

The evaluator SHALL verify that there is a clear statement in the TOE Overview part of the ST Introduction:
- that explains that the implementation of the cryptographic primitives and related key management are excluded from the evaluation
- that specifies who has tested and verified the implementation.

Example 1: The cryptographic library "EpicEncryption v.1.2", relied upon by the TOE, has been tested by the developer "Software Implementations AB". The implementation of "EpicEncryption" is outside the TOE scope, and its internals are not covered by the evaluation.

Example 2: The cryptographic module "SuperCrypt v1.0", relied upon by the TOE, has been FIPS 140-2 validated by NIST and CSE, Certificate No: 1234. "SuperCrypt" is outside the TOE scope, and therefore its internals are not covered by the evaluation.

Example 3: The cryptographic module "MiliCrypt v3.0", relied upon by the TOE, has been tested and approved by the Swedish NCSA. "MiliCrypt" is outside the TOE scope, and therefore its internals are not covered by the evaluation.

The evaluator also SHALL ensure that the third party affirmation of the cryptographic implementation outside the scope of the TOE covers all cryptographic primitives and key management called from the TOE, and applies to the version of the implementation used by the TOE.

The evaluator SHALL verify that the calls to cryptographic primitives and related key management result in actions that comply with the standards referenced by the SFRs in the ST/PP. This may be done by comparison with the results of a reference implementation known to comply with the standards in question. Key management operations SHALL be verified by the evaluator if they are invoked explicitly by the TOE or if the TOE takes active part in the operation.

At EAL 4, or if there is an ADV_IMP augmentation in the ST/PP, all calls to cryptographic primitives and related key management, implemented in the TOE Environment, SHALL be verified by code review performed by the evaluator. The review shall focus on verifying that the calls are suitable for achieving the SFRs in the ST/PP, considering to the syntax of the call, described in the interface description of the cryptographic implementation.
3.3 **Documentation of evaluation results**

The results of the evaluation may be documented separately, in the evaluation reports covering ASE, ADV and ATE, or as parts of suitable CEM work units. It shall be clear from the evaluation reports that the Scheme Crypto Policy has been taken into consideration.
Appendix A  Allowed Cryptographic Standards

This document provides a list of allowed cryptographic standards in CC evaluations of products and PPs, containing cryptographic functionality, under the Swedish CC Scheme. Cryptographic standards and options not present in this list may be accepted in an evaluation on a case by case basis.

This list is only applicable to products which undergo CC evaluations in accordance with the Swedish CC scheme. The list applies to evaluations in general as well as when approval as a KSU system will be sought with the Swedish NCSA. Please note that further restrictions may apply if for approval by the Swedish NCSA.

This list is not applicable to COMSEC systems intended to be approved in Sweden for COMSEC classification levels SG RESTRICTED or above.

A.1  Cryptographic Primitives

Asymmetric Algorithms

RSA  standard PKCS #1 v. 2.1
key size 2048 bits, 3072 bits, or higher
key generation standard FIPS 186-3, Appendix B or C

It is important that a sequence which for the intended adversary is computationally undistinguishable from a uniformly random sequence be used to form the private exponent and the prime factors p and q.

ECC  standard FIPS 186-3
domain parameters P-256, P-384, P-521 (FIPS 186-3 Appendix D.1.2)
key generation standard FIPS 186-3 Appendix B.4.2

It is important that a sequence which for the intended adversary is computationally undistinguishable from a uniformly random sequence be used to form the private scalar. The sequence should be post-processed according to appendix B.4.2 in FIPS 186-3 to form the scalar.

Block Ciphers

AES  standard FIPS 197
key size 128 bit, 192 bit, 256 bit
key generation standard FIPS 197

TDEA  standard NIST SP 800-67
key size 168 bit
key generation standard FIPS 46-3
Cryptographic Hash Functions

SHA-224 standard FIPS 180-3

SHA-256 standard FIPS 180-3

SHA-384 standard FIPS 180-3

SHA-512 standard FIPS 180-3

A.2 Modes of Operation

Encryption

CBC
standard NIST SP 800-38A
primitives AES (128, 192, 256 bit), TDEA (168 bit)

CFB
standard NIST SP 800-38A
primitives AES (128, 192, 256 bits), TDEA (168 bits)

CTR
standard NIST SP 800-38A
primitives AES (128, 192, 256 bits), TDEA (168 bits)

GCTR
standard NIST SP 800-38D
primitives AES (128, 192, 256 bits)
Note: This is an instantiation of CTR with a specified incrementing function for 128 bit blocks.

OFB
standard NIST SP 800-38A
primitives AES (128, 192, 256 bits)

XTS
standard NIST SP 800-38E
primitives AES (128, 192, 256 bits)
only to be used for encrypting block devices

Message Authentication

HMAC
standard FIPS 198 (or rfc 2104)
Swedish Certification Body for IT Security
188 Scheme Crypto Policy

4.0
2013-06-18

SP-188

11 (16)

CMAC
standard NIST SP 800-38B
to be used with AES
AES key size 128 bit, 192 bit, 256 bit

GMAC
standard NIST SP 800-38D
to be used with AES
AES key size 128 bit, 192 bit, 256 bit

Authenticated Encryption

GCM
standard NIST SP 800-38D

A.3 Asymmetric Schemes

Encryption
RSAES-OAEP
standard PKCS #1 v. 2.1
To be used with key pair approved for RSA.
The mask generation function MGF1 shall be used, based on SHA-224, SHA-256, SHA-384 or SHA-512

Digital Signature
RSASSA-PKCS1-v1_5
standard PKCS #1 v. 2.1
To be used with key pair approved for RSA.
To be used with SHA-224, SHA-256, SHA-384, or SHA-512.

RSASSA-PSS
standard PKCS #1 v. 2.1
To be used with key pair approved for RSA.
To be used with SHA-224, SHA-256, SHA-384, or SHA-512.
The mask generation function MGF1 shall be used, based on the same hash function as is used for the message hash.

to be used with SHA-224, SHA-256, SHA-384, or SHA-512
key size 224 bit with SHA-224
key size 256 bit with SHA-256
key size 384 bit with SHA-384
key size 512 bit with SHA-512
EC-DSA

standard FIPS 186-3
To be used with a domain parameter and key pair approved for ECC.
To be used with SHA-224, SHA-256, SHA-384 or SHA-512.
The hash digest length should be approximately equal to or greater than
the order of the elliptic curve generator point.
It is important that a sequence which for the intended adversary is
computationally undistinguishable from a uniformly random sequence be
used to form the per message random scalar. The sequence should be
post-processed according to appendix B.5.2 in FIPS 186-3 to form the
scalar.
Appendix B

Questions and Answers

Some SFR:s implies use of cryptographic primitives implicitly. For example, assume that FTP_ITC "Inter-TSF trusted channel" based on crypto is present in the ST. Is it then necessary to specify FCS_COP.1 Cryptographic operation SFRs for the cryptographic primitives?

Yes, all usage of cryptographic primitives to protect assets must be specified by FCS_COP.1 "Cryptographic operation". This is required both by CC and the crypto policy (see quotes below):

CC Part 2 §149 (FCS_COP) states that: "This family should be included whenever there are requirements for cryptographic operations to be performed", and SP-188 section 2.5 requires that: "Cryptographic primitives being used by the TOE, which are necessary to accomplish security objectives in the ST/PP SHOULD be instantiated through FCS_COP".

Is it necessary to specify a new FCS_COP.1 Cryptographic operation for every invocation of a given cryptographic primitive?

No, not always. Several invocations from the TOE of the same particular standard (including relevant parameters) only need to be covered by one instance of FCS_COP.1 in the ST/PP. However, when several different cryptographic standards (including relevant parameters) for a crypto primitive are being invoked, each will need a separate FCS_COP in the ST/PP. During evaluation, the evaluator must ensure coverage for all implementations and/or invocations of cryptographic primitives used by the TOE while evaluating ATE and AVA.

Is it necessary to specify a new FCS_CKM for each invocation of a key management function?

No, not always. When different cryptographic standards (including relevant parameters) are being used, each will need a separate instantiation of FCS_CKM (similar to the case with FCS_COP above). When several implementations of the same standard are used, the evaluator must consider all distinct implementations in ATE and AVA.

Can a high level call to cryptographic primitives, such as to TLS, serve to define the logical boundary between the TOE (the invocation) and the environment (the implementation)?

Yes, as long as it can be clearly seen which part of the source code (implementation representation) belongs to the TOE, and which belongs to the environment. It is understood that the cryptographic primitives used to protect assets should be specified by FCS_COP.1.

Is it allowed to use a specific implementation as a cryptographic standard in SFRs?

No, an implementation independent, well defined, public cryptographic standard must be used – or a standard approved by the Swedish NCSA for the intended purpose.

How shall the evaluator verify the correctness of cryptographic primitives and protocols?
In ADV, the evaluator verifies that the TOE calls the crypto implementation with correct syntax and parameterization.

In ATE the evaluator should specify an independent reference implementation, other than the one used by the TOE, and verify the crypto primitives and protocols against this. In particular, verify that the specified primitives actually are being used.

_How does the evaluator verify the correctness of primitives and protocols, implemented in the TOE, that are not visible through external interfaces?_

The evaluator may choose between the following alternatives:

- Work with the developer to get access to internal interfaces
- Write a test tool, using the relevant TOE source code
- Review the source code
- Propose another way to the certifier
- Propose that the developer re-designs the product. It is not acceptable to have vital security mechanisms that cannot be verified.
# Appendix C  Referenced Standard Documents

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIPS 46-3</td>
<td>Data Encryption Standard (DES), NIST,</td>
<td>October 25, 1999</td>
</tr>
<tr>
<td>FIPS 186-3</td>
<td>Digital Signature Standard (DSS), NIST,</td>
<td>June, 2009</td>
</tr>
<tr>
<td>FIPS 197</td>
<td>Advanced Encryption Standard, NIST,</td>
<td>November 26, 2001</td>
</tr>
<tr>
<td>FIPS 180-3</td>
<td>Secure Hash Standard, NIST,</td>
<td>October 2008</td>
</tr>
<tr>
<td>FIPS 198</td>
<td>The Keyed-Hash message Authentication Code (HMAC), NIST,</td>
<td>March 06, 2002</td>
</tr>
<tr>
<td>NIST SP 800-38A</td>
<td>Recommendations for Block Cipher Modes of Operation, Methods and Techniques, NIST,</td>
<td>December 2001</td>
</tr>
<tr>
<td>NIST SP 800-38B</td>
<td>Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, NIST,</td>
<td>May 2005</td>
</tr>
<tr>
<td>NIST SP 800-38D</td>
<td>Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, NIST,</td>
<td>November 2007</td>
</tr>
<tr>
<td>NIST SP 800-38E</td>
<td>Recommendations for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices, NIST,</td>
<td>January 2010</td>
</tr>
<tr>
<td>NIST SP 800-67</td>
<td>Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, NIST,</td>
<td>May 2004</td>
</tr>
<tr>
<td>PKCS #1 v2.1</td>
<td>PKCS#1: RSA Cryptography Standard, RSA Laboratories,</td>
<td>June 14, 2002</td>
</tr>
<tr>
<td>rfc 2104</td>
<td>HMAC: Keyed-Hashing for Message Authentication, IETF,</td>
<td>February 1997</td>
</tr>
</tbody>
</table>
Appendix D  Scheme Policy Addendum - Evaluations
being subject for approval by the Swedish NCSA

D.1  TOE invoking cryptographic functions, approved by the
Swedish NCSA, and implemented in the environment

Summary
In case a TOE invokes cryptographic functions, approved by the Swedish NCSA, and
these functions are implemented in the environment, the standards for cryptographic
primitives and key management of the corresponding functions do not have to be
evaluated and do not have to be explicitly specified as FCS_COP/FCS_CKM
requirements.

Description
This section describes rules that MAY be used as an alternative to the rules described
in section 2.3 “Description of key management” and 2.5 “Use of cryptographic
primitives” of the policy when a TOE invokes cryptographic functions, implemented
by a software or hardware module in the environment, which have been approved for
the purpose by the Swedish NCSA. Note that the module does not necessarily have to
be a specialized cryptographic module.

When cryptographic functions in such modules are being invoked by the TOE, the
corresponding SFRs for cryptographic operation (FCS_COP) do not need to be
specified in the ST if the requirements for cryptographic functions are implicitly stated
through other SFRs. SFRs for key management (FCS_CKM) only need to be specified
when explicit management of cryptographic keys takes place within the TOE.

The ST should provide sufficient information to enable the reader to conclude that the
cryptographic functions are adequate to fulfil the security objectives.

The ST should clearly demonstrate that the cryptographic functions are used in
accordance with the cryptographic approval statement by the Swedish NCSA. When
necessary, the cryptographic approval statement may need to be complemented by
NCSA to provide such clarification.

In the ST, the following information must be specified, e.g. in application notes:

• The precise version of the module implementing the cryptographic functions.
• Any relevant parameters such as cipher suite, and settings which affect the
  security relevant behaviour (i.e. necessary to demonstrate the fulfilment of the
  security objectives).

D.2  How to specify confidential information in ST’s

In evaluations that are subject to cryptographic approval by the Swedish NCSA, an ST
may need to refer to some limited pieces of information that are confidential. In order
to avoid classifying the entire ST, it is allowed to replace such confidential
information with a reference (and possibly a symbolic name). If so, these references
(and symbolic names) shall be specified in a separate document with appropriate
classification. Only staff with sufficient security clearance may have access to this
document, preferably only on-site in the information owner’s premises.

It can be noted that certifications based on ST:s that contain references to confidential
documents are not subject for mutual recognition.