Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Common Criteria and Protection Profiles: How to Evaluate Information

The purpose of this paper is to discuss the standards of Common Criteria and the security framework provided by the Common Criteria. In addition, this paper will review the background and applicability of Common Criteria Protection Profiles established to evaluate specific Information Technology (IT) functional and assurance security requirements. The Common Criteria (CC) security framework establishes a methodology to apply security standards to an IT system or product and establishes the understanding of how specific...

Copyright SANS Institute
Author Retains Full Rights

AD

Common Criteria and Protection Profiles: How to Evaluate Information Technology Security

Kathryn Wallace
Practical Version 1.4b

Summary

The purpose of this paper is to discuss the standards of Common Criteria and the security framework provided by the Common Criteria. In addition, this paper will review the background and applicability of Common Criteria Protection Profiles established to evaluate specific Information Technology (IT) functional and assurance security requirements. The Common Criteria (CC) security framework establishes a methodology to apply security standards to an IT system or product and establishes the understanding of how specific Protection Profiles (PP) fit into the overall CC process.

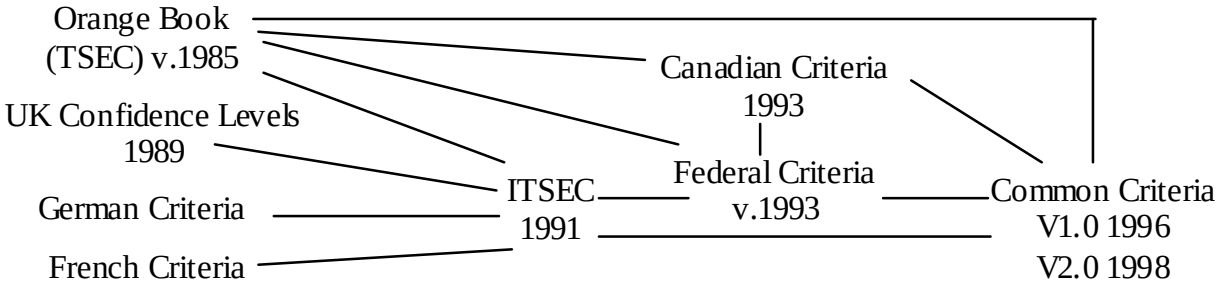
CC baselines activities for IT systems and products assurance evaluations. Developers, consumers, or evaluators of IT systems and products may use the CC security framework to institute a level of security assurance. This paper will document the CC process and explore its importance to IT security.

Common Criteria Overview

Common Criteria (CC) is the set of internationally and nationally recognized technical standards and configurations that allow for security evaluations of Information Technology (IT) products and technology. The individual set of common criteria technical standards or configurations developed for a specific product or technology is qualified as a protection profile.

The first set of United States Federal technical standards for security evaluations was the DoD Trusted Computer System Evaluation Criteria (TCSEC) commonly referred to as the "Orange Book published in August 1983.[i] Independently, organizations in other countries were developing IT standards for their own governments to use. In June 1993, the sponsoring organizations of the existing US, Canadian, and European criterias started the CC Project to align the separate standards into a single set of IT security criteria.[ii]

Figure 1: Common Criteria Source Documents Development[iii]



© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The following seven governmental organizations (collectively called "the Common Criteria Project Sponsoring Organizations") are joint holders of the copyright of CC for IT security evaluations and retain the right to use, distribute, translate, and modify the CCs they see fit.[iv]

Canada:	Communications Security Establishment (CSE)
France:	Direction Centrale de la Securite des Systemes d'Information (DCSSI)
Germany:	Bundesamt für Sicherheit in der Informationstechnik (BSI)
Netherlands:	Netherlands National Communications Security Agency NLNCSA)
United Kingdom:	Communications-Electronics Security Group (CESG)
United States:	National Institute of Standards and Technology (NIST
United States:	National Security Agency (NSA)[v]

The international community enforces the standards of the CC through the Common Criteria Recognition Arrangement (CCRA), which states that participating members agree to accept the results of CC evaluations performed by other CCRA members.[vi]

The National Institute for Standards and Technology (NIST) and the National Security Agency (NSA) jointly operates United States CC activities under the National Information Assurance Partnership (NIAP). NIAP is a U.S. Government initiative designed to meet the security testing needs of both information technology producers and users.[vii] The Common Criteria Evaluation and Validation Scheme (CCEVS) was established by NIAP to implement the CCRA compliant evaluation scheme within the US. [viii]

Common Criteria Paradigm

To effectively implement or evaluate according to the CC standards the security concepts and CC terminology are aligned in a Common Criteria Evaluation and Validation Scheme (CCEVS) hierarchical security framework.[ix]

The terminology used in the common criteria process is unique to the process and the semantics are fundamental to understanding the CC activities. The CC terms are requirements of the CC methodology and correspond to steps of the CCEVS security framework.

The first step of evaluating of a system or application using common criteria methodology is to identify a Target of Evaluation (TOE.) The TOE is a system, application, or IT product that is selected to be evaluated according to CC standards. The second step is to develop a set of Security Targets (ST).[x] The ST is the set of criteria to applied for the evaluation of the TOE. For specific technologies or IT products, previously established protection profiles may be used as the ST criteria.

With each step of the security framework, the CC evaluation process requires increasingly detailed information regarding the application or system security profile.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Figure 2: Common Criteria Evaluation and Validation Scheme (CCEVS) Security Framework[xi]

Security Environment	
Laws, organizational security policies, etc, which define the context in which the TOE is to be used. Threats present in the environment are also included.	
TOE – Target of Evaluation	An Information Technology (IT) product or system and its associated administrator and user guidance documentation that is the subject of an evaluation
Security Objectives	
A statement of intent to counter the identified threats and/or satisfy intended organizational security policies and assumptions.	
ST - Security Target	Set of security requirements and specification to be used as the basis for evaluation of an identified TOE. The ST may claim conformance to one or more Protection Profiles (PPs) and forms the basis of the evaluation.
TOE Security Requirements	
The refinement of the IT security objectives into a set of technical requirements for security functions and assurance, covering the TOE and its IT environment.	
TSP – TOE Security Policy	A set of rules that regulate how assets are managed, protected, and distributed within a TOE.
SF – Security Function	A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.
SFP – Security Function Policy	The security policy enforced by a SF.
TOE Security Specifications	
Define an actual or proposed implementation for the TOE.	
TSF - TOE Security Functions	As set security functions for all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
SOF - Strength of Functions	Qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behavior by directly attacking its underlying security mechanisms.
TSC - TSF Scope of Control	The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.
TSFI - TOE Interface	Set of interfaced, whether interactive (man-machine interface) or programmatic (application programming interface), through which TOE resources are accessed, mediated by the TSF, or information is obtained from the TSF.
TOE Implementation	
The realization of a TOE in accordance with its specifications.	

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The resulting product of progressing through the CC Security Framework steps is a IT product or system that meets a baseline set of security criteria and/or processes that institute fundamental security techniques. Specific security mechanisms or techniques for IT products and technology are addressed through the Common Criteria Protection Profiles.

Applying the Common Criteria

There are three sections to the Common Criteria (CC) version 2.0.[xii] These three sections are Introduction and General Model (section one), Security Functional Requirements (section two), and Security Assurance Requirements (section three).[xiii] The CC general audience, groups who would apply CC standards, is comprised of IT system or product consumers, developers, and evaluators.[xiv] The three CC sections provide guidance on how CC establishes baseline security requirements for buying, developing, or evaluating an IT system or product.

The technical specifications of applying IT security are provided in the second and third sections, security functional and assurance requirements, of the CC.[xv] These security requirements are grouped into high-level sets of related security requirements defined for the purposes of the CC as classes. The classes of related security requirements are unique to the either security functional requirements or security assurance requirements. Functional and assurance requirement classes guide consumers, developers, and evaluators on how to apply the security requirement components to meet security policy or counter threats.[xvi]

Section One – Introduction and General Model

Security defines information technology attributes and assurance mechanisms for protecting the confidentiality and integrity of information, and availability of critical services.[xvii] Common Criteria proposes that all security specifications and requirements should come from a general security context that protects assets from threats and categorizes these threats in accordance to their potential. [xviii]

The CCEVS security framework establishes a logical progression where a security environment is described (e.g. TOE) and then security objectives are determined based on the indicated security environment (e.g. ST).[xix] The TOE security function, TSF, is the set of information technology attributes and assurance mechanisms that support individual security function policies (SFP). Essentially, the TSF is the functional and technical logic built into the TOE system or technology required to meet established TOE security requirements or policy (e.g. TSP).

The confidentiality, integrity, and availability of the system are enforced through the security specifications of the TOE. The strength and scope of the security mechanisms are designed and implemented to secure the TOE Interface (TSFI).

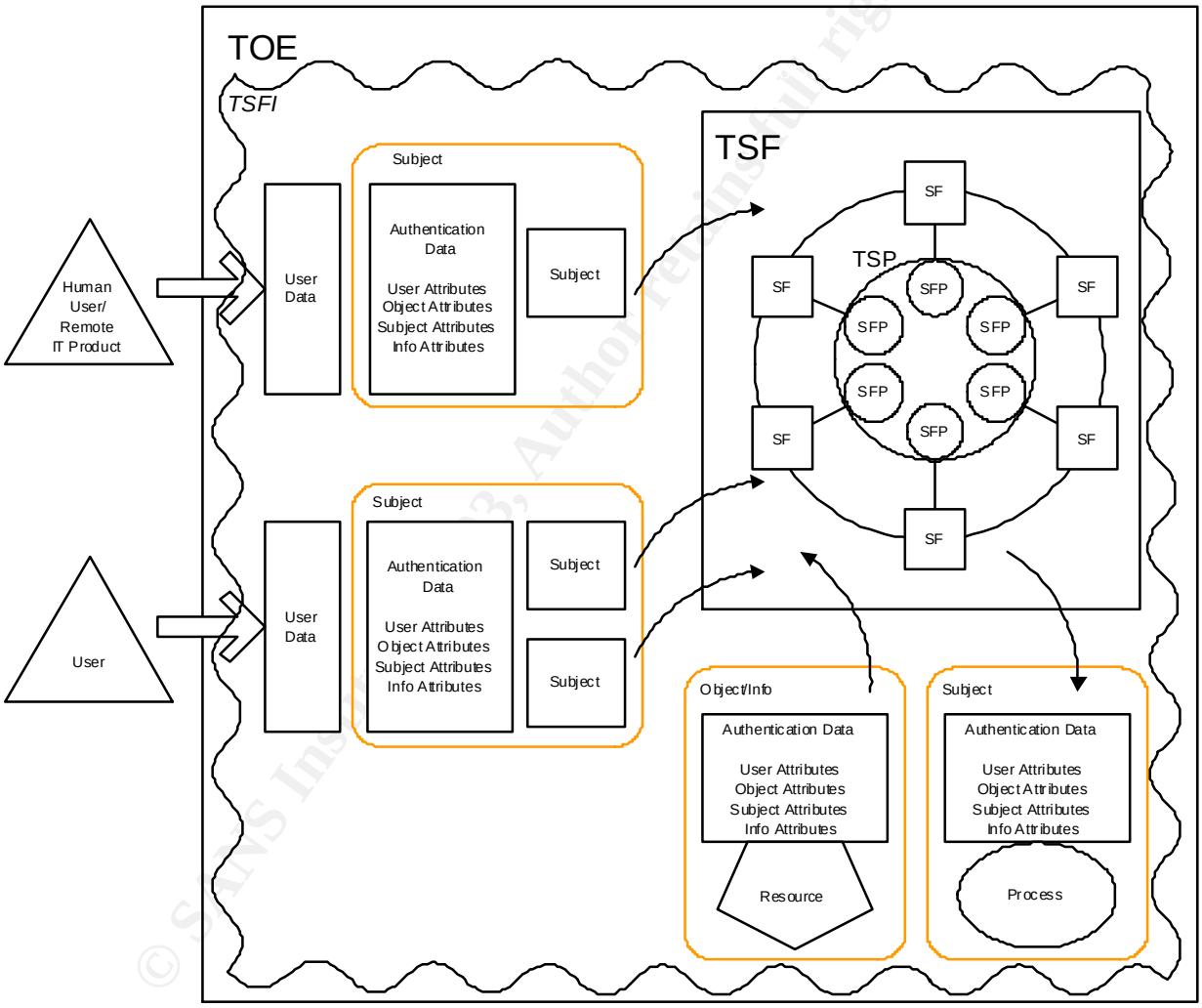
While the steps of the CCEVS security framework progressively detail the TOE environment and require security objectives to be established, it does not fully

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

explain the detailed security configuration requirements for a TOE operational and production environment. The CC general model of the TOE establishes the logical interdependencies of security policies and the security functions to establish the technical expression of security techniques (e.g. TSF).

The TSF security techniques provide the mechanism by which users access and interface with the TOE. The TOE Security Function Interface (TSFI) is the layer of the TOE where users, either human users or remote IT products gain access into the TOE environment.

Figure 3: Common Criteria "TOE" General Model[xx]



Section Two – Security Functional Requirements

The security functional requirements establish a set of functional components (e.g. classes) as a standard to express the TOE security functional requirements.[xxi] Consumers, developers, and evaluators use these functional requirements as guidance and for reference when developing and interpreting security function

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

statements, formulating functional TOE specifications, and assessing compliance of a TOE to the required security functions.[xxii]

The eleven classes of security functional requirements including the CC class short name and purpose are:

Security Audit (FAU) – monitor, capture, store, analyze, and report information related to security event.[xxiii]

Communication (FCO) – Assure the identity of originators and recipients of transmitted information; non-repudiation. [xxiv]

Cryptographic Support (FCS) – Management and operational use of cryptographic keys.

User Data Protection (FDP) – Protect user data and the associated security attributes within a TOE and data that is imported, exported, and stored. [xxv]

Identification & Authentication (FIA) – Ensure unambiguous identification of authorized users and the correct association of security attributes with users and subjects.[xxvi]

Security Management (FMT) – Management of security attributes, data, and functions and definitions of security roles. [xxvii]

Privacy (FPR) – Protect users against discovery and misuse of their identity. [xxviii]

Protection of the TOE Security Functions (FPT) – Maintain the integrity of the TSF management functions and data.[xxix]

Resource Utilization (FRUO) – Ensure availability of system resources through fault tolerance and the allocation of services by priority.[xxx]

TOE Access (FTA) – Controlling user session establishment.[xxxi]

Trusted Path Channels (FTP) – Provide a trusted communications path between users and the TSF and between the TSF and other trusted IT products. [xxxii]

Section Three – Security Assurance Requirements

The security assessment requirements establish a set of assurance components (e.g. classes) as a standard to express the TOE assurance requirements. [xxxiii] Consumers, developers, and evaluators use these assurance requirements as guidance and for reference when determining assurance levels and requirements, assurance techniques, and evaluation criteria.[xxxiv]

The ten classes of security assessment requirements CC class abbreviation, and purpose are:

Protection Profile Evaluation (APE) –Demonstrate that the PP is complete, consistent, and technically sound.[xxxv]

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Security Target Evaluation (ASE) – Demonstrate that the ST is complete, consistent, technically sound, and suitable for use as the basis for a TOE evaluation.[xxxvi]

Configuration Management (ACM) – Control the process by which a TOE and its related documentation is developed, refined, and modified. [xxxvii]

Delivery & Operation (ADO) – Ensure that the delivery, installation, generation, and initialization of the TOE.[xxxviii]

Development (ADV) –Ensure that the development process is methodical by requiring various levels of specification and design and evaluating the consistency between them.[xxxix]

Guidance Documents (AGD) – Ensure that all relevant aspects of the secure operation and use of the TOE are documented in user and administrator guidance.[xl]

Life Cycle Support (ALC) – Ensure that methodical processes are followed during the operations and maintenance phase so that security integrity is not disrupted. [xli]

Vulnerability Assessment (AVA) – Analyze the existence of latent vulnerabilities, such as exploitable covert channels, misuse or incorrect configuration of the TOE, the ability to defeat, bypass, or compromise security credentials. [xlii]

Maintenance of Assurance (AMA) – Assure that the TOE will continue to meets its security target as changes are made to the TOE or its environment.[xliii]

Tests (ATE) – Ensure adequate test coverage, test depth, functional and independent testing.[xliv]

Protection Profile Overview

The Common Criteria methodology establishes the core set of processes by which organizations can approach computer security evaluations and/or apply Protection Profile (PP) criteria. PPs provide a detailed level of security requirements and standards pertinent to a specific technology or security risk area based on the overall CC framework or specific to the evaluated IT product or technology.

Each PP provides a reusable set of IT security requirements that can be certified as complete, consistent and technically sound in addressing threats that exist in a specified environment.[xlv] A PP would be appropriate in the following cases:

- A consumer group wishes to specify security requirements for an application type (e.g. electronic funds transfer)
- A government wishes to specify security requirements for a class of security products (e.g. firewalls)
- An organization wishes to purchase an IT system to address its security requirements (e.g. patient records for a hospital). [xlvi]

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The international CCRA supports PP development by providing certificates on PPs that can be accepted among the CCRA participants. PPs have been developed to provide mechanisms to defend and support fundamental areas of security risk to the network, infrastructure, system boundary, and computing environment. [xlvii]

Defense-In-Depth Strategy

The Information Assurance Technical Framework (IATF) recognizes support and defense of these four areas of security risk to be the basis of the security-in-depth strategy.[xlviii] The IATF provides technical guidance for protecting information and information infrastructures defining a systematic process for developing information assurance and the security requirements for the hardware and software components.[xlix]

The Defense-in-Depth strategy is to provide information infrastructure protection in the of the following four core technology layers through defense and support mechanisms:

1. Defend the Network and Infrastructure,
2. Defend the Enclave Boundary,
3. Defend the Computing Environment, and
4. Supporting Infrastructures.[l]

Protection Profile Categorization

The Protection Profiles (PP) provide detailed technology techniques and solutions to implement the defense-in-layers strategy. NIAP categorizes PPs according to the four core technology defense and support layers. Products and technology evaluated in compliance to established PPs are recognized by NIAP to provide means to defend and support the TOE against major security risks to the system or product environment (e.g. TOE).

Figure 4: NIAP Protection Profile Evaluation Groupings[li]

Defend the Network & Infrastructure	Defend the Enclave Boundary	Defend the Computing Environment	Support the Infrastructure (PKI, Detect, Mgmt)
• Routers • WLANS • Switches & Routers	• Firewalls • VPN • Multiple Domain Solutions • Mobile Code • Remote Access • Guards	• Operating Systems • Biometrics • Single-Level Web Servers • Tokens • Secure Messaging • Peripheral Switch • Trusted DBMS • PC Access Control • Sensitive Data Protection	• PKI/KMI • IDS • Network Management • Smart Cards • Key Recovery • Certificate Mgt

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

A PP is intended to be reusable and to define TOE requirements that are known to be useful and effective in meeting identified functional and assurance security objectives.[lii] PPs permit security objectives independent of the implementation of a TOE or set of TOEs that complies fully with a set of security requirements and provides justification for security objectives and security requirements.[liii]

In total there are 30 evaluated, developed, and drafted recognized PPs which address technologies, hardware/software, operations, manpower, and services.[liv] The area of Defense-in-Depth strategy the PPs address separates these PPs out.

Certified, Developed, and Draft Protection Profiles

Defend the Network & Infrastructure

PPs to defend the network and infrastructure address the availability, confidentiality, and management requirements of large transport networks and various other transmission and switching capabilities.[lv]

Defend the Network & Infrastructure [lvi]				
Entry Label	*Type*	*Title*	*Supplier*	*Status*
PP-024	Switches & Routers	Protection Profile for Switches and Routers	NSA	Draft
PP-023	WLAN	Peer-to-Peer Wireless Local Area Network (WLAN) for Sensitive But Unclassified Environments - V0.6	Booz·Allen & Hamilton/ NSA / Tresys Technology	Draft
PP-027	WLAN	Infrastructure Wireless Local Area Network (WLAN) For Sensitive But Unclassified Environments	Booz·Allen & Hamilton/ Tresys Technology	Draft

Defend the Enclave Boundary (System Boundary)

PPs to defend the enclave boundary deal with perimeter defenses.[lvii] An enclave boundary is the points of connection for Local Area Network (LAN), a Wide Area Network (WAN), or similar networks to the service layer of another network.[lviii] This category includes: protection for network access; protection for remote access from both remote enclaves and traveling laptops; and protection during interoperation across security level.[lix]

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Defend the Enclave Boundary[lx]				
Entry Label	*Type*	*Title*	*Supplier*	*Status*
PP-004	Access Control	Role-Based Access Control Protection Profile Version 1.0	NIST	Certified
PP-009	Access Control	Role-Based Access Control Protection Profile Version 1.0	NIST	Certified
PP-001	Access Control	Directory for US Department of Defense Class 4 PKI PP	NSA	Certified
PP-002	Access Control	Trusted Platform Module (TPM) Protection Profile	Trusted Computing Platform Alliance (TCPA)	Develop
PP-014	Access Control	Privilege Directed Content Protection Profile	Authorizor Ltd.	Certified
PP-008	Databases	Oracle DBMS Protection Profile	Oracle Corporation	Certified
PP-030	Databases	Oracle Government Database Management System	Oracle Corporation	Certified
PP-005	Firewalls	Traffic Filter Firewall Protection Profile For Medium Robustness Environments	NSA	Certified
PP-010	Firewalls	Traffic Filter Firewall Protection Profile for Low Risk Environments (Version1.1)	NSA	Certified
PP-011	Firewalls	Application Level Firewall Protection Profile for Low Risk Environments (Version1.d)	NSA	Draft
PP-015	Firewalls	Application-level Firewall Protection Profile For Medium Robustness Environments	NSA	Certified
PP-026	VPN	A Goal VPN Protection Profile For Protecting Sensitive Information - V2.0	NSA	Draft

Defend the Computing Environment

PPs to defend the computing environment attend to the security considerations for end user workstations, servers, applications, and operating systems.[lxi]

Defend the Computing Environment[lxii]				
Entry Label	*Type*	*Title*	*Supplier*	*Status*
PP-016	Biometrics	U. S. Department of Defense Biometrics Office, Biometric System. Protection Profile For Medium Robustness Environments, v0.01	DoD Biometrics Management Office (DoD BMO)	Draft

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

PP-007	Operating Systems	Labeled Security Protection Profile Version 1.b	NSA	Certified
PP-012	Operating Systems	Controlled Access Protection Profile	NSA	Certified
PP-022	Operating Systems	Protection Profile for Multilevel OS - Requiring Medium Robustness	NSA	Certified
PP-025	Operating Systems	Single-level OS's in Environments Requiring Medium PP	NSA	Certified
PP-013	Misc	Postage Meter Approval Protection Profile	Consignia	Certified
TCPAT PMPP_ V1.9.7	Misc	Trusted Computing Platform Alliance (TCPA) Trusted Platform Module Protection Profile	null	Certified

Supporting Infrastructures

PPs to support infrastructures address the security capabilities for supporting infrastructures of defense-in-depth requirements. This includes incident handling, Key Management Infrastructure (KMI), and Public Key Infrastructure (PKI) technologies.

Supporting Infrastructures[lxiii]				
Entry Label	*Type*	*Title*	*Supplier*	*Status*
PP-006	Certificate Mgt	Certificate Issuing and Management Components	NSA	Certified
PP-017	IDS	Intrusion Detection System Analyzer - Draft 3	NSA	Draft
PP-018	IDS	Intrusion Detection System Sensor - Draft 3	NSA	Draft
PP-019	Key Recovery	Key Recovery for Third Party Requestors Ver. 1.0	NSA	Draft
PP-020	Key Recovery	Key Recovery for Agent Systems Ver. 1.1	NSA	Draft
PP-021	Key Recovery	Key Recovery for End Systems Ver. 2	NSA	Draft
PP-028	Smart Card	Smart Card Protection Profile	SCSUG	Certified
PP-029	PKI	The PKI Secure Kernel Protection Profile	PKI PP Working Group	Certified

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Conclusion

Common Criteria standards and the technology specific Protection Profiles institute world-wide criteria for evaluating information technology operational security. Organizations recognized and sponsored by the United States government; NIST, NSA, NIAP, and the IATF Forum; are coordinating security assessment techniques and standards for use through out the United States government. Information Technology developers, consumers, and evaluators who must implement or assess security within a system or product can use the Common Criteria and Protection Profiles to establish an internationally recognized baseline of security requirements and techniques.

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

REFERENCES

1. Krause, Micki and Tipton, Harold. Information Security Management Handbook, 4th Edition, Vol. 3. Washington D.C.: Auberbach Publications, 2002.

2. Krause, Micki and Tipton, Harold. Information Security Management Handbook, 4th Edition, Vol. 4. Washington D.C.: Auberbach Publications, 2002.

3. Syntegra for the Common Criteria Organization, "Common Criteria an Introduction." October 1999.
URL: http://www.commoncriteria.org/introductory_overviews/CCIntroduction.pdf (28 April 2003)

4. Syntegra for the Common Criteria Organization, "Common Criteria for Information Technology Security Evaluations User Guide." October 1999.
URL: http://www.commoncriteria.org/introductory_overviews/CCUsersGuide.pdf (28 April 2003)

5. Common Criteria Organization, "Common Criteria for Information Technology Security Evaluation: Part 1 Introduction and General Model." Version 2.1 CCIMB-99-031. August 1999.
URL: http://www.commoncriteria.org/docs/PDF/CCPART1V21.PDF (28 April 2003)

6. Common Criteria Organization, "Common Criteria for Information Technology Security Evaluation: Part 2 Security Functional Requirements." Version 2.1 CCIMB-99-032. August 1999.
URL: http://www.commoncriteria.org/docs/PDF/CCPART2V21.PDF (28 April 2003)

7. Common Criteria Organization, "Common Criteria for Information Technology Security Evaluation: Part 3 Security Assurance Requirements." Version 2.1 CCIMB-99-033. August 1999.
URL: http://www.commoncriteria.org/docs/PDF/CCPART3V21.PDF (28 April 2003)

8. Common Criteria Organization, "Protection Profiles: What is a Protection Profile?"
URL: http://www.commoncriteria.org/protection_profiles/index.html (28 April 2003)

9. Common Criteria Organization, "Protection Profile List – All."
URL:http://www.commoncriteria.org/ccc/protection_profiles/ppinfo.jsp?id=99&status=Certified (28 April 2003)

10. National Institute of Standards and Technology (NIST) Computer Security Resource Center (CSRC): "Common Criteria for IT Security Evaluation, Common Language to Express Common Needs"

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

URL: http://csrc.nist.gov/cc/index.html (28 April 2003)

11. National Information Assurance Partnership (NIAP). "Introducing the National Information Assurance Partnership"
URL: http://niap.nist.gov/howabout.html (28 April 2003)

12. National Information Assurance Partnership (NIAP). "Common Criteria Evaluation and Validation Scheme (CCEVS)"
URL: http://niap.nist.gov/cc-scheme/defining-ccevs.html (28 April 2003)

13. National Information Assurance Partnership (NIAP). "Validated Products List (by Type)"
URL: http://niap.nist.gov/cc-scheme/defining-ccevs.html (28 April 2003)

14. Defense Logistical Agency Comptroller (J-8). "Defense-wide Information Assurance Program: Definitions"
URL: http://www.dla.mil/J-8/IT%20Stuff/FMR%20PPI%20Defns.htm (28 April 2003)

15. The Information Assurance Technical Framework Forum. "What is the IATF Forum?"
URL: https://www.iatf.net/file_serve.cfm?chapter=introduction.pdf (28 April 2003)

16. Radium Trust Technology Assessment Program (TTAP). "Frequently Asked Questions (V4)"
URL: http://www.radium.ncsc.mil/tpep/process/Q3 (28 April 2003)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

ENDNOTES

[i] Trusted Product Evaluation Program (TPEP) Overview
http://www.radium.ncsc.mil/tpep/process/overview.html

[ii] NIST CSRC. "Common Criteria for IT Security Evaluation, Common Language to Express Common Needs" http://csrc.nist.gov/cc/index.html

[iii] CC Organization. "CC: An User Guide" pg 7
http://www.commoncriteria.org/introductory_overviews/CCUsersGuide.pdf

[iv] CC Organization. "Common Criteria Part 2: Security Functional Requirement" page ii
http://www.commoncriteria.org/docs/PDF/CCPART2V21.PDF

[v] CC Organization. "Common Criteria Part 2: Security Functional Requirement" page ii
http://www.commoncriteria.org/docs/PDF/CCPART2V21.PDF

[vi] NIST CSRC. "Common Criteria for IT Security Evaluation, Common Language to Express Common Needs"
http://csrc.nist.gov/cc/index.html

[vii] NIAP. "Introducing the National Information Assurance Partnership"
http://niap.nist.gov/howabout.html

[viii] NIAP. " CCEVS"
http://niap.nist.gov/cc-scheme/defining-ccevs.html

[ix] CC Organization. "CC: An Introduction" pg 4
http://www.commoncriteria.org/introductory_overviews/CCIntroduction.pdf

[x] CC Organization. "CC: An Introduction" pg 4
http://www.commoncriteria.org/introductory_overviews/CCIntroduction.pdf

[xi] CC Organization. "CC: An Introduction" "pgs. 5,
http://www.commoncriteria.org/introductory_overviews/CCIntroduction.pdf
***(this diagram is an original analysis of concepts and definitions spread through the CC documentation)

[xii] CC Organization. "CC: An Introduction" pg 4
http://www.commoncriteria.org/introductory_overviews/CCIntroduction.pdf

[xiii] CC Organization. "CC: An Introduction" pg 4
http://www.commoncriteria.org/introductory_overviews/CCIntroduction.pdf

[xiv] CC Organization. "CC: An Introduction" pg 4
http://www.commoncriteria.org/introductory_overviews/CCIntroduction.pdf

[xv] CC Organization. "CC: An Introduction" pg 4
http://www.commoncriteria.org/introductory_overviews/CCIntroduction.pdf

[xvi] CC Organization. "CC: An Introduction" pg 7
http://www.commoncriteria.org/introductory_overviews/CCIntroduction.pdf

[xvii] Krause. "Information Security Management Handbook, 4th Edition, Vol. 3" pg. 580

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

[xviii] Krause. "Information Security Management Handbook, 4th Edition, Vol. 3" pg. 580

[xix] Krause. "Information Security Management Handbook, 4th Edition, Vol. 3" pg. 580

[xx] CC Organization. "Common Criteria Part 2: Security Functional Requirement" pgs. 3, 4, 7 http://www.commoncriteria.org/docs/PDF/CCPART2V21.PDF (28 April 2003)

***(this diagram is an original analysis of several diagrams into one CC framework environment overview)

[xxi] CC Organization. "CC: An User Guide" pg 6 http://www.commoncriteria.org/introductory_overviews/CCUsersGuide.pdf

[xxii] CC Organization. "CC: An User Guide" pg 6 http://www.commoncriteria.org/introductory_overviews/CCUsersGuide.pdf

[xxiii] Krause. "Information Security Management Handbook, 4th Edition, Vol. 4" pg. 284

[xxiv] Krause. "Information Security Management Handbook, 4th Edition, Vol. 4" pg. 284

[xxv] Krause. "Information Security Management Handbook, 4th Edition, Vol. 4" pg. 284

[xxvi] Krause. "Information Security Management Handbook, 4th Edition, Vol. 4" pg. 284

[xxvii] Krause. "Information Security Management Handbook, 4th Edition, Vol. 4" pg. 284

[xxviii] Krause. "Information Security Management Handbook, 4th Edition, Vol. 4" pg. 284

[xxix] Krause. "Information Security Management Handbook, 4th Edition, Vol. 4" pg. 284

[xxx] Krause. "Information Security Management Handbook, 4th Edition, Vol. 4" pg. 284

[xxxi] Krause. "Information Security Management Handbook, 4th Edition, Vol. 4" pg. 284

[xxxii] Krause. "Information Security Management Handbook, 4th Edition, Vol. 4" pg. 284

[xxxiii] CC Organization. "CC: An User Guide" pg 6http://www.commoncriteria.org/introductory_overviews/CCUsersGuide.pdf

[xxxiv] CC Organization. "CC: An User Guide" pg 6 http://www.commoncriteria.org/introductory_overviews/CCUsersGuide.pdf

[xxxv] Krause. "Information Security Management Handbook, 4th Edition, Vol. 4" pg. 287

[xxxvi] Krause. "Information Security Management Handbook, 4th Edition, Vol. 4" pg. 287

[xxxvii] Krause. "Information Security Management Handbook, 4th Edition, Vol. 4" pg. 287

[xxxviii] Krause. "Information Security Management Handbook, 4th Edition, Vol. 4" pg. 287

[xxxix] Krause. "Information Security Management Handbook, 4th Edition, Vol. 4" pg. 287

[xl] Krause. "Information Security Management Handbook, 4th Edition, Vol. 4" pg. 287

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

[xli] Krause. "Information Security Management Handbook, 4th Edition, Vol. 4" pg. 287

[xlii] Krause. "Information Security Management Handbook, 4th Edition, Vol. 4" pg. 287

[xliii] Krause. "Information Security Management Handbook, 4th Edition, Vol. 4" pg. 287

[xliv] Krause. "Information Security Management Handbook, 4th Edition, Vol. 4" pg. 287

[xlv] CC Organization. "Protection Profiles: What is a Protection Profile?"
http://www.commoncriteria.org/protection_profiles/index.html

[xlvi] CC Organization. "Protection Profiles: What is a Protection Profile?"
http://www.commoncriteria.org/protection_profiles/index.html

[xlvii] NIAP. "Validated Products List (by Type)"
http://niap.nist.gov/cc-scheme/ValidatedProducts.html

[xlviii] IATFF. " What is the IATF Forum?"
https://www.iatf.net/file_serve.cfm?chapter=introduction.pdf

[xlix] IATFF. " What is the IATF Forum?"
https://www.iatf.net/file_serve.cfm?chapter=introduction.pdf

[l] IATFF. " What is the IATF Forum?"
https://www.iatf.net/file_serve.cfm?chapter=introduction.pdf

[li] NIAP. "Validated Products List (by Type)"
http://niap.nist.gov/cc-scheme/ValidatedProducts.html

[lii] Radium TTAP. "Frequently Asked Questions (V4)"
http://www.radium.ncsc.mil/tpep/process/faq-sect2.html#Q3

[liii] Radium TTAP. "Frequently Asked Questions (V4)"
http://www.radium.ncsc.mil/tpep/process/faq-sect2.html#Q3

[liv] DLA. "Defense-wide Information Assurance Program: Definitions"
http://www.dla.mil/J-8/IT%20Stuff/FMR%20PPI%20Defns.htm

[lv] DLA. "Defense-wide Information Assurance Program: Definitions"
http://www.dla.mil/J-8/IT%20Stuff/FMR%20PPI%20Defns.htm

[lvi] CC Organization. "**Protection Profile List - All**?"
http://www.commoncriteria.org/ccc/protection_profiles/ppinfo.jsp?id=99&status=Certified

[lvii] DLA. "Defense-wide Information Assurance Program: Definitions"
http://www.dla.mil/J-8/IT%20Stuff/FMR%20PPI%20Defns.htm

[lviii] DLA. "Defense-wide Information Assurance Program: Definitions"
http://www.dla.mil/J-8/IT%20Stuff/FMR%20PPI%20Defns.htm

[lix] DLA. "Defense-wide Information Assurance Program: Definitions"
http://www.dla.mil/J-8/IT%20Stuff/FMR%20PPI%20Defns.htm

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

[lx] CC Organization. "**Protection Profile List - All**?"
http://www.commoncriteria.org/ccc/protection_profiles/ppinfo.jsp?id=99&status=Certified

[lxi] DLA. "Defense-wide Information Assurance Program: Definitions"
http://www.dla.mil/J-8/IT%20Stuff/FMR%20PPI%20Defns.htm

[lxii] CC Organization. "**Protection Profile List - All**?"
http://www.commoncriteria.org/ccc/protection_profiles/ppinfo.jsp?id=99&status=Certified

[lxiii] CC Organization. "**Protection Profile List - All**?"
http://www.commoncriteria.org/ccc/protection_profiles/ppinfo.jsp?id=99&status=Certified

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: September 1st, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced