



Australian Government

Department of Defence

Intelligence and Security - Australasian Information Security Evaluation Program

AI 002

Australasian Certification Authority

AISEP Interpretation

AI No.	002
Author	Richard Helliwell
Issue Date	11 January 2006
Status	FINAL
Version	1.0
Summary	Cryptographic testing requirements by AISEFs in Common Criteria evaluations
Reference	Common Criteria Part 1: Scope Common Criteria Part 3: ATE

Evaluation Requirement

AISEFs are now required to verify the implementation of cryptographic algorithms in Common Criteria (CC) evaluations. This will apply to all evaluations that have yet to submit a test plan. Exemptions to this requirement will be considered on a case by case basis.

Note that tasks that are exempted from this requirement will not be certified until successfully passing an internal DSD evaluation. This may require additional evaluation work to occur if issues are discovered during the DSD evaluation.

Background

CC excludes the evaluation of the strength of function of cryptographic functionality. However, the CC requires that cryptographic functionality meet the claims made by the Target of Evaluation (TOE). Thus, the implementation of the cryptographic functionality still needs to be verified without examining the strength of function.

Historically, AISEFs have not been required to verify the implementation of cryptographic algorithms. DSD has performed this aspect of the evaluation as part of its internal evaluation of a product. However, as the internal DSD evaluation focuses upon aspects that are outside the scope of the CC, this can introduce significant delays to the final certification. This was identified as an issue during the Scheme renewal process and has been addressed through recognition that the DSD internal evaluation is a separate and independent process from CC evaluations.

The following benefits are expected to arise from AISEFs undertaking this aspect of evaluation:

- reduced time frame for evaluation and certification activities;
- the AISEP will become a more competitive Scheme for undertaking security evaluations; and
- the AISEP will become more closely aligned with the practices of other CCRA certificate producing schemes.

Evaluation Guidance

Cryptographic functions should be treated in a similar manner to other security functions that are claimed by a TOE, with the following exceptions:

- Strength of cryptographic function does not need to be investigated - this includes measuring the degree of entropy in random number generators.
- Vulnerabilities associated with specified cryptographic algorithm or protocols do not need to be investigated.

The following aspects are considered to be within scope of an evaluation:

- Correct implementation of an algorithm or protocol. For instance, a cryptographic algorithm should comply with its associated standard (eg. FIPS 197 for AES).
- Vulnerabilities associated with an incorrect implementation of a cryptographic algorithm or protocol that is independent of strength of function. For example, a vulnerability that allows the complete bypass of a cryptographic algorithm is considered to be within scope.

It is expected that the majority of this assurance will be gained during testing (ATE Class). As with any other security functions, all investigations into cryptographic functionality are to be commensurate with the level of assurance being sought by the TOE.