CSEC

Swedish Certification Body for IT Security

188 Scheme Crypto Policy

Issue: 11.0, 2021-jun-07

Authorisation: Dag Ströman, Head of CSEC , CSEC

Table of Contents

1 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:

Swedish Certification Body for IT Security
FMV / CSEC
Postal address: SE-115 88 Stockholm, Sweden
Visiting address: Banérgatan 62

Telephone: +46-8-782 4000 E-mail: csec@fmv.se
Web: www.csec.se

1.1 Purpose

This document provides instructions for evaluations of targets of evaluation (TOE) with cryptographic functionality, including a list of cryptographic algorithms that may be subject to Common Criteria (CC) evaluation, instructions how to define the target of evaluation boundaries, and rules for specification of security functional requirements (SFR) in a protection profile (PP) or security target (ST).

1.2 Terminology

1 Abbreviations commonly used by CSEC are described in SP-001 Certification and Evaluation - Scheme Overview.

2 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). CC part 1 states that the evaluation scheme under which the CC is applied has to make provision for such assessments if needed. The Common Methodology for Information Technology Security Evaluation (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 defines the policy for CC evaluations performed within the Swedish Scheme as required by FMV/CSEC and the Swedish NCSA.

2.2 Definition of Target of Evaluation Scope

The physical boundaries of the target of evaluation SHOULD be explicitly defined as a continuous perimeter which contains all the hardware, software and/or firmware components of the target of evaluation. The physical scope of the target of evaluation is comprised of all hardware, firmware and software parts within this boundary.

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

2.3 Description of Key Management

Key management operations, invoked by the target of evaluation, 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 target of evaluation 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 security functional requirements (SFR) referring to well defined publicly available cryptographic standards.

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

If the target of evaluation 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 certification report 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 target of evaluation 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

2.6.1 Certifications Subject to CCRA and/or SOGIS-MRA

Regarding certifications subject to the Common Criteria Recognition Arrangement (CCRA) and/or Senior Officials Group Information Systems Security - Mutual Recognition Agreement (SOGIS-MRA) standards for implementation of cryptographic primitives and their related parameters in FCS_COP SHOULD be chosen among CSEC’s list of recommended cryptographic standards, as specified in Appendix A, or from the SOGIS document Agreed Cryptographic Mechanisms.

Other cryptographic standards and options not present in this list may also be allowed in an evaluation conditioned that they

- are well-defined and publicly available,
- do not exhibit publicly known vulnerabilities or weaknesses, and
- have strength that is consistent with the attack potential specified by the ST/PP.
- Cryptographic primitives allowed as per above are subject to CSEC approval on a case-by-case basis.

2.6.2 Certification Subject to Swedish NCSA KSU Approval

If the product being evaluated also is subject to Swedish “krypto för skyddsvärda uppgifter” (KSU) approval with the Swedish NCSA, standards for implementation of cryptographic primitives and their related parameters in FCS_COP SHALL be chosen among CSEC's list of recommended cryptographic standards, as specified in Appendix A. Please note that further restrictions may apply if the product is subject to approval by the Swedish NCSA.

2.7 Implementation of Cryptographic Primitives

2.7.1 Exclusion of Implementation of Cryptographic Primitives from the Scope of the Target of Evaluation

The implementation of cryptographic primitives and related key management (i.e. FCS_COP, FCS_CKM and random bit generation), MAY be located in the target of evaluation environment and hence be excluded from evaluation.

In such case:

The excluded part shall not contain an implementation of any other cryptographic mechanisms necessary to meet target of evaluation security objectives and therefore is represented by an security functional requirements in the ST/PP. Typical such cryptographic mechanisms are protocols such as SSL, TLS, IPSec, and SSH.

The excluded part may contain the implementation of cryptographic primitives, modes for symmetric encryption, schemes for signatures and encryption using RSA, signature schemes using DSA and elliptic curve cryptography. HMAC is also allowed.

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 target of evaluation, from the implementation being a part of the environment.

The target of evaluation 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.

The purpose for allowing the placement of the cryptographic implementation in the environment as described above is to make it possible to evaluate a TOE with a 3rd party crypto module .

2.7.2 Verification of Excluded Cryptographic Implementations

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,
- Certification or validation through another conformity assessment scheme being subject for mutual recognition by Sweden. Such schemes are: Common Criteria Recognition Arrangement (CCRA), Senior Officials Group Information Systems Security - Mutual Recognition Agreement (SOGIS-MRA) and/or the European cooperation for accreditation multilateral agreement (EA MLA).
- CSEC may on a case by case basis allow other cryptographic approval certification schemes than noted above.

In all cases, it will be the responsibility of the user of the certified products to ensure that the cryptographic approval of primitives has been granted by an authority that is in accordance with relevant regulations and policies.

The ST/PP and certification report SHALL describe who performed verification of correctness of implementation.

Proof of such endorsement shall be provided to CSEC. 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.

A special case of the second alternative above is when a cryptographic implementation is placed in the environment, but all aspects of the cryptographic implementation (such as source code review) are completely evaluated anyway within the ongoing evaluation, as if the implementation was placed within the TOE. In this case the excluded cryptographic implementation will be considered to be verified in a satisfactory manner.

3 Instructions for the Evaluator

3.1 Scope

In the case where no cryptographic security functional requirements (SFRs) are needed to protect the assets in the PP/ST, this document does not provide any requirements or guidance beyond CC/CEM.

When cryptographic SFRs are needed to protect assets in the PP/ST, and all cryptography is implemented in the TOE, the requirements in section 3.2.2 apply.

In the case where cryptographic security functional requirements exist in the ST/PP, but some cryptographic primitives and related key management are implemented outside the physical scope of the TOE, the requirements in section 3.2.1 as well as in 3.2.2 have to be fulfilled.

3.2 Evaluation Activities

3.2.1 For Cryptographic Security Functional Requirements Implemented in the Environment

The following work units should be performed and documented along with the work units from the CEM whenever there are cryptographic security functional requirements (SFR) in the security target (ST), but the implementation has been placed in the target of evaluation environment:

Assurance Class Security Target Evaluation ASE_CRYPT.1-1

The evaluator shall examine whether it is clearly expressed in the Security Target Introduction (ST Introduction) which security functional requirements enforcing cryptographic functionality has been placed in the environment, and which party has verified and tested the implementation.

The ST Introduction must make clear which parts of the implementation of the cryptographic primitives and related key management are excluded from the scope of the target of evaluation, and which security relevant functionality that has been excluded from the scope of the target of evaluation.

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

The evaluator SHALL check that the party responsible for verification of the cryptographic functionality is in accordance with the section "Verification of excluded cryptographic implementations" above.

This work unit should be performed in conjunction with assurance class security target evaluation family ASE_INT.1-4.

Assurance Class Security Target Evaluation ASE_CRYPT.1-2

The evaluator shall examine that the boundary of the cryptographic implementation is well defined.

For example, the boundary must not divide a binary file into a target of evaluation part and an environment part.

This work unit should be performed in conjunction with assurance class security target evaluation family ASE_INT.1-9.

Assurance Class Security Target Evaluation ASE_CRYPT.1-3

The evaluator shall examine that the logical scope of the cryptographic implementation placed in the environment is well defined.

All functionality in the cryptographic implementation in the environment that is used by the target of evaluation has to be described in the security target.

This work unit should be performed in conjunction with assurance class security target evaluation family ASE_INT.1-10.

Assurance Class Security Target Evaluation ASE_CRYPT.1-4

The evaluator shall examine the security target and determine, that all cryptographic operations performed by the implementation in the environment, that are necessary to protect assets in the security target, have been represented by appropriate security functional requirements.

This includes all FCS_COP SFRs and the FCS_CKM operations directly invoked by the target of evaluation or where the target of evaluation handles the cryptographic keys in any way.

This work unit should be performed in conjunction with assurance class security target evaluation family ASE_REQ.2-11. If the security target contains ASE_REQ.1, all cryptographic functionality mentioned as protecting assets in the security target has to be represented by a security functional requirement.

Assurance Class Development ADV_CRYPT.1-1

The evaluator shall examine the implementation representation and verify that the calls to the cryptographic implementation in the environment are suitable to invoke the functionality described in the security target.

The purpose is to verify, for example, that if the security target states that AES with a 256 bit key is used in CBC mode (see Appendix A.4), it shall be verified that this is what the target of evaluation actually invokes.

Key management operations SHALL be verified by the evaluator if they are invoked explicitly by the target of evaluation or if the target of evaluation takes active part in the key management.

This work unit only applies at evaluation assurance level 4 (EAL 4) and above, i.e. when the security target contains an assurance class development family, ADV_IMP requirement, and should be performed in conjunction with the ADV_IMP.1-3 work unit.

Assurance Class Tests ATE_CRYPT.1-1

The evaluator shall examine whether all cryptographic functionality, implemented in the environment but represented by security functional requirements, has been covered by the developer tests, and add all missing tests to the evaluator's testing.

Every algorithm, mode, and signature/encryption scheme stated in the security target and implemented in the environment must be verified using a trusted reference implementation.

The reference implementation must be independent from the target of evaluation implementation, i.e. must not be another instance of the same crypto implementation. The reference implementation must be well known and in common use.

The evaluator shall provide a reference (name, version, configuration) to reference implementations used in the evaluation report.

Key management operations must be verified by the evaluator if they are invoked explicitly by the target of evaluation or if the target of evaluation takes active part in the key management. When an assurance class development family; ADV_IMP requirement is present in the security target, this may be done as part of the code review.

This work unit should be performed in conjunction with assurance class tests families ATE_COV.1-1 or ATE_COV.2-1 and any missing tests be added to the evaluator's independent tests in conjunction with ATE_IND.1-3 or ATE_IND.2-6.

Assurance Class Vulnerability Assessment AVA_CRYPT.1-1

The evaluator shall examine sources of information publicly available to identify potential vulnerabilities in the target of evaluation.

Specifically, public vulnerability databases shall be searched for any vulnerability related to the cryptographic implementation placed in the environment, each algorithm used, each mode, and each scheme used.

This work unit should be performed as an extension to the assurance class vulnerability assessment families AVA_VAN.1-3, AVA_VAN.2-3, AVA_VAN.3-3, AVA_VAN.4-3, or corresponding, and the results should be used in the vulnerability assessment in the same way as the results from these work units.

3.2.2 For all Evaluations

The following extra work units should always be performed when cryptographic functionality is included in the security target.

Assurance Class Security Target Evaluation ASE_ALGO.1-1

The evaluator SHALL verify that the cryptographic primitives, modes, schemes and protocols used to protect assets in the security target are compatible with the requirements in Appendix A in this document.

CSEC reserves the right not to accept evaluations when cryptographic primitives, modes, schemes or protocols are specified in the security target, that is not in accordance with the requirements in Appendix A.

Assurance Class Tests ATE_REF.1-1

The evaluator SHOULD verify the cryptographic mechanisms specified in the PP/ST using a reference implementation that is independent, i.e. that is not generated from the same or closely related source code. A cryptographic module that has previously been validated/certified MAY be used as reference implementation even if it is not independent.

3.3 Documentation of Evaluation Results

The results of the evaluation of the specific work units described above should be documented in the single evaluation report (SER) as any work unit from the Common Methodology for Information Technology Security Evaluation (CEM). It is recommended that the work units are documented in the same report and together with the related Common Methodology for Information Technology Security Evaluation work units listed in the work unit texts above.

Appendix A Recommended Cryptographic Standards

This appendix provides a list of recommended cryptographic standards in CC evaluations of products and protection profiles, containing cryptographic functionality, under the Swedish CC Scheme.

The list is based on the SOGIS "Agreed Cryptographic Mechanisms" document. Other cryptographic primitives than those listed here may be acceptable, decided on a case-by-case basis.

The reader is referred to SOGIS "Agreed Cryptographic Mechanisms" for more information.

A.1 Block Ciphers

Recommended

AES	Standard FIPS 197, ISO 18033-3 Key sizes 128, 192 or 256 bits

Legacy

Triple DES	Standard FIPS 46-3, ISO 18033-3 Key sizes 168 or 112 bits

A.2 Stream Ciphers

No agreed dedicated stream cipher. Agreed modes of operation of a block cipher, such as the counter mode, provide an agreed stream cipher mechanism when applied to an agreed block cipher.

A.3 Hash Functions

Recommended

SHA-2	Standard FIPS 180-4, ISO 10118-3 Hash length 256 bits (SHA-256) Hash length 384 bits (SHA-384) Hash length 256 to 512 bits (SHA-512/h)
SHA-3	Standard FIPS 202 Hash length 512 bits Hash length 384 bits Hash length 256 bits

Legacy

SHA-2	Standard FIPS 180-4, ISO 10118-3 Hash length 224 bits (SHA-224) Hash length 224 bits (SHA-512/224)

A.4 Modes of Operation

The following modes are for use in conjunction with the recommended block ciphers

CTR	Standard SP 800-38A, ISO 10116 Counter mode
OFB	Standard SP 800-38A, ISO 10116 Output feedback mode
CBC	Standard SP 800-38A, ISO 10116 Cipherblock chaining mode
CBC-CS	Standard SP 800-38A Addendum Cipherblock chaining mode, ciphertext stealing
CFB	Standard SP 800-38A, ISO 10116 Cipher feedback mode

A.5 Asymmetric Algorithms

Recommended

RSA	PKCS #1 v2.2 Key size 3072 bits or higher Key generation standard FIPS 186-4, 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.

Legacy

RSA	PKCS #1 v1.5 Key size 2048 bits or higher Key generation standard FIPS 186-4, 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.

A.6 Asymmetric Schemes, Encryption

Recommended

RSAES-OAEP	Standard PKCS #1 v2.2 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 In case the OAEP decryption procedure is not correctly implemented, that is to say, the checks performed by EME-OAEP decoding are not performed in the specified order, RSA-OAEP may be vulnerable to oracle attacks.

A.7 Digital Signatures

Recommended

RSASSA-PSS	Standard PKCS #1 v2.2
KCDSA	Standard ISO 14888-3
Schnorr	Standard ISO 14888-3/am1
DSA	Standard ISO 14888-3, FIPS 186-4
EC-KCDSA	Standard ISO 14888-3
EC-DSA	Standard ISO 14888-3, FIPS 186-4
EC-GDSA	Standard TR-03111
EC-Schnorr	Standard ISO 14888-3/am1

Legacy

RSASSA-PKCS1-v1_5	Standard PKCS#1 v1.5

A.8 Message Authentication

Recommended

CMAC	Standard SP 800-38B, ISO 9797-1
CBC-MAC	Standard ISO 9797-1, algorithm 1, padding 2 Note: CBC-MAC is agreed only in contexts where the sizes of all the inputs for which CBC-MAC is computed under the same key are identical. Trivial length extension forgeries can be performed when variable length inputs are allowed.
HMAC	Standard RFC 2104, ISO 9797-2 Key size at least 125 bits

Legacy

HMAC	Standard RFC 2104, ISO 9797-2 Key size at least 100 bits
HMAC-SHA-1	Standard RFC 2104, ISO 9797-2, FIPS 180-4 Key size at least 100 bits The HMAC construction does not require the collision resistance of the underlying hash function. For the time being, HMAC-SHA-1 is considered as an acceptable legacy mechanism, even though SHA-1 is not considered as an acceptable general purpose hash function. It is recommended however to phase out HMAC-SHA-1.

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 target of evaluation, 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 target of evaluation 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 target of evaluation 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.

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 target of evaluation calls the crypto implementation with correct syntax and parameterization (at EAL 4 and above).

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

In AVA the evaluator searches in public vulnerability databases for vulnerabilities related to any security relevant third party modules, the primitives, modes, schemes and protocols used.

How does the evaluator verify the correctness of primitives and protocols, implemented in the target of evaluation (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 target of evaluation 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

Standard	Description	Date
FIPS 46-3	Data Encryption Standard (DES), NIST	October 25, 1999
FIPS 186-4	Digital Signature Standard (DSS), NIST	July, 2013
FIPS 197	Advanced Encryption Standard, NIST	November 26, 2001
FIPS 180-4	Secure Hash Standard NIST	August 2015
FIPS 198-1	The Keyed-Hash message Authentication Code (HMAC) NIST	July, 2008
FIPS 202	SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, August	2015
NIST SP 800-38A	Recommendations for Block Cipher Modes of Operation, Methods and Techniques, NIST	December 2001
NIST SP 800-38B	Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, NIST	May 2005
NIST SP 800-38D	Recommendation for Block Cipher Modes of Operation:Galois/Counter Mode (GCM) and GMAC, NIST	November 2007
NIST SP 800-38E	Recommendations for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices, NIST	January 2010
NIST SP 800-67	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, NIST	January 2012
PKCS #1 v2.2	PKCS#1: RSA Cryptography Standard, RSA Laboratories	October, 2012
RFC 3447	Public-Key Cryptography Standards (PKCS) #1 RSA Cryptography Specifications	Version 2.1

Appendix D Scheme Policy Addendum - Evaluations being Subject for Approval by the Swedish NCSA

Target of evaluation (TOE) invoking cryptographic functions, approved by the Swedish NCSA, and implemented in the environment

D.1 Summary

In case a target of evaluation (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.

D.2 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 target of evaluation 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 target of evaluation, the corresponding security functional requirements for cryptographic operation (FCS_COP) do not need to be specified in the security target if the requirements for cryptographic functions are implicitly stated through other security functional requirements. Security functional requirements for key management (FCS_CKM) only need to be specified when explicit management of cryptographic keys takes place within the target of evaluation.

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

The security target 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 security target, 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.3 Specify Confidential Information in Security Targets

In evaluations that are subject to cryptographic approval by the Swedish NCSA, an security target may need to refer to some limited pieces of information that are confidential. In order to avoid classifying the entire security target, 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 security targets that contain references to confidential documents are not subject for mutual recognition.