Australian Government
Department of Defence

Defence Signals Directorate

Australasian Information Security Evaluation Program

Prevention of Modification (ADO_DEL.3) CC V2.2

Common Evaluation Methodology

11 November 2005

Version 1.1

Amendment Record

Version	Date	Description
1.0	13 October 2005	Release
1.1	11 November 2005	Releasable to AISEFs

Table of Contents

1 PREVENTION OF MODIFICATION (ADO_DEL.3) 4

1.1 OBJECTIVES 4
1.2 INPUT 4
1.3 EVALUATOR ACTIONS 4
1.3.1 ADO_DEL.3.1E 4
1.4 IMPLIED EVALUATOR ACTION 6
1.4.1 ADO_DEL.3.2D 6

1 Prevention of Modification (ADO_DEL.3)

1.1 Objectives

1 The objective of this sub-activity is to determine whether the delivery documentation describes all procedures used to maintain security and detect & prevent modification or substitution of the TOE when distributing the TOE to the user's site.

1.2 Input

2 The evaluation evidence for this sub-activity is:

a) the delivery documentation.

1.3 Evaluator Actions

1.3.1 ADO_DEL.3.1E

ADO_DEL.3.1C	The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

ADO_DEL.3-1 The evaluator ***shall examine*** the delivery documentation to determine that it describes all procedures that are necessary to maintain security when distributing versions of the TOE or parts of it to the user's site.

3 The delivery documentation describes proper procedures to maintain security of the TOE during transfer of the TOE or its component parts and to determine the identification of the TOE.

4 The delivery documentation should cover the entire TOE, but may contain different procedures for different parts of the TOE. The evaluation should consider the totality of procedures.

5 The delivery procedures should be applicable across all phases of delivery from the production environment to the installation environment (e.g. packaging, storage and distribution). Standard commercial practise for packaging and delivery may be acceptable. This includes shrink wrapped packaging, a security tape or a sealed envelope. For the distribution, physical (e.g. public mail or a private distribution service) or electronic (e.g. electronic mail or downloading off the Internet) procedures may be used.

6 Interpretation of the term "necessary to maintain security" will need to consider the nature of the TOE (e.g. whether it is software or hardware), the overall security level stated for the TOE, and the security objectives provided by the ST.

ADO_DEL.3.2C The delivery documentation shall describe how the various procedures and technical measures provide for the **prevention** of modifications, or any discrepancy between the developer's master copy and the version received at the user site.

ADO_DEL.3-2 The evaluator ***shall examine*** the delivery documentation to determine that it describes how the various procedures and technical measures provided for the prevention of modifications or any discrepancy between the developer's master copy and the version received at the user site.

7 The level of protection provided should be commensurate with the chosen component of the Vulnerability Assessment. If the TOE is required to be resistant against attackers of a certain potential in its intended environment, this should also apply to the delivery of the TOE. The evaluator should determine that a balanced approach has been taken, such that delivery does not present a weak point in an otherwise secure development process.

8 The security aspects (integrity, confidentiality, availability) relevant for the actual TOE should be derived from the security objectives defined in the ST. The emphasis in the delivery documentation is likely to be on measures related to integrity, as integrity of the TOE is always important. However, confidentiality and availability of the delivery will be of concern in the delivery of some TOEs; procedures relating to these aspects of the secure delivery should also be discussed in the procedures.

9 Cryptographic checksums or a software signature may be used by the developer to ensure that tampering or masquerading can be detected. Tamper proof seals additionally indicate if the confidentiality has been broken. For software TOEs, confidentiality might be assured by using encryption. If availability is of concern, a security transport might be required.

10 The evaluator should ensure that various active and passive procedures and technical measures are employed by the vendor to prevent (or restrict) modification of a TOE during the delivery process and in the event of a modification or modification attempt alert the recipient in some manner. It is expected that those measures will do any or all of the following:

a) Avoid or detect any tampering with the hardware and physical media shipped as the TOE.

b) Detect masqueraded deliveries of the TOE.

c) Conceal knowledge of shipment of the TOE.

d) Avoid or detect interception of the TOE during the delivery process.

e) Avoid the delay of the TOE during distribution.

11 Technical measures for the prevention and detection of any discrepancy between the developer's master copy and the version received at the user site should be described in the delivery procedures.

ADO_DEL.3.3C The delivery documentation shall describe how the various procedures allow detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user's site.

ADO_DEL.3-3 The evaluator ***shall examine*** the delivery documentation to determine that it describes how the various mechanisms and procedures allow detection of attempted masquerading even in cases in which the developer has sent nothing to the user's site.

12 This requirement may be fulfilled by delivering the TOE or parts of it (e.g. by an agent known to and trusted by both developer and user). For a software TOE a digital signature may be appropriate.

13 If the TOE is delivered by electronic download, the security can be maintained by using digital signatures, integrity checksums, or encryption.

1.4 Implied evaluator action

1.4.1 ADO_DEL.3.2D

ADO_DEL.3-4 The evaluator ***shall examine*** aspects of the delivery process to determine that the delivery procedures are used.

14 The approach taken by the evaluator to check the application of delivery procedures will depend on the nature of the TOE, and the delivery process itself. In addition to examination of the procedures themselves, the evaluator should seek some assurance that they are applied in practice. Some possible approaches are:

a) a visit to the distribution site(s) where practical application of the procedures may be observed;

b) examination of the TOE at some stage during delivery, or at the user's site (e.g. checking for tamper proof seals);

c) observing that the process is applied in practice when the evaluator obtains the TOE through regular channels;

d) questioning end users as to how the TOE was delivered.

15 For guidance on site visits see CEM Annex B.5.

16 It may be the case of a newly developed TOE that the delivery procedures have yet to be exercised. In these cases, the evaluator has to be satisfied that appropriate procedures and facilities are in place for future deliveries and that all personnel involved are aware of their responsibilities. The evaluator may request a “dry run” of a delivery if this is practical. If the developer has produced other similar products, then an examination of procedures in their use may be useful in providing assurance.