
UK IT SECURITY EVALUATION & CERTIFICATION SCHEME

UK CC Interpretation - UK/2.3/013

1 March 2007

Status: Endorsed for use in UK Scheme

Subject: Secure electronic delivery

REFERENCES CC/CEM, Version 2.3, August 2005

Issue

1. Electronic delivery via the Internet is widely used by commercial developers for their products. It is a cost-effective and quick alternative to physically delivering media to customers.
2. The delivery medium, the Internet, is unrestricted and insecure. Consequently, any product stored in a manner accessible via the Internet and delivered to the customer over the Internet is subject to increased security risks.
3. This interpretation addresses the question of how to assess the procedures associated with the electronic delivery via the Internet of a TOE.

Scope of Interpretation

4. Graduation of the interpretation will be based upon the assurance level/possible assurance package claimed for the TOE, limited to those assurance components included in EAL4 and the ALC_FLR family.
5. This interpretation is not applicable to any hardware or firmware items (with the exception of software updates for firmware) within a TOE.
6. This issue is based upon the following premises:
 - a. It is assumed that the delivery process only takes place:
 - ◆ After product development when the final TOE has been generated;
 - ◆ Before the customer installs the TOE.
 - b. It is therefore assumed that the TOE development process results in the same TOE regardless of whether the delivery method is physical (e.g. on CDROM) or electronic (e.g. over the Internet). Consequently, the CC assurance requirements assumed to be unaffected by this interpretation, which are associated with those activities in the TOE's lifecycle that fall within the responsibility of the developer, are ASE, ADV, ATE, ACM_AUT.1, ALC_TAT and AVA_SOF.
 - c. It is therefore also assumed that the TOE installation process results in the same TOE regardless of whether the delivery method is physical (e.g. on CDROM) or electronic (e.g. over the Internet). Consequently, the CC assurance requirements assumed to be unaffected by this interpretation, which are associated with those activities in the TOE's lifecycle that fall within the responsibility of the consumer, are ADO_IGS and

AGD.

- d. This interpretation does not include TOEs that are used to provide a service over the Internet, e.g. an anti-virus product which is maintained centrally and accessed by TOE users over the Internet when necessary.

Interpretation

7. Each relevant CC Part 3 class is discussed in turn below, identifying where components are affected by the use of electronic delivery.

ACM activities

8. The configuration management assessment sub-activities are to be performed as described in CC and CEM, with the following additions:

ACM_CAP.1 ACM_CAP.2	This requirement is unchanged but applies equally to the physically delivered TOE and the electronically delivered TOE and/or TOE components.
ACM_CAP.3 ACM_CAP.4	The CM plan shall include details of how configuration items are maintained during transfer from development to, and while present on, any storage device that holds the TOE ready for download. This may include the use of checksums, but if so the means to calculate them must be sufficiently robust for the threat environment in question (e.g. MD5 is considered satisfactory for a low threat environment such as that expected for EAL 4). The TOE, any fixes or patches, customer guidance and verification information (e.g. MD5 checksum values) shall all be considered to be configuration items. Other aspects of this requirement remain unchanged but apply equally to the physically delivered TOE and the electronically delivered TOE and/or TOE components.
ACM_SCP.1 ACM_SCP.2	This requirement is unchanged but it should be noted that the TOE suitable for testing (ATE_IND.2) may be either the physically delivered TOE or the electronically delivered TOE and therefore these items should be on the configuration items list.

ADO activities

9. Transfer of the IT TOE/TOE components using the Internet provides more opportunity for interference than during physical transfer. This is due to the fact that the item is stored in a publicly accessible domain, relying on technical controls to prevent access, whereas the items for physical delivery are typically stored in a controlled environment where only a limited number of people have access. Also, interference during electronic transfer can be initiated from anywhere in the world, irrespective of the locations between which the items are being transferred; and there is no requirement to be physically present as there would be for someone to interfere during physical transfer.
10. The delivery and operation assessment sub-activities are to be performed as described in CC and CEM, with the following additions described in the table below. The delivery

procedures detail all aspects of the delivery process; those that are the responsibility of the developer and those of the consumer. These procedures are generally only available in their entirety internally to the development organisation. The delivery guidance is an extract of the delivery procedures, containing the aspects of the procedures that are the responsibility of the consumer. Any information required to verify the authenticity of the item delivered is termed the verification information, and may form part of the delivery guidance.

ADO_DEL.1	<p>The delivery procedures shall describe the procedures to be followed to securely transfer the TOE and/or its components from a storage item, e.g. Web Server, to the consumer's site via the Internet.</p> <p>The delivery procedures shall also describe the consumers' responsibilities concerning TOE delivery. This shall include how the consumer is notified of relevant details of the delivery procedures (consumer delivery guidance) and how a consumer obtains any verification information¹ required by the procedures. If the consumer delivery guidance or verification information is accessible via the Internet it shall be stored in a form which is not easily modifiable, e.g. as a PDF file. If no technical measure exists for the consumer to authenticate the website used to host delivery of the TOE (e.g. a digital certificate issued by a reputable certificate authority) then the procedures shall ensure that the consumer delivery guidance and verification information is available to all consumers via a route other than this website (e.g. specified point of contact in Customer Support). The consumer delivery guidance and verification information may also be made available through a third party controlled source, e.g. the TOE Certification Report. This may help prevent recursive issues where the guidance or verification information is required to confirm authenticity of delivered items. Either the third party source will publish the verification information on behalf of the developer or they will quote significant points of the delivery procedures that would otherwise be included in the guidance documentation.</p> <p>The procedures shall state, in general terms, the measures taken to protect the IT TOE and/or IT TOE components² during transfer across the Internet to the customer.</p> <p>In the absence of explicit threats in the ST against the delivery of the TOE the use of mechanisms such as MD5 checksums for the protection of the integrity of the IT TOE/IT TOE components during download, e.g. across the Internet, is deemed sufficient. This allows the integrity of the item to be confirmed upon receipt of the item. (It is not necessary to protect documentation with technical measures such as MD5. These measures are only required for IT portions of the TOE.)</p> <p>The evaluator shall verify the hash value generated by the developer</p>
-----------	---

1 For example, the MD5 checksum value published by the developer against which the consumer is to check the value obtained when generating the checksum for the item received.

2 IT TOE components may include patches required as part of the certified TOE.

	<p>for an item through use of an independent implementation of the algorithm as part of the delivery activities.</p> <p>The consumer is responsible for verifying the items received. If this includes verification of a checksum value such as MD5, the consumer should use a hash value calculator in which they have confidence to generate a checksum for the received item.</p> <p>The consumer and evaluator are to use an independent implementation of the algorithm rather than an algorithm downloaded with the TOE to ensure that a “spoof” algorithm is not used, which supplies the correct hash by incorrect means.</p> <p>Provided a technical mechanism verifying the integrity of the image received is sufficiently strong such that the chances of engineering a collision can be considered infeasible e.g. MD5, then it can be argued that there is no need to detect masquerade as the consumer can be confident that they have received the correct image. This relies on the assumption that verification information is distributed to the consumer via an independent mechanism to the image, i.e. the verification information is not downloaded from the same website as the TOE image.</p> <p>Other aspects of this requirement remain unchanged but apply equally to the physically delivered TOE and the electronically delivered TOE and/or TOE components.</p>
ADO_DEL.2	<p>The delivery procedures will include a description of how and why the technical measures are effective in protecting the IT TOE/IT TOE components from undetected modification and masquerade during delivery.</p> <p>Other aspects of this requirement remain unchanged but apply equally to the physically delivered TOE and the electronically delivered IT TOE and/or IT TOE components.</p>

11. It is noted that the differences between ADO_DEL.1 and ADO_DEL.2 are the inclusion of various descriptions. This is because technical measures, normally only required for ADO_DEL.2, are included in ADO_DEL.1 because download over the Internet is impossible without them.

ALC activities

12. The life-cycle assessment sub-activities are to be performed as described in CC and CEM, with the following additions:

ALC_DVS.1	<p>Any storage item, e.g. Web Server, shall be considered part of the development environment, and the protection of the TOE and/or its components while in storage waiting for download shall be fully evaluated in accordance with this assurance requirement.</p>
-----------	--

ALC_FLR.1 ALC_FLR.2 ALC_FLR.3	The delivery of flaw information, correction (e.g. patches) and guidance resulting from the application of flaw remediation procedures is governed by the guidance provided for ADO_DEL.1 above.
-------------------------------------	--

AVA activities

13. The vulnerability assessment sub-activities are to be performed as described in CC and CEM, with the following additions:

AVA_MSU.1 AVA_MSU.2	The delivery procedures visible to the TOE user shall be considered by the Misuse analysis. The assumption that TOE users are competent enough to correctly use any publicly available facilities (e.g. SSL v3.0/TLS v1.0, MD5) without further guidance is considered valid.
AVA_VLA.1	The delivery procedures shall be considered by the Vulnerability analysis with reference to the threat environment for delivery (which may vary from that for operation). Commercially available protection (SSL v3.0/TLS v1.0) and verification (MD5) mechanisms of reputable strength are considered sufficient when implemented correctly. The TOE user is responsible for this implementation on his equipment.
AVA_VLA.2	As for AVA_VLA.1 except that particular attention should be paid to vulnerabilities in any technology used by the procedures, e.g. MD5. It should also be noted that man-in-the-middle attacks, using current technology, during download over the Internet are not considered obvious penetration attacks and hence will not be carried out by an attacker with a low attack potential.