

## Research paper: Common Criteria Mutual Recognition

Mr. Keith Beatty  
Science Applications International Corporation  
Common Criteria Testing Laboratory  
May 02, 2007

---

### Abstract

The Common Criteria (CC) provides a master list of IT products that have been certified for use by all Common Criteria signatories to the Arrangement on the Recognition of Common Criteria certificates (CCRA). This master list is the sum total of the products that have been evaluated and certified by national schemes and published by each scheme's Certification/Validation Body (CB) for EAL1 through EAL4. This evaluated product list (EPL) is international in its scope and represents a one to many agreement by which each IT product listed therein having been evaluated once by a national scheme may be used by any and all consumers (internationally) without the need for further (re-) evaluation by the scheme representing the nationality (government) of the consumer. It is the responsibility of each CB to provide the CC with a list of the scheme's evaluated products and their associated certificates for publication on the CC's master EPL; it is the responsibility of the CC to list those products on its site which meet the CCRA. It is further the responsibility of each CB to provide technical support to activities relating to the Arrangement. This includes individually maintained web sites containing information pursuant to the CCRA. This information is generally, but not necessarily limited to, links providing documentation on the CC, the CCRA, and scheme evaluated product lists. The web sites are intended to provide interested parties with readily accessible information regarding the certification of IT products. It was theorized that the CCRA information contained on individual CB web sites would vary from scheme to scheme. Furthermore, it was speculated that, at EAL4, mutual recognition would break down and become national resulting in EAL4 certificates listed on scheme EPLs but not on the CC master list. An examination of the certificate authorizing CB web sites concluded that the individual schemes vary greatly in the presentation and representation of the CC/CCRA material. A comparison of the EAL4 products between the EPLs of the signatory participants and the CC did not support the original hypothesis. However, recent events within the US scheme may result in an increase national (versus international) motivation.

### Background

The National Computer Security Center (NCSC)<sup>1</sup> was established in 1981 as part of the DoD National Security Agency (NSA). One of the NCSC goals was to create a range of security ratings that could be used to indicate protection levels offered by commercial operating systems, network components, and trusted applications. In December, 1985 these ratings were set forth in a DoD Standard (DOD 5200.28-STD) entitled the Department of Defense Trusted Computer System Evaluation Criteria which came to be

referred to as the "Orange Book", or the TCSEC standard.<sup>2</sup>

The TCSEC's European counterpart was the Information Technology Security Evaluation Criteria (ITSEC) [Pfleeger, p303]. In May 1990, [France](#), [Germany](#), the [Netherlands](#) and the [United Kingdom](#) published the Information Technology Security Evaluation Criteria (ITSEC) based on existing work in their respective countries. Following extensive international review, Version 1.2 was subsequently published in June 1991 by the [Commission of the European Communities](#) for operational use within evaluation and

---

<sup>1</sup> Available at [www.radium.ncsc.mil/tpep/](http://www.radium.ncsc.mil/tpep/)

<sup>2</sup> Available at <http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html>

certification schemes. ITSEC was a structured set of criteria for evaluating computer security within products and systems. Each evaluation involved a detailed examination of IT security features culminating in comprehensive and informed functional and penetration testing.

Predictably, the efforts of these two certification bodies, along with a Canadian initiative (CTCPEC) left vendors, as well as consumers, of international breath with competing standards (certifications). Out of these ashes arose the Common Criteria whose approach closely resembled that of the US Federal Criteria which was heavily influenced by the ITSEC and Canadian efforts. [Pfleeger, p307]

The CC<sup>3</sup>, then, represents an international initiative by the following organizations: CSE (Canada), SCSSI (France), BSI (Germany), NLNCSA (Netherlands), CESG (UK), NIST (USA) and NSA (USA). It represents the outcome of efforts to develop criteria for evaluation of IT security that are widely useful within the international community.

Products commenced evaluation under the auspices of the Common Criteria in 1995 but it was not until the agreement on mutual recognition for the certification of evaluated IT products became effective on May 23<sup>rd</sup>, 2000 [CCRA, p9], that these evaluations were mutually recognized amongst the participating members of the CC. Designed to provide assurance continuity for products up to and including Evaluation Assurance Level 4 (EAL4) across national boundaries (schemes), the IT products certified under the auspices of one scheme (nation) are recognized by all other participating schemes (nations). In order for this to occur the participating schemes must agree to follow the guidelines established in the CCRA and provide supporting information on each scheme's website indicating participation in, and recognition of, the CCRA.

The CCRA permits comparability between the results of independent security evaluations. It does so by providing a common set of requirements for the security functions of IT products and systems and for assurance measures applied to them during a security evaluation. The evaluation process establishes a level of confidence that the security functions of such

products and systems and the assurance measures applied to them meet these requirements. [Common Criteria Part 1, p.7]

In order to allow for greater flexibility in the evaluation process, the Arrangement on the recognition of the Common Criteria (CCRA), also referred to as mutual recognition, was published in May, 2000. This document established an agreement among the participant members of the Common Criteria to cooperate in recognizing evaluations.

There are two different sets of participants in the Common Criteria: certificate authorizing and certificate consuming members. As the name implies, certificate authorizing members create certificates for IT products. Certificate consuming members may utilize the evaluated products but, due to the lack of a CB, cannot certify IT products; certificate authorizing members may also be certificate consumers. According to the CCRA web site, there are currently 23 members of the CC of which 12 members are certificate authorizing with the remaining 11 members designated as certificate consumers.<sup>4</sup> The initial CCRA was signed by 12 participants and included both producing as well as consuming members of the CC.

Within the certificate authorizing schemes is the responsibility of each CB to provide the CC with a list of the scheme's evaluated products and their associated certificates for publication on the CC's master EPL; it is the responsibility of the CC to list those products on its site which meet the CCRA. It is further the responsibility of each CB to provide technical support to activities relating to the Arrangement.

The CCRA is currently utilized, almost exclusively, by defense-related organizations within the governments of each of the certificate authorizing countries. However, with the inclusion of newer certificate consuming members of the CC community, it is unclear if this will continue to be the case. For instance, the Turkish site <http://www.tse.org.tr/english/tsedefault1.asp> appears to indicate a use of the CCRA in conjunction with European ISO standards for IT security purposes other than those which are

---

<sup>4</sup>List of CCRA members:  
<http://www.commoncriteriaportal.org/public/consumer/index.php?menu=4>

---

<sup>3</sup> Available at [www.commoncriteriaportal.org](http://www.commoncriteriaportal.org)

strictly defined as defense-related initiatives and programs. Hungary, another new consumer <http://www.tse.org.tr/english/tsedefault1.asp> appears to be using its CCRA membership to solicit investment capital for its Ministry of Economy and Transport.

### Alternatives and Impact

Members of the CC that wish to participate in the CCRA agree to share the following objectives [CCRA, p4]:

- a) to ensure that *evaluations of Information Technology (IT) products and protection profiles* are performed to high and consistent standards, and are seen to contribute significantly to confidence in the security of those products and profiles;<sup>5</sup>
- b) to improve the availability of evaluated, security-enhanced IT products and protection profiles;
- c) to eliminate the burden of duplicating evaluations of IT products and protection profiles;
- d) to continuously improve the efficiency and cost-effectiveness of the evaluation and *certification/validation* process for IT products and protection profiles.

The purpose of the Arrangement is to advance the objectives above in order to create an atmosphere in which IT products (and protection profiles) may be used without the need for further evaluation. However, it is recognized that for certain sensitive government systems the procurement, certification, and recognition of such products will be accomplished according to separate bilateral or multilateral arrangements/agreements.<sup>6</sup>

The CCRA recognizes this and does not constrain any such agreements. However, it does encourage the various participants (certificate authorizing members particularly) to “endeavour to work actively to improve the application of the criteria and methodology, for example by developing and establishing more *cost-effective* assurance packages, and by identifying and

*discarding requirements that do not make a significant contribution to assurance.* The Participants also plan to advance the *economical reuse of evaluation output*” [CCRA, p4 - *emphasis added*].

The significance of the CCRA is that there are now over 650 products listed as mutually recognized on the CC EPL<sup>7</sup>. This number does not include those products which are certified by schemes but are not candidates for mutual recognition. The mutual recognition evaluation and certifications alone represent a significant investment by at least a portion of the certificate authorizing community in certification as well as international cooperation and recognition. If the CCRA is to be believed, then these 650 evaluations represent certifications for IT security products that, for the particular configurations evaluated, will not have to be duplicated by other certificate authorizers. This is significant in that, for example, a product certified in the Republic of Korea, may be used in Defence Signals Directorate effort in Australasia.

Because the EPL represents a one to many agreement by which each IT product listed therein having been evaluated once by a national scheme may be used by any and all consumers (internationally) without the need for further (re)evaluation by the scheme representing the nationality (government) of the consumer; one presumes that this would result in cost savings by avoiding what is commonly referred to as “reinventing the wheel”.

Examination of the CCRA results above would appear to indicate a robust level of international cooperation and recognition. An average of approximately 90 certificates per year appearing in the CCRA (2000 to current) seems to point to the continuation of the CCRA in, at least, the near term. If conferences are any measure of successful programs, then it should be noted that the International Common Criteria Conference will convene for its eighth annual symposium this fall. Additionally, the list of certificate authorizing as well as certificate consuming members continues to grow.

<sup>5</sup> Analysis of Protection Profiles was not included in this paper; it remains a potential topic for future investigation.

<sup>6</sup> CCRA, p.4.

<sup>7</sup> CCRA EPL:  
<http://www.commoncriteriaportal.org/public/consumer/index.php?menu=5>

However, as with all things, there are multiple issues and consequences at work. Because of the large number of mutually recognized products, it is incumbent upon the individual schemes to correctly represent the CCRA information in a timely fashion. This includes individually maintained web sites containing information pursuant to the CCRA. This information is generally, but not necessarily limited to, links providing documentation on the CC, the CCRA, and scheme evaluated product lists. The web sites are intended to provide interested parties with readily accessible information regarding the certification of IT products.

As shown in Table 1, located at the end of this paper, an examination of the individual scheme web sites revealed a number of inconsistencies arising across schemes. The issues relate directly to the ability of interested parties being able to navigate a particular scheme's web site and find a link to the CC's master list of certified products. The master list represents the sum total of the products that have been evaluated and certified by national schemes and published by each scheme's Certification/Validation Body (CB) for EAL1 through EAL4.

The issues include:

- member lists posted that are incomplete relative to the CC web site
- EPL web pages out of date
- lack of pointers to the EPL
- language issues (English only on sites with large EPLs)
- missing or hidden CCRA links
- lack of uniformity in web page design

Nor were these issues confined to the CCRA members. The CC webpage was found not to contain current links for all of the participants (consumers). In these cases email contacts were provided. However, this represents more inconsistency in the approach; for every space on the CCRA members list, there should be an accompanying URL.\

As previously stated, the CCRA acknowledges that there are circumstances under which products will not qualify for mutual recognition. Individual countries appear to apply this process differently and across EALs. Examining the certificate authorizing schemes bears this out. The European contingent (France, Germany, the UK) all have separate evaluation results that

have not been submitted through the CCRA process. Australia/New Zealand scheme takes certified products and applies, where necessary, an additional cryptographic evaluation to each product.

It was assumed that any delta in the CCRA would most clearly be exhibited at EAL4. Table 1 (EAL4 column) shows an examination of the individual scheme certifications at EAL4 against those EAL4 certifications listed on the CC master EPL. This revealed, some what surprisingly, that aside from France, there were relatively few differences between the EAL4 products listed on an individual scheme site and those appearing on the master list. This leads to a negative conclusion to that part of the original hypothesis which stated that at EAL4 national interests would be more clearly reflected than those of mutual recognition

However, recent events in the United States may give rise to a greater concern than EAL4 certifications. Of the 650+ certificates listed on the CC EPL, over 180 evaluations were produced in the US<sup>8</sup>. This appears to have placed a tremendous strain on the budget of the CB (NIAP). In the fall of 2006, NIAP issued the following statement:

*Due to fiscal constraints, beginning on October 1, 2006, for FY07, the NIAP CCEVS will only accept Medium and High Robustness PP compliant products in support of National Security customers. Product submissions meeting the above criteria will be queued and validation resources will be allocated as they become available. As a condition of acceptance, detailed letters of intent that identify the intended DoD or IC customer (containing POC name, organizations, email, phone number) will be required<sup>9</sup>.*

This statement limiting evaluations to Medium and High Robustness PP compliant products is a cause for significant concern. Medium and High Robustness PPs contain explicit Assurance requirements. NIAP goes on to state:

---

<sup>8</sup>NIAP Validated Products List:

<http://www.niap-ccevs.org/cc-scheme/vpl/>

<sup>9</sup> NIAP announcement: <http://www.niap-ccevs.org/cc-scheme/>

Assurance is approximately EAL4: EAL4 (v2.3) with explicitly-stated versions of ADV\_FSP.2, ADV\_HLD.2, ADV\_LLD.1, augmented with ADV\_IMP.2, ALC\_FLR.2, ATE\_DPT.2, AVA\_VLA.2, and the explicitly-stated component ADV\_ARC, and (if the TOE includes cryptographic functionality) an explicitly-stated versions of AVA\_CCA.1. The characteristics of medium robustness are further explained in the *Consistency Instruction Manual for development of US Government Protection Profiles for use in Medium Robustness Environments*<sup>10</sup>

These explicit requirements (and an “approximate” EAL4) are outside of the purview CCRA which means that any product certified under the above conditions will not qualify for the CC master list. Whether fiscally constrained or not, this is an action that could have the consequence of nationalizing certifications in the US across all EALs – not just EAL4.

It is unclear what, if any, other motivation(s) may be behind this decision other than a budgetary crisis. Unfortunately it does have the immediate perceptual impact that NIAP (and in particular its handler the NSA) is attempting to aggressively restructure the validation process both here and abroad. Regardless, this open-ended decision by the US scheme has the potential impacts:

- duplicate effort in product certification;
- (re)nationalize certification;
- Shift “low end (EAL2/3) evaluation work from this country elsewhere

If the latter comes to pass, there could be significant economic impact on the CC testing laboratories here in the US.

The issue of restrictive certificates in the US scheme does provide for a number of alternatives. First, if the issue is truly one of fiscal constraint, then creating a commercial entity within (at least) the US scheme (within NIST?) for certifying products (EAL1-EAL4) would ease the burden on NIAP (and the NSA). According to the CCRA, it is accepted that both

governmental and non-governmental CBs are potentially capable of performing trustworthy certification/validation [CCRA, p.4]. Institution of a fee for service approach is another method by which the apparent fiscal issues could be eliminated. As a third alternative, the US could choose to pull out of the CCRA and/or the CC. Finally, the entire evaluation community could decide that it was time to throw the entire CC effort away and look to create a new certification and validation framework in much the same way that TCSEC and ITSEC evolved into the Common Criteria effort.

The tradeoffs to any of the approaches above involve the ability to sell the ideas to the parties most impacted by any change. For instance, the idea of a “fee for service” as a basis for certifications has been, according to one source within SAIC, “kicking around since the CC was established.” Vendors, already wary of the significant cost in performing an evaluation are notoriously hesitant to any change that might be perceived as costing money. In this regard, on a personal and unsubstantiated note, I was raked over the proverbial coals at a conference last spring because I represented the “slow, expensive, and useless (except for the piece of paper that I need to do business)” Common Criteria. In point of fact, who really needs another “standard”?

### **Analysis and Recommendation**

Based upon the analysis of the certificate authorizing web sites, it is possible to conclude that the CCRA has been successful and will continue to be so in the near term. However, there is a disconnect between the CC and the individual schemes in how the CC is represented. Whether this is due to a lack of funding, voluntary effort, politics, or other, the fact remains that the CC’s web-facing representation varies from scheme to scheme. That it has brought, and continues to bring, a level of international cooperation to the IT security appears to be obvious. It would be an interesting exercise to attempt to calculate the actual economies derived from mutual recognition. However, the existence of 650+ certified IT security products listed anywhere, let alone on one site, would appear to argue for, if nothing else, an organizational benefit let alone a potential economic benefit.

---

<sup>10</sup>Robustness Frequently Asked Questions (FAQs): <http://www.niap-ccevs.org/cc-scheme/faqs/faqs-robustness.cfm>

The CC started with 7 nations; it is now 23 nations strong. If it continues to grow, and the sense is that it will continue to do so, the CC will need to encourage the individual schemes to improve their customer-facing abilities as well as encourage more active participation amongst the certificate authorizing members in order to relieve some of the burden on those nations whose schemes (US and France come to mind) make up the bulk of the certification efforts.

Adding new members will be somewhat tricky. It is not in the best interest of the CCRA to become an advertisement clearing house ala the Hungarian website.

Therefore, it remains the conclusion of this investigation that, particularly given the size of the CC EPL, the schemes should be looking to establish some form of commercial, non-governmental/defense certification body. Splitting the CC into two bodies with a defense/non-defense posture would allow the current methodology (defense) to continue to exist while potentially soliciting customers (and other interested parties) from the commercial space thereby ensuring a longer, healthier life for the CC effort.

If the process was commercialized, then EAL2 and EAL3 level certifications could come to be viewed as commodities; EAL4, entailing a more rigorous effort could continue to be focused on defense-related products. This would also allow for EAL4 to become the level at which national interests are more directly served and could, possibly, eliminate the need for medium and high robustness Assurance requirements.

The problem with this approach, of course, is in convincing vendors to allow their products to undergo the rigors and (prohibitive) expense of a CC certification effort.

Finding examples of commercial companies that have embraced the CC as a means of certifying their products is the challenge; no one certifies for altruistic motives. Nevertheless, finding companies willing to use the CC for commercial certification is possible.

A case study for this is the evaluation of the InterSystems' Cache product<sup>11</sup>. Cache is a

commercial database application primarily sold to healthcare customers. Because it is a database product that nominally competes with Oracle for market share in the healthcare space, InterSystems made the apparent decision to certify this product at the same EAL level as Oracle. However, upon examination of the InterSystems web site, no apparent defense-related motivation could be ascertained. This appears to be a case of a commercial company using the CC for purposes of making (their) applications more valuable. InterSystems Cache was listed on the CC master EPL as of 15feb07.

Hopefully, the precedent that the Cache product represents will lead to more commercial use of the CC/CCRA. Due to the rigor of the certificate effort this could lead to the CC making inroads into the heretofore unexplored commercial space. In turn, this could bring more work into the schemes and, potentially, cause them, particularly the US scheme, to evolve in a manner that will allow the commercial space to utilize a time-tested validation and certification methodology.

Personally, I can not think of a better reference for a commercial product that to state that a product certified by the CC and recognized internationally "Is good enough for the NSA." The potential economic opportunities afforded (US) companies in the international markets, particularly with India now a certificate consuming member, should be enough motivation to ensure the continuing evolution of the CCRA both her and abroad..

As a final note on my initial hypothesis, I would like to admit to being extremely naïve when I started this investigation. I didn't realize that recognition of national interests (in the form of bilateral and multilateral agreements) was already embedded in the CCRA. In my current work I am not privy to daily CC information, despite my interest in the Common Criteria as a legitimate means of comparing IT security products. What I learned here is two fold:

- all evaluations have a national component and
- each nation has its own, rather unique, way of presenting the CCRA.

---

<sup>11</sup> InterSystems - <http://www.intersystems.com/cache/security/index.html>

Table 1<sup>12</sup>: Scheme Web Site Data

<b>Producing Country</b>	<b>CB</b>	<b>CCRA<sup>13</sup></b>	<b>CC EPL link<sup>14</sup></b>	<b>Scheme EPL</b>
Australia/New Zealand	DSD	yes	Portal	Yes
Canada	CSE	yes	Portal	Yes
France	DCSSI	yes	Portal	Yes
Germany	BSI	yes	Portal	yes
Japan	JISEC	??	Product	Yes
Republic of Korea	ITSCC	yes	Scheme list??	Yes
Netherlands	TNO??	no	No	No
Norway	SERTIT	yes	No	Yes
Spain	CCN	No	Portal	Yes
UK	CESG	yes	Portal	Yes
US	NIAP	yes	Portal	Yes

Table 1 continued

<b>Producing Country</b>	<b>EAL4 not on CC EPL</b>	<b>List page last modified<sup>15</sup></b>	<b>CC Member list<sup>16</sup></b>	<b>Language(s) available</b>
Australia/New Zealand	3/8	29sep06	Partial	Eng
Canada	0/9	06mar07	Yes	Eng/Fr
France	23/79	27jul05	Partial	Fr/Gr/Sp/Eng
Germany	n/a	n/a	No	Gr/Eng
Japan	3/5	19apr07	no	Jap/Eng
Republic of Korea	2/9 <sup>17</sup>	Unknown	Yes	Kor/Eng
Netherlands	n/a	Unknown	No	Dutch
Norway	1/1	Unknown	partial	Nor/Eng
Spain	2/6 <sup>18</sup>	Unknown	No	Sp/Eng
UK	5/39	2006	Through portal	Eng
US	1/54 <sup>19</sup>	Unknown	Through portal	Eng

<sup>12</sup> List of Schemes: <http://www.commoncriteriaportal.org/public/consumer/index.php?menu=7>

<sup>13</sup> The CCRA is listed on the scheme site

<sup>14</sup> Through CC portal to developers link to General Information to link for Evaluated Products.

<sup>15</sup> Last date that the Scheme EPL was updated

<sup>16</sup> Must match CC Scheme list for producing countries at

<http://www.commoncriteriaportal.org/public/consumer/index.php?menu=7>

<sup>17</sup> 2 products certified in April, 2007 not yet listed on CC EPL.

<sup>18</sup> 4 products currently undergoing (lengthy) evaluations – not yet certified.

<sup>19</sup> 8 EAL4 products were listed under different certification report numbers (VIDs) on the CC EPL.

Table 2: Scheme Evaluated Product URLs

Producing Country	EPL URL
Australia/ New Zealand	<a href="http://www.dsd.gov.au/infosec/evaluation_services/epl/epl.html">http://www.dsd.gov.au/infosec/evaluation_services/epl/epl.html</a>
Canada	<a href="http://www.cse-cst.gc.ca/services/common-criteria/trusted-products-e.html">http://www.cse-cst.gc.ca/services/common-criteria/trusted-products-e.html</a>
France	<a href="http://www.ssi.gouv.fr/en/confidence/certificats.html">http://www.ssi.gouv.fr/en/confidence/certificats.html</a>
Germany	<a href="http://www.bsi.bund.de/literat/doc/vshardw/TL_03305eng.pdf">http://www.bsi.bund.de/literat/doc/vshardw/TL_03305eng.pdf</a>
Japan	<a href="http://www.ipa.go.jp/security/jisec/jisec_e/certfy_list.html">http://www.ipa.go.jp/security/jisec/jisec_e/certfy_list.html</a>
Republic of Korea	<a href="http://www.kecs.go.kr/">http://www.kecs.go.kr/</a>
Netherlands	Not available
Norway	<a href="http://sertit.no/article/4/">http://sertit.no/article/4/</a>
Spain	<a href="http://www.oc.ccn.cni.es/certificacion_en.html">http://www.oc.ccn.cni.es/certificacion_en.html</a>
UK	<a href="http://www.cesg.gov.uk/site/iacs/index.cfm?menuSelected=1&amp;displayPage=151">http://www.cesg.gov.uk/site/iacs/index.cfm?menuSelected=1&amp;displayPage=151</a>
US	<a href="http://www.niap-ccevs.org/cc-scheme/vpl/">http://www.niap-ccevs.org/cc-scheme/vpl/</a>

## Bibliography

Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security. May 2000. <http://www.commoncriteriaportal.org/public/files/cc-recarrange.pdf>

Assurance Continuity: CCRA Requirements. v1.0. CCIMB-2004-02-009. February, 2004. <http://www.commoncriteriaportal.org/public/files/2004-02-009.pdf>

Common Criteria: List of CCRA members. <http://www.commoncriteriaportal.org/public/consumer/index.php?menu=4>

Common Criteria. List of Evaluated Products. <http://www.commoncriteriaportal.org/public/consumer/index.php?menu=5>

Common Criteria. List of Schemes. <http://www.commoncriteriaportal.org/public/consumer/index.php?menu=7>

Common Criteria. List of Schemes In Australia and New Zealand. <http://www.dsd.gov.au/infosec>.

Common Criteria. List of Schemes In Canada. <http://www.cse-cst.gc.ca/services/common-criteria/common-criteria-e.html>

Common Criteria. List of Schemes In France. <http://www.ssi.gouv.fr>

Common Criteria. List of Schemes In Germany. <http://www.bsi.bund.de>

Common Criteria. List of Schemes In Japan. [http://www.ipa.go.jp/security/jisec/jisec\\_e/index.html](http://www.ipa.go.jp/security/jisec/jisec_e/index.html)

Common Criteria. List of Schemes In the Republic of Korea. <http://www.kecs.go.kr>

Common Criteria. List of Schemes In the Netherlands. <http://www.tno-certification.nl>

Common Criteria. List of Schemes In Norway. <http://www.sertit.no/>

Common Criteria. List of Schemes In Spain. <http://www.oc.ccn.cni.es>

Common Criteria. List of Schemes In the United Kingdom. <http://www.cesg.gov.uk>

Common Criteria. List of Schemes In the United States. <http://www.niap-ccevs.org>

Common Criteria. Part 1: Introduction and general model. August 2005, v2.3. CCMB-2005-08-001. <http://www.commoncriteriaportal.org/public/files/ccpart1v2.3.pdf>

InterSystems Cache: <http://www.intersystems.com/cache/security/index.html>

Pfleeger, Charles P. and Pfleeger, Shari Lawrence. Security in Computing. Prentice Hall, 2004, fourth edition.

Robustness Frequently Asked Questions (FAQs). <http://www.niap-ccevs.org/cc-scheme/faqs/faqs-robustness.cfm>

Medium Robustness Environments. [http://www.niap-ccevs.org/cc-scheme/pp/PP\\_FW\\_MR2.0\\_V1.0.cfm](http://www.niap-ccevs.org/cc-scheme/pp/PP_FW_MR2.0_V1.0.cfm)