Netherlands Scheme for Certification in the Area of IT Security (NSCIB)

Nederlands Schema voor Certificatie op het gebied van IT-Beveiliging (NSCIB)

NSCIB Scheme Instruction 11

Remaining strength of cryptographic implementations

Approved.....

Technical Manager NSCIB

Instruction	11
Report title	Remaining strength of cryptographic implementations
Date of issue	23 July 2015
Version	1.0
Distribution	Public
Filename	NSI_11_Remaining_strength_of_cryptographic_implementations_v1.0.docx

TÜVRheinland®
Precisely Right.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

1 Purpose of this document

Many of the smartcard products or similar devices implement cryptographic operations that are subject to attacks such as fault injection and side-channel attacks at a high attack potential (AVA_VAN.5). Current state of the art of attack technology is such that some decrease of the security provided by the product is highly likely, and at the same time the decrease can quite possibly be small enough to not lead to exploitable weaknesses.

NSCIB currently[1] considers 100 security bits sufficient for common usage without further constraints, in line with the SOG-IS Crypto WG consensus. Cryptographic implementations that still have at least 80 security bits left after the best high attack potential attack (AVA_VAN.5) may still be sufficiently strong for the intended usage, but the user should be made aware of this.

This interpretation describes how NSCIB determines whether the resulting cryptographic implementation can be claimed as meeting the requirements, potentially with a warning to users of this TOE.

1.1 Constraints

This interpretation only addresses questions around the strength of the implementation of cryptographic implementations in the face of high attack potential (AVA_VAN.5) attackers, interpreted according to the applicable guidance for the specific TOE domain.

This interpretation does not address determination of the strength of the cryptographic algorithm itself, nor whether specific algorithms are suitable for national use.

[1] At the time of issuance of this interpretation. This may be updated as needed.

2 Remaining strength of cryptographic implementations

The strength of a cryptographic implementation is here expressed as an amount of security bits, describing the remaining amount of unknown key space that needs to be brute forced to fully compromise the protected input/output/key.

The determination of the remaining strength has three checks and leads to three possible outcomes. These three outcomes are:

1. The security level is insufficient and that cryptographic implementation cannot be claimed to be in the scope of the evaluation.
2. The security level is sufficient to allow claiming the cryptographic implementation to be in scope, but not sufficient to be always sufficient to use. Clear warning of the limitations is needed.
3. The security level is sufficient to allow claiming the cryptographic implementation to be in scope without further limitations.

2.1 Determination of remaining strength

NSCIB generally does not rate the algorithmic security level of cryptographic algorithms itself but follows the current consensus on the algorithmic security level in the open domain. The security level is expressed in security bits, and takes into account the current-best cryptanalytic attacks, translation of key sizes to the security level in bits for asymmetrical algorithms, and similar calculations for hash algorithms. See Chapter 4 for references.

The first check is on the algorithmic security level. The algorithmic security level needs to be more than 100 security bits. Failing this, the mechanism cannot be claimed for evaluations aiming at resistance against High attack potential.

The remaining checks are based on the best attack result from the evaluation: within a High attack potential (AVA_VAN.5), what is the highest amount of information the attacker gains and consequently the lowest amount of remaining security level?[2]:

- If this remaining security level is 80 security bits or less, the mechanism cannot be claimed.
- If this remaining security level is more than 100 security bits, the mechanism can be claimed as usual.
- If this remaining security level is more than 80 security bits, but is equal or less than 100 security bits, the mechanism can be claimed, but only with a warning.

In a table:

Algorithmic security level (in bits)	Remaining security level after best attack (in bits)	Cryptographic mechanism
≤ 100		Cannot be claimed
> 100	≤ 80	Cannot be claimed
> 100	> 80, yet ≤ 100	Can be claimed, with warning
> 100	> 100	Can be claimed.

2.2 Impact on Security Target and other evaluation evidence

The result on the Security Target and the other evaluation evidence is as follows:

[2] This approach pre-assumes that any bit leaked or reduced by the attacks is a bit less brute force effort. This (overly) simplifies the cost and efficiency of transferring information into the brute force attack, for reasons of clarity and assurance.

2.2.1 Out of scope of the evaluation

The ST must clearly indicate that this cryptographic implementation is out of scope of the evaluation. Especially cryptographic implementations that have an algorithmic security level of > 100 bits, i.e. those that can be expected to be sufficiently secure but aren't in this TOE, must be very explicitly excluded.

Note that any cryptographic implementations that is in the TOE but not claimed, must as usual under ASE requirements be clearly excluded.

2.2.2 In scope of the evaluation, with warning

The ST claims the cryptographic implementation as usual. The guidance documents provided to the user and the ETR for Composition provided to any composite evaluator must both clearly describe that the 100 security bits are not met, yet the more than 80 security bits are met.

To facilitate efficient composite evaluations NSCIB encourages, but does not mandate, disclosure in the ETRfC of a clear lower bound on the amount of security level still reached by the TOE.

2.2.3 In scope of the evaluation

The ST claims the cryptographic implementation as usual. Guidance on the proper usage is expected as usual.

2.3 Documentation in the Evaluation Technical Report

To clearly communicate the disposition of the cryptographic algorithms, the evaluators have to document in the ETR and ETR for Composition what cryptographic mechanisms are considered in scope, their formal key sizes, the theoretical algorithmic security level, and the lowest security level remaining after the best (partial) attack within the attack potential. Cryptographic mechanisms are to be identified with their SFRs.

Below is an example overview in the ETRs of security level of the claimed cryptographic mechanisms:

SFR	Algorithmic security level theoretically (in bits)	Remaining security level after best attack (in bits)
FCS_COP.1[AES]	>100	>100
FCS_COP.1[TDES]	>100	**>80**
FCS_COP.1[RSA]	>100*	>100*

*: The TOE supports operations with adequate key sizes to reach this level, please refer to the guidance, and national and international references.

2.4 Documentation in the Certificate Report

The Certification Report will reflect the information from the ETR by summarizing it into a statement that either:

- The remaining security level of all cryptographic functionality exceeds 100 bits, or
- For some cryptographic functionality the security level could be reduced, however the remaining security level still exceeds 80 bits.

The Certificate Report refers to the ETR for Composition for identification of the specific cryptographic functionality and its remaining security level. This approach keeps this security relevant information available to the composite evaluator and user, and does not educate a potential attacker on the weak functionality identified.

Note that as this statement constitutes relevant security information from the evaluation, it should be reflected in the user guidance.

3 Glossary of terms and abbreviations

NSCIB Nederlands Schema voor Certificatie op het gebied van IT-Beveiliging

4 References

The following references are to be included in any determination of the algorithmic security level. At the time of writing, the www.keylength.com website provides a comfortable overview for documents [1] – [8].

[1] Selecting Cryptographic Key Sizes, Arjen K. Lenstra and Eric R. Verheul, Journal Of Cryptology, vol. 14, p. 255-293, 2001.

[2] Key Lengths, Arjen K. Lenstra, The Handbook of Information Security, 06/2004.

[3] Yearly Report on Algorithms and Keysizes (2012), D.SPA.20 Rev. 1.0, ICT-2007-216676 ECRYPT II, 09/2012.

[4] Recommendation for Key Management, Special Publication 800-57 Part 1 Rev. 3, NIST, 07/2012.

[5] Mécanismes cryptographiques - Règles et recommandations, Rev. 2.03, ANSSI , 02/2014.

[6] Fact Sheet Suite B Cryptography, NSA, 09/2014.

[7] Determining Strengths for Public Keys Used for Exchanging Symmetric Keys, RFC 3766, H. Orman and P. Hoffman, 04/2004.

[8] Algorithms for Qualified Electronic Signatures, BNetzA, BSI, 01/2014 updated with BSI Draft, 10/2014.

[9] Algorithms, Key Size and Parameters Report - 2014, Enisa, November 2014.