
I-0473: Ability To Obtain The Unique Identifier Of The TOE

TYPE: NIAP Interpretation
NUMBER: I-0473
STATUS: Ready for External Review

TITLE: Ability To Obtain The Unique Identifier Of The TOE
COMMENTS DUE BY: Tuesday, October 28, 2003 to cc-cmt@nist.gov

SOURCE REFERENCE: CC v2.1 Part 3 Subclause 8.2 ACM_CAP
CC v2.1 Part 3 Subclause 9.2 ADO_IGS
CEM v1.0 Part 2 Subclause 5.5.1
CEM v1.0 Part 2 Subclause 6.4.1
CEM v1.0 Part 2 Subclause 6.5.2
CEM v1.0 Part 2 Subclause 7.5.2
CEM v1.0 Part 2 Subclause 8.5.2

RELATED TO: <None>

ISSUE:

There is a disconnect between Paragraph 259 in Part 3 of the CC ("Labelling of the TOE with its reference will ensure that users of the TOE can be aware of which instance of the TOE they are using") and ACM_CAP.2.2C, which only requires that the TOE be labelled with its reference, not that any user have the ability to obtain the reference.

STATEMENT

The installing user must be able to determine that a package being installed or delivered is indeed the evaluation version, based on some form of unique identifier tied to the certificate. However, there is no requirement that, after installation, end users must have the ability to determine the unique CM identifier assigned to each component of the TOE. There is also no requirement that the unique identifier of each component of the TOE be the same as the overall TOE identifier on the certificate. The mapping of each component identifier to the overall TOE is maintained by, and visible to, CM personnel who assemble the TOE installation package for shipping.

RECOMMENDED CRITERIA CHANGES

To address this interpretation, the following changes should be made to Common Criteria v2.1, Part 3:

- In Subclause 8.2, the following changes for clarification purposes are made to paragraphs 258, 259, 261, 264, and 268 (Additions marked thusly; deletions marked ~~thusly~~):

A unique reference is required to ensure that there is no ambiguity in terms of which instance of the TOE is being evaluated. Labelling the TOE with its reference ensures that ~~the users~~ those installing the TOE can be aware of which instances of the TOE they are ~~using~~ installing. Ideally, end users will

also be provided with the ability to verify that the version of the TOE they are using has the same unique identifier of (and thus corresponds to) the version of the TOE that was evaluated, but this functional capability is not implied by the ACM_CAP components.

- ADO_IGS.1 is relabeled as ADO_IGS.1-NIAP-0473. Unless otherwise noted in these changes, all normative and informative material associated with ADO_IGS.1 is incorporated unchanged into ADO_IGS.1-NIAP-0473, and all references to ADO_IGS.1 in the CC, CEM, or other Common Criteria documentation are changed to refer to ADO_IGS.1-NIAP-0473. A similar change is made to ADO_IGS.2.
- In Subclause 9.2, ADO_IGS, the following elements are added:

ADO_IGS.1.2-NIAP-0473C. The documentation shall describe how the installer verifies that the version of the TOE being installed corresponds to the version of the TOE identified in the evaluation certificate.

ADO_IGS.2.3-NIAP-0473C. The documentation shall describe how the installer verifies that the version of the TOE being installed corresponds to the version of the TOE identified in the evaluation certificate.

The following changes should be made to CEM v1.0, Part 2:

- The following work unit is added to Subclause 5.5.1.4.1 after paragraph 531, to Subclause 6.5.2.4.1 after paragraph 680, to Subclause 7.5.2.4.1 after paragraph 976, and to Subclause 8.5.2.4.1 after paragraph 1354, with x being replaced by the appropriate EAL:

ADO_IGS.1.2-NIAP-0473C

x:ADO_IGS.1-2-NIAP-0473. The evaluation shall check that the documentation describes how the installer is to verify that the version of the TOE being installed corresponds to the version of the TOE identified in the evaluation certificate.

In order to have confidence in an evaluation, the site installing a system must be able to verify that the installer product is indeed the TOE that was evaluated. The goal of this work unit is to ensure that the installer has such an ability.

At minimum, every TOE should have a unique identification, which is specified in the ST and on the certificate issued by the evaluating scheme. Depending on ACM components selected, the TOE may also have specific configuration item versions available. In performing this work unit, the evaluator should check that the installer is provided with a procedure to verify that the version of the TOE being installed corresponds to the version on the certificate. Ideally, the installed should also be able to verify that the components that make up the TOE correspond to the components under configuration management for this version of the TOE.

- In Subclause 5.5.1.4.2, Subclause 6.5.2.4.2, Subclause 7.5.2.4.2, and Subclause 8.5.2.4.2, work unit x:ADO_IGS.1-2 is renumbered as x:ADO_IGS.1-3-NIAP-0473.

SUPPORT:

The CC requires (ACM_CAP.1.1C, ACM_CAP.1.2C) that the TOE be labeled with a unique reference. The objectives for ACM_CAP clarify one of the purposes for this reference; namely, that the users of the TOE be aware of which instance of the TOE they are using. The Configuration Management requirements also require (starting at ACM_CAP.2) that a list be maintained of the configuration items that comprise the TOE.

Based on these requirements and objectives, it is clear that what is labeled is the TOE as a whole. Individual components may have their own unique reference (version numbers), but these need not correspond to that of the overall TOE. However, in the configuration management documentation, there

should be a list of the components of the TOE (including their version numbers). There are no requirements that each component provide users with the ability to ascertain the version numbers of each component.

It is also clear that the recipient of the TOE must be able to ascertain the unique reference for the TOE delivered, presumably to verify that reference against the certificate. Ideally, the installation package would include a list of the version numbers of the components of the TOE, but as there is no mandated interface to verify these, the only way to ascertain that the evaluated TOE is installed is to reinstall the package.

Note that neither the requirements for Delivery (ADO_DEL) nor the requirements for Installation, Generation, and Startup reference the unique identifier for the TOE. This is a mistake. Part of the delivery and installation procedures should be that the recipient verifies the unique reference for the TOE.