

CCEVS vs. C&A: The Alphabet Soup Decoded

August 2005



1. Introduction

The Common Criteria Evaluation Validation Scheme (CCEVS) and the U.S. Government certification and accreditation (C&A) processes are “sister” processes with a few, very significant differences. In general, both processes are formal approaches toward risk management. The CCEVS process is oriented toward “evaluating” a product¹ (hardware and software) independent of its environment and is inflexible in the requirements that are being met. The C&A process is oriented toward “accrediting” a whole system in a specific environment (e.g., hardware, software, processes, procedures, facilities, training) and allows the Government accreditors some level of discretion as to how much risk they are willing to accept. Because the C&A process targets an entire system in a particular environment, rather than a specific product (regardless of whether the product is a large or small component of the system), it is never correct to state that a *product* is “accredited.” Vendors who claim that their product(s) are “accredited by DIA” or “certified by NSA” or other similar claims are technically inaccurate. They should state that their product is part of an accredited system. In addition to possibly being part of an accredited system, a product may or may not also be “evaluated” under the CCEVS. A better understanding of the differences between these two processes will help Government buyers separate fact from fiction when interacting with commercial-off-the-shelf (COTS) vendors and Government-off-the-shelf (GOTS) suppliers.

2. CCEVS

The CCEVS process involves evaluating² a product. Evaluation is defined as follows:

Evaluation – [A process of] assessing degrees of effectiveness of hardware and software security controls built into an automated information system (AIS). [NST92] The technical analysis of a component's, product's, subsystem's, or system's security that establishes whether or not the component, product, subsystem, or system meets a specific set of requirements. A security analysis of a component against a given set of standards or criteria without regard to the environment. [NCSC94]

The U.S. performs evaluations using the CCEVS process, which is executed by commercial Common Criterial Testing Laboratories (CCTLs) with oversight from a Government body (i.e., CCEVS). The focus of the CCTLs is on confirming that a product meets a given set of functional and assurance security requirements that are drawn from the Common Criteria (CC) [CC04] and captured in a Security Target (ST). The ST can also include characteristics that must be present in the environment where the product is used, but these characteristics are not verified.³

The ST might claim to meet an Evaluation Assurance Level (EAL), which is a particular grouping of CC assurance requirements. EALs describe the level of rigor that went into developing and evaluating a

-
1. It is possible for a group of products to be evaluated, but it is rare for more than a single product to be evaluated.
 2. The term “certification” is also associated with the CCEVS process because a product that successfully completes the process is issued a “certificate.” TCS uses the term “evaluation” in this document for clarification.
 3. These environmental characteristics must be taken into consideration during a C&A effort.

product (e.g., modularity, reviews, testing, documentation), independent of the functionality that the product provides. It is important to note that an EAL says nothing about “what” the product does – it just describes how much effort went into assuring that the product provides the claimed security functionality.

The ST might also claim to meet one or more Protection Profiles (PPs), which are particular groupings of CC functional requirements (e.g., identification and authentication, discretionary access control, mandatory access control) plus an EAL. A PP is the customer’s way of saying “I want;” an ST is the product developer’s way of saying “I provide.” Example PPs include the Controlled Access Protection Profile (CAPP), the Labeled Security Protection Profile (LSPP), and the Role-Based Access Control (RBAC) Protection Profile. A PP provides a comparison point for customers when they are considering which product(s) to pursue to meet their functional needs.

CCTLs review design documentation and source code, examine development processes and procedures, and perform numerous technical tests on the product they are evaluating. There is typically a good bit of interaction between the product developer and the CCTL to demonstrate compliance and address deficiencies. Once the CCTL confirms that all of the requirements in the ST have been met and the CCEVS validates the CCTL’s work, the CCEVS issues a certificate stating the PPs, EALs, and other CC requirements met by the product. The product is then considered “evaluated.”

3. U.S Government Accreditation

The U.S. Government accreditation process involves certifying and accrediting a whole system in a particular environment. Certification and accreditation are defined as follows:

Certification – A comprehensive analysis of the technical and nontechnical security features of an AIS and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements. [NST92] Note: Certification is done in support of the accreditation process and targets a specific environment. A security analysis of a system against a given set of security requirements in a given environment. [NCSC94]

Accreditation – A formal declaration by a Designated Approving Authority (DAA) that an AIS is approved to operate in a particular security mode using a prescribed set of safeguards. [NST92] Note: Accreditation is the formal declaration by a DAA that a system is approved to operate: (a) in a particular security mode; (b) with a prescribed set of countermeasures (e.g., administrative, physical, personnel, COMSEC, emissions, and computer security controls); (c) against a defined threat and with stated vulnerabilities and countermeasures; (d) within a given operational concept and environment; (e) with stated interconnections to other systems; (f) at an acceptable level of risk for which the accrediting authority has formally assumed responsibility; and (g) for a specified period of time. [NCSC94]

In the U.S., the C&A process is executed by Government personnel serving in pre-defined roles: Designated Approving Authority (DAA), Certification Authority (CA), Program Manager (PM), and User Representative. Different Government organizations participate in the C&A process and use different C&A approaches depending on the type of system that is being accredited:

- Department of Defense (DoD) personnel use the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) [DoD97] to accredit Unclassified, Secret, and Top Secret systems.
- Defense Information Systems Agency (DISA) and National Security Agency (NSA) personnel are part of the Secret and Below Interoperability (SABI) C&A process [SABI00], where additional DITSCAP-based C&A activities are performed if a cross domain solution (CDS) touches a Secret or Top Secret network.⁴
- Intelligence Community (IC) personnel use the Director of Central Intelligence Directive (DCID) 6/3 [DCID02] C&A approach to accredit Top Secret / Sensitive Compartmented Information (SCI) systems.
- Defense Intelligence Agency (DIA), Central Intelligence Agency (CIA), NSA, and other personnel are part of the Top Secret SCI and Below Interoperability (TSABI) C&A process [TSABI00], where additional DCID 6/3-based C&A activities are performed if a CDS touches a Top Secret SCI network.⁵

C&A evidence is captured in a System Security Authorization Agreement (SSAA), which includes a number of appendices. Some of the SSAA appendices are a Security Requirements Traceability Matrix (SRTM), C&A Test Procedures (technical and non-technical), Test and Evaluation (T&E) Report, and a Site Security Management Plan (SSMP). The SRTM captures security requirements that are drawn from applicable government documents like DoDD 8500.2 [DoD03], NSA Guard Security Requirements [NSA04], and DCID 6/3. It turns out that many of the requirements in the SRTM are very similar to CC requirements, especially those that are technical. The C&A Test Procedures demonstrate compliance with the requirements in the SRTM, and the results of executing those tests are captured in the T&E Report. The SSMP captures site-specific policies and procedures that are primarily non-technical.

The CA reviews all of the C&A evidence and provides a recommendation to the DAA about whether the residual risk associated with the system in its environment is acceptable. The recommendation is primarily based on the results of various testing activities. Technical testing activities are conducted in a laboratory environment to examine the compliance of the product(s) used in the system. This kind of testing is similar to the testing performed by the CCTLs.⁶ For example, NSA might conduct a Certification Test and Evaluation (CT&E) activity⁷ or DIA might perform a Beta I activity. Non-technical testing

4. The SABI C&A process has officially changed its name to the CDS C&A process. Since “CDS” is a generic term that applies to many C&A processes (e.g., Top Secret SCI and Below Interoperability), TCS uses the term SABI in this document for clarification.

5. The National Institute for Standards and Technology (NIST) is also developing a C&A process for civilian Government systems.

6. C&A laboratories emphasize penetration tests that C&A personnel write, and CCTLs emphasize more formal requirements-based tests that developers write. The similarity is that both approaches perform intense technical testing one time in a laboratory environment, resulting in a test report that is valid for all customers that use a particular product version.

7. NSA CT&E activities are what customers mean when they ask, “Has NSA looked at it?” It is important to note that NSA does not “approve” anything – NSA conducts testing and provides the results of that test as input to a risk management decision.

activities are conducted on-site to examine the compliance of the system with required policies and procedures. This kind of testing focuses on proper configuration of the product(s) and on the SSMP details. For example, the site might conduct a Security Test and Evaluation (ST&E) activity or DIA might perform a Beta II activity.

The DAA reviews the CA's recommendation and makes an accreditation decision (e.g., Interim Authority to Operate (IATO)). This accreditation decision is based on the urgency of the mission being executed at the particular site, the anticipated threats at the site, the technical protection mechanisms provided by the products in the system, and the environmental protection mechanisms provided by the policies, procedures, and physical plant at the site. If the DAA determines that the residual risk is acceptable, he or she grants approval and the overall system at that particular site is then considered "accredited."

4. Comparing the Two Processes

Now that we have covered the "alphabet soup" terms associated with each process, this section provides some important comparison points.

4.1. Products can be Evaluated, but not Accredited

A product can be evaluated under the CCEVS process, but it can only be accredited as part of a whole system in a particular environment. On the other hand, whole systems can be evaluated, but the cost-benefit tradeoff rarely makes this option attractive.

4.2. The Two Processes are Independent

Completing the CCEVS process does not satisfy the U.S. Government accreditation process, and vice versa. In theory, the time and cost associated with a C&A effort is reduced if evaluated products are used in the system. Evaluated products are not required, however, to successfully complete a C&A effort.

4.3. Separate Technical Testing is Required

CCTLs perform intense technical testing on products that go through the CCEVS process. Government testers perform intense technical testing (e.g., CT&E, Beta I) on the products that make up a system going through the accreditation process. The CCTL testing does not satisfy the technical testing required by the C&A process. All products (evaluated or not) must go through full technical testing as part of the C&A process.

4.4. Separate Approval Bodies between Evaluation and Accreditation

The CCEVS determines that a product meets the evaluation requirements, and that decision is valid anywhere. The DAA determines that a whole system meets the accreditation requirements, and that decision is valid for a particular environment.

4.5. Separate Approval Bodies within Accreditation

The accreditation approval body is dependent on the classification of the information being processed and on the networks that the system touches. The approval body can be a local DAA (at a particular site) or a "group" DAA (e.g., DSAWG, DICAST). Satisfying one approval body does not mean that any other approval body will be satisfied.

5. Summary

The CCEVS and the C&A processes are “sister” processes that address risk. The CCEVS process focuses on “evaluating” a product independent of its environment, and the C&A process focuses on “accrediting” a whole system in a particular environment. Evaluated products can benefit the process of accrediting a system in its environment, but it is never correct to state that a *product* is “accredited.” Vendors should say that their product is part of an accredited system.

References

- [CC04] Common Criteria Project Sponsoring Organizations, *Common Criteria for Information Technology Security Evaluation*, Version 2.2, Revision 256, January 2004.
- [DCID02] Director of Central Intelligence Directive (DCID) 6/3, *Protecting Sensitive Compartmented Information within Information Systems*, April 2002.
- [DoD97] DoD Instruction 5200.40, *DoD Information Technology Security Certification and Accreditation (C&A) Process (DITSCAP)*, 30 December 1997.
- [DoD03] DoD Directive 8500.2, *Information Assurance (IA) Implementation*, 6 February 2003.
- [NSA04] National Security Agency (NSA) Network Infrastructure Products and Technology Division, *Guard Certification Test and Evaluation (CT&E) Handbook*, Version 3.0, 30 September 2004
- [NCSC94] NCSC-TG-029, *Introduction to Certification and Accreditation*, Version 1, January 1994.
- [NST92] National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4009, *National Information Systems Security (INFOSEC) Glossary*, June 1992.
- [SABI00] SABI Guidelines, *Secret and Below Interoperability (SABI) [Guidance CD-ROM]*, Version 1.0, June 2000.
- [TSABI00] Office of the Intelligence Community Chief Information Officer, *Top Secret/Sensitive Compartmented Information (SCI) And Below Interoperability Policy (TSABI)*, Version 3, 7 February 2000.