Common Criteria Schemes Around the

Eve Pierre

22 September 2009

Co-Authors and their (Scheme)

- James Arnold, SAIC Accredited Testing & Evaluation Laboratories (U.S.)
- Tony Boswell, SiVenture (UK)
- Richard Boyns, BT CLEF, BT Global Services (UK)
- Erin Connor, EWA-Canada IT Security Evaluation & Testing Facility (Canada)
- Gerald Krummeck, Atsec Information Security GmbH (Germany)
- Jean Pierre Lacoustille, SERMA Technologies ITSEF (France)
- Aleks Lubiejewski, STRATSEC (Australia)
- Eve Pierre, SAIC Accredited Testing & Evaluation Laboratories (U.S.)

Synopsis

- Introduction
- Schemes requirements for evaluation admittance
- Schemes validation/certification milestones
- Schemes requirements for ongoing evaluations
- Factors driving the use of common criteria (CC) evaluated products
- Schemes requirements beyond those in the CC
- Validator/certifier – evaluator working relationship
- Scheme informational requirements
- Conclusions

Introduction

- The general idea for this effort was for a few evaluators from different Schemes to get together and discuss the differences between the various International Common Criteria (CC) Schemes from an evaluator and evaluation laboratory point-of-view

- This presentation is a summary of our findings

- It is important to stress that the intent of our research was not to identify which of the schemes is better or to identify weaknesses in their implementation, rather it is purely informational

Schemes Requirements for Evaluation Admittance

- Each common criteria scheme has requirements to be fulfilled prior to a product being formally accepted into evaluation.
  - The requirements differ from scheme to scheme, but generally include combinations of:
    - The delivery of required information from various sources, potentially including:
      - Evaluation Work Plan or schedule
      - Security target (ST) in some state of completeness and perhaps having undergone some degree of review or evaluation
      - Letters or other information indicating consumer interest in the product
      - Other forms, letters or pertinent information specific to a scheme
    - Specific scheme requirements for evaluation acceptance
    - Meetings to discuss various aspects of the product and evaluation

SAIC
From Science to Solutions

Energy | Environment | National Security | Health | Critical Infrastructure

Schemes Requirements for Evaluation Admittance

Scheme	Required Start-up Information – Security Target (ST)
Australia	**Reviewed ST** Complete ST accompanied by a review showing that the ST is suitable for evaluation.
Canada	**ST (with cursory review)** Mostly complete security target – all major sections and no obvious deficiencies in accordance with published scheme policy
France	**ST (with cursory review)** Largely complete security target – seemingly complete, except rationale may be incomplete.
Germany	**Draft ST** Early draft of the security target (for re-evaluation a description of relevant changes)
UK	**Reviewed ST** The ST is developed, evaluated, and certified only after the Scheme has reviewed pertinent information about the product, met with the developer and laboratory, and agreed that the product is suitable for evaluation and all parties have agreed to the claims and scope of evaluation.
U.S.	**Evaluated ST** Complete ST accompanied by a passing evaluation report. Upon receipt, the Scheme validates the evaluation results , checks the ST against published policies, and allows the evaluation to proceed if the validation uncovers no major issues to be resolved.

Schemes Requirements for Evaluation Admittance

Scheme	Required Start-up Information – Evaluation Work Plan
Australia	Evaluation Work Plan identifying milestones and the overall schedule
Canada	Evaluation Work Plan identifying milestones and the overall schedule
France	Evaluation file including the estimated workload and work to be performed
Germany	Evaluation Work Plan identifying milestones and the overall schedule
UK	Evaluation Work Plan (EWP) identifying milestones and the overall schedule; and Certification Work Plan identifying any agreements on interim progress meetings.
U.S.	Evaluation Work Plan identifying VORs timeline

SAIC
From Science to Solutions

Energy | Environment | National Security | Health | Critical Infrastructure

Schemes Requirements for Evaluation Admittance

Scheme	Required Start-up Information – Consumer Interest
Australia	**'Letter of interest'** from a government or critical infrastructure department or justification of suitability for government use.
Canada	**'Eligibility Report'** with intended claims and government and critical infrastructure deployment information.
France	The Scheme may refuse to admit products into evaluation based on perceived missing 'public interest'.
Germany	The Scheme may refuse to admit products into evaluation based on perceived missing 'public interest'.
UK	Perceived consumer interest is taken into account during pre-evaluation review and meetings.
U.S.	**'Letter of interest'** from a Department of Defense or intelligence community customer who is interested in purchasing the product and using it in a manner consistent with the security target (ST).

SAIC
From Science to Solutions

Energy | Environment | National Security | Health | Critical Infrastructure

Schemes Requirements for Evaluation Admittance

Scheme	Required Start-up Information – Other Information
Australia	A letter to the sponsor outlining their responsibilities under the scheme
Canada	None
France	An 'evaluation file' from the developer with product information and an identified laboratory and official request for registration letter
Germany	Application form filled in and signed by the sponsor and a signed contract with the evaluation lab
UK	A questionnaire about the product is the first deliverable; target of evaluation (TOE) scope information; and, a presentation detailing how the TOE works, potential certification issues, how the evaluation will be carried out, etc.
U.S.	Available user guidance for the TOE and a presentation detailing the already completed security target (ST) evaluation and how various scheme policies are fulfilled

From Science to Solutions

Energy | Environment | National Security | Health | Critical Infrastructure

torsdag 3. september 2009

Schemes Requirements for Evaluation Admittance

Scheme	Required Start-up Information – Other Scheme Requirements
Australia	As previously indicated
Canada	As previously indicated; adequate Scheme resources must be available; and the Scheme may refuse to admit a product into evaluation if it doesn’t include/claim sufficient security functionality.
France	As previously indicated; the Scheme may refuse to launch an evaluation if the product security functionality is not considered consistent or sufficient.
Germany	As previously indicated; adequate Scheme resources must be available; and the Scheme may refuse to admit products into evaluation if a product doesn’t provide sufficient security functionality to be meaningfully evaluated.
UK	As previously indicated – note that if a product doesn’t have sufficient security functionality to be meaningfully evaluated or if the evaluation would not have adequate scope, that is identified relatively early and the evaluation would not proceed.
U.S.	As previously indicated ; the Scheme only accepts up to 10 new evaluations per month; the Scheme may refuse to admit products into evaluation if a product doesn’t provide sufficient security functionality to be meaningfully evaluated; the Scheme requires all identified security functions to be included in the scope of the evaluation; the Scheme requires that all products include a security audit function; and the Scheme requires that all products conform to government Protection Profiles or must be evaluated using Evaluation Assurance Level 4 or higher

Energy | Environment | National Security | Health | Critical Infrastructure

Schemes Requirements for Evaluation Admittance

Scheme	Required Start-up Information – Formal Evaluation Start
Australia	A task start-up meeting is held to officially start the evaluation after the deliverables are approved.
Canada	Registration into evaluation occurs after the deliverables are approved. A kick-off meeting may be held.
France	Registration into evaluation occurs after the deliverables are approved.
Germany	A kick-off workshop is held between the scheme, developer, and laboratory to officially start the evaluation after the deliverables are received.
UK	Registration into evaluation occurs after the Security Target has been reviewed and agreed by the certifier.
U.S.	A kick-off meeting is held between the Scheme, developer, and laboratory to officially start the evaluation after the security target evaluation is agreed (without major issues) by the validators.

SAIC
From Science to Solutions

Energy | Environment | National Security | Health | Critical Infrastructure

Schemes Requirements for Evaluation Admittance

- While there are certainly differences among the schemes, there are also a number of similarities
  - Details like Scheme specific forms are not particularly interesting.
  - Similarly, the fact that all Schemes require some sort of plan or schedule and also have some defined registration or kick-off process to start an evaluation is not particularly interesting.
  - The more interesting points of comparisons revolve around the timing of security target evaluation, consideration of potential consumers, and the imposition of other scheme-specific technical requirements.

Schemes Requirements for Evaluation Admittance

- Timing of security target (ST) evaluation
  - Each Scheme requires a security target (ST) to be available prior to the start of evaluation.
    - While several Schemes have policies dictating the scope and content of STs, only one Scheme appears to perform substantive work prior to the development of an ST to ensure it has the content they want.
      - » This Scheme investment obviously expends Scheme resources, but likely reduces some risk for the evaluation sponsor.
    - Half the Schemes require at least a review of the ST prior to acceptance and one of those actually require that the ST be acceptably evaluated.
      - » All Schemes require that the ST be reviewed first, so this effectively results in a delayed formal start of evaluation while it should allow the Scheme to better ensure that the ST has the content they prefer.

SAIC
From Science to Solutions

Energy | Environment | National Security | Health | Critical Infrastructure

Schemes Requirements for Evaluation Admittance

- Consideration of potential consumers
  - Half of the Scheme have a formal requirement for information regarding potential or interested government (including defense or intelligence community) or critical infrastructure consumers.
    - With one exception, the remaining Schemes informally consider potential consumers when deciding whether an evaluation should proceed.
      - The bottom line is that most of the Schemes recognize that they have limited resources and need to ensure that their resources are focused on products that will best benefit the security needs of their respective countries.

Schemes Requirements for Evaluation Admittance

- Scheme-specific technical requirements
  - One-third of the Schemes appear to have no added technical requirements while the other two-thirds are at least concerned about the suitability of the product for evaluation and the scope of the evaluation.
    - Suitability involves determining whether it appears that the product has sufficient security functions and characteristics to be meaningfully evaluated.
      - » It is not meaningful to evaluate products that are inherently insecure, can be bypassed, are subject to tampering, etc.
    - Scope involves ensuring that the security target includes security claims representative of the security functions apparently available in the product.
      - » It may not be acceptable to exclude security functions from the scope of evaluation that users will expect to be secure.

SAIC
From Science to Solutions

Energy | Environment | National Security | Health | Critical Infrastructure

Schemes Requirements for Evaluation Admittance

- Scheme-specific technical requirements (cont)
  - One Scheme has raised the bar even further where, for example:
    - Conformance must be claimed either to a government Protection Profile or Evaluation Assurance Level 4; and
    - Security Audit events must be generated by the target of evaluation (and claimed in the security target).
      - » The former is an apparent attempt to ensure that Scheme resources yield the most value relative to evaluating products for its own customers (i.e., Department of Defense and Intelligence Community) and would tend to mitigate effort that would otherwise be spent making acceptance decisions more subjectively.
      - » The latter is an apparent attempt to impose government standards in evaluation claims generally rather than through Protection Profiles (which would seem more appropriate).

Schemes Validation/Certification Milestones (1)

Scheme	
Australia	No specific milestones – usually 3-4 certifier assurance meetings at different times in the evaluation
Canada	Three milestones: Completion of the security target evaluation; completion of ADV evaluation; and submission of the final evaluation technical report (ETR). Interaction with certifiers is continual
France	Three milestones: Initial Evaluation Meeting (called RE0) after the scheme has registered the evaluation; Intermediary Evaluation Meetings (called REx) to discuss issues/concerns raised during the evaluation; Final Evaluation Meeting after the final ETR has been submitted
Germany	Three milestones: Phase 1 – Evaluation of Security Target; Phase 2 – Evaluation of other evidence (ADV, AGD, ALC, ATE, AVA); Phase 3 – Final ETR submission for certification. There are no required status meetings, such meetings are scheduled on an as-needed basis with the certifiers
UK	Four milestones: Task startup review; ST evaluation successfully completed; Evaluation progress reviews; ETR completed
U.S.	Four milestones – 3 validation oversight review (VOR) meetings and 1 evaluation kickoff meeting: Initial VOR (ST evaluation successfully completed and before the formal start of the evaluation); evaluation kick-off (after a successful Initial VOR); Test VOR (after all evidence has been successfully evaluated except those areas related to hands-on testing of the product); Final VOR (after all evaluation team actions are complete) – VORs are graded, Pass, Conditional Pass, and Fail. The Scheme allows only 2 failed VORs per evaluation and the number of failed VORs are considered when the lab must be re-certified.

SAIC
From Science to Solutions

Energy | Environment | National Security | Health | Critical Infrastructure

Schemes Validation/Certification Milestones (2)

- Whether specifically defined or not all the Schemes recognize three distinct milestones
  - Successfully completed ST evaluation
  - Successfully completed evaluation of all other evidence
  - Final evaluation technical report submission
- The benefits for establishing specific milestones are that they offer a way to
  - Measure the progress of an evaluation for both the Scheme and the lab
  - Help limit the time it takes to complete evaluation
  - Help the Schemes identify evaluations that need to be stopped
- There are no real drawbacks, except for vendors who enter evaluation without a plan to complete the evaluation

Schemes Validation/Certification Milestones (2)

- The level of interactions between the certifiers and the evaluators differ. For about half the schemes interactions is continual, for the other half there are 3 formal meetings corresponding to the three milestones

- The effect of continual interactions are
  - There are no great surprises at any point of the evaluation
  - Certifiers see several versions of the evaluation technical report (ETR) and they may be able to provide more meaningful input to the evaluation
  - The exchanges are more collaborative because the evaluator gets to know the certifier and vice versa
  - This approach may seem to put greater demands on certification/validation resources

- The effect of minimal interactions
  - May appear to impose less demands on certification/validation resources, however certifiers/validators may need to (re-)climb a learning curve at each interaction point
  - No informal interactions
  - Certifiers see only the final version of ETRs
  - Issues are not resolved immediately
  - The evaluation team may get less support from the validator
  - This approach put more demands on evaluation resources, because evaluators must put more time into preparing for these meetings

- The level of interactions between certifiers and evaluators does not appear to affect the quality of an evaluation

Schemes Requirements for Ongoing Evaluations (1)

- Due to the number of evaluations running in parallel within a national Scheme, there may be a need for defining rules such as:
  - Maximum duration of an evaluation,
  - Ending uncompleted evaluations based upon specific restrictions.

Schemes Requirements for Ongoing Evaluations (2)

Scheme	Maximum duration of evaluations
Australia	No strict maximum is defined. Limits based on progress requirements
Canada	CCS Instruction #3: Final ETR after 14, 18 and 22 months respectively for EAL2, EAL3 and EAL4
France	No strict maximum is defined. Left at CB’s discretion, based on evaluation workplan
Germany	No strict maximum is defined. Limits based on progress requirements as defined in AIS28
UK	No strict maximum is defined. Left at CB’s discretion, based on evaluation workplan
U.S.	Policy letter #18: completion after 12, 18 and 24 months respectively for EAL2, EAL3 and EAL4. To be negotiated for higher levels

Schemes Requirements for Ongoing Evaluations (3)

- Two main policies appear to be applied for maximum duration of evaluations:
  - either a fixed duration is set, associated to each EAL level,
  - or no strict maximum is defined, and monitoring is based only on evaluation progress with regard to EWP and/or inactivity periods.
- Progress monitoring generally still applies on top of the maximum evaluation duration.

Schemes Requirements for Ongoing Evaluations (4)

Scheme	Progress requirements – Ending of uncompleted evaluations
Australia	Progress monitored based on EWP(*). If insufficient, evaluation can be removed from program. 1 month warning before removal.
Canada	Interim milestone timing points based on maximum time limit for EAL: 50% for ST evaluation, 75% for ADV class evaluation. If overrun, product removed from In Evaluation list, certifier released to other projects, evaluation may continue to eventual completion.
France	If more than 3 months inactivity is observed, developer is warned and evaluation can be removed from program.
Germany	Based on EWP. If more than 3 months delay, warning to the developer. Closing of certification after 4 weeks if still no activity.
UK	If unreasonable delay is observed with regard to EWP without significant progress, the CB reserves the right to withdraw the product from the list.
U.S.	If 2 months inactivity is observed, termination warning letter sent to developer, requesting activity within 30 days. For second notice, inactivity window reduced to 1 month.

Schemes Requirements for Ongoing Evaluations (5)

- Even if not fully harmonized, progress monitoring is performed in the same way under all schemes:
  - Generally based on initial evaluation workplan,
  - Inactivity periods are monitored (2 to 3 months),
  - Warnings are sent to developers to check the status of their evaluation,
  - Evaluation is terminated if no new activity is performed within a defined period (about 1 month).

Factors Driving the Use of Common Criteria (CC) Evaluated Products (1)

Scheme	Government Policies
Australia	Australian and New Zealand Government ICT security policies advise agencies that they SHOULD use evaluated products from a common criteria scheme
Canada	There are no mandatory requirements to use CC validated products, but increasingly procurement vehicles coming out of the GoC make references to products meeting the CC
France	For French administrations and agencies, the requirement is to use CC evaluated products. For specific types of products, there are also requirements in terms of conformance to the Protection Profiles as well as to European Commission directives.
Germany	German government does not require CC validated products for general IT equipment, only for specific products like the German health card, digital tachographs, electronic passports, and digital devices.
UK	There are no mandatory policies for using CC validated products – only the EU CC mandates for hardware-based products (smartcards and digital tachographs)
U.S.	There is an overriding NSTISSP No. 11 policy that requires for all information assurance and information assurance enabled products in US Government Departments and Agencies to be CC evaluated or certified via the Federal Information Processing Standards (FIPS) program as applicable. In addition, the US Department of Defense (DoD) mandates the use of CC-evaluated products for its agencies.

Factors Driving the Use of Common Criteria (CC) Evaluated Products (2)

- Government policies or preference is the main reason users consider CC evaluated products.
  - where policies are clearly defined, users demand it
  - Where not, few vendors are interested
- Of the six schemes reviewed
  - Only the French and US Government security policies require the use of CC certified products for agencies
  - The other schemes
    - Some encourage the use of Common Criteria Evaluated Products
    - Others consider CC certified products only to satisfy EU CC mandates

Scheme Requirements Beyond Those in the Common Criteria (CC)

Scheme	
Australia	No additional requirements
Canada	The Canadian Scheme publishes a combination of guides; only one adds requirements to the CC. This guide addresses how cryptographic security functionality (FCS class) must be handled if it is to be claimed by a product.
France	The French Scheme has setup a 'Qualification" process that corresponds to EAL3 or EAL4 specific augmentations; there are several qualification levels ("standard", "reinforced", "high") corresponding to the needs of the various administrations (e.g. "high" for Defense).
Germany	Additional requirements about how to conduct site visits. AIS sets the methodology for EAL5 evaluations; and defines specific methodologies for smartcard evaluations, digital tachographs, and random number generators.
UK	The UK Scheme publishes national interpretations of the CC that are mandatory.
U.S.	The US Scheme publishes a number of policy letters that are considered additional requirements to those of the CC because they are applied on all evaluations. In addition, the scheme requires conformance to PPs whenever one is available for the type of product under evaluation.

SAIC
From Science to Solutions

Energy | Environment | National Security | Health | Critical Infrastructure

torsdag 3. september 2009

Certifier/Validator – Evaluator Working Relationship (1)

- Certifiers/validators have to ensure that evaluations are carried out correctly and can be recognized under common criteria recognition agreement (CCRA). They therefore :
  - Carry out technical assurance
  - Ensure that methodology has been correctly applied
  - Make judgements on interpretations outside ‘normal’ or ‘known’ CC

- Essential points:
  - Is the relationship collaborative or adversarial?
  - Is work done (analysis or testing) to supplement the evaluators’ report?
  - Consistency

Certifier/Validator – Evaluator Working Relationship (2)

Scheme	Collaborative or adversarial?
Australia	Mostly collaborative – regular progress discussions with certifiers during evaluations
Canada	Collaborative –certifiers focused on achieving successful evaluations while meeting overall requirements
France	Usually collaborative – helped by certifier participation in technical and quality audits of labs
Germany	Usually collaborative – helped by long-term relationships with certifiers and specialization of certifiers
UK	Usually collaborative – frequent dialogues and reviews of test plans during evaluation
U.S.	Sometimes adversarial – highly dependent on validator

SAIC
From Science to Solutions

Certifier/Validator – Evaluator Working Relationship (3)

Themes emerging:

- Frequent communication and transparency during evaluation
- Experience and specialization of certifiers/validators
- Continuity and length of relationship
- Trust in validator commitment to successful outcomes while upholding standards

SAIC
From Science to Solutions

Energy | Environment | National Security | Health | Critical Infrastructure

Certifier/Validator – Evaluator Working Relationship (4)

Scheme	Supplementary (Repeated or Extended) Work?
Australia	Certifier access to deliverables at labs, but no additional work carried out
Canada	Certifier right of access to all deliverables, but may not choose to receive them; certifiers will generally perform detailed review of specific deliverables, e.g., ST, ADV, etc.
France	All deliverables made available to certifier but generally no additional work carried out
Germany	All deliverables available to certifier when reviewing evaluation report; no additional work carried out (reviews may lead to additional evaluator work)
UK	Certifier access to deliverables on request; no additional work carried out (clear distinction of evaluator role, but reviews may lead to additional evaluator work)
U.S.	Validator access to all deliverables; often questioning of evaluator conclusions based on additional work

Certifier/Validator – Evaluator Working Relationship (5)

Themes emerging:

- General right of access to deliverables – but variation in use from very little, through to additional analysis leading to questioning of evaluator conclusions

- Certifiers usually make technical challenges to the evaluation findings and reporting, but the difference seems to be between ensuring understanding (sometimes requiring additional work by evaluators), and challenging based on independent review of deliverables by validators

SAIC
From Science to Solutions

Energy | Environment | National Security | Health | Critical Infrastructure

Certifier/Validator – Evaluator Working Relationship (5)

Scheme	Consistency?
Australia	Differences in personal style of certifiers, but strong consistency on evaluation issues and propagation of policy interpretations to all labs
Canada	Generally consistent – helped by regular reviews of current evaluations, and quick publication of policy interpretations where needed
France	Generally consistent with few differences in personal style of certifiers or their different specialisations within the CB
Germany	Generally consistent – founded on long-term work and often specialization of certifiers
UK	Generally consistent, will make evidence-based interpretations to resolve issues within an evaluation
U.S.	Difference in personal style and expertise of validators – often dependent on validator; tendency to ask for things in excess of usual CC requirements

SAIC
From Science to Solutions

Energy | Environment | National Security | Health | Critical Infrastructure

Certifier/Validator – Evaluator Working Relationship (6)

Themes emerging:

- Interpretations are often needed for individual evaluations, and in these cases interpretation based on evidence and documented rationale (rather than dogma) is important
- Consistency is helped by long-term relationships between evaluators and certifiers/validators and frequent contact during evaluations
- Interpretation and policy has both formal (documented) and informal aspects (during reviews)

Scheme Informational Requirements

Scheme	Evaluation Evidence Access Requirements
Australia	Access to evaluation evidence at laboratories
Canada	With few exceptions all evaluation evidence made available. Right to access evaluation evidence upon request.
France	All evaluation evidence made available
Germany	All evaluation evidence made available
UK	Right to access evaluation evidence upon request
U.S.	All evaluation evidence made available

SAIC
From Science to Solutions

Energy | Environment | National Security | Health | Critical Infrastructure

Scheme Informational Requirements

- All schemes reserve the right to access evaluation evidence
  - Some require delivery of evidence so that it is available while doing certification/ validation work
  - Others require access upon request or at the laboratory facility should some need arise
- All schemes require schedules or Work Plans to be maintained throughout the evaluation
- All schemes require evaluation results to be submitted for approval (i.e., certification/validation)

- Ultimately, there is not a lot of difference in terms of what is required in terms of information – the primary differences lie in what is done with it

SAIC
From Science to Solutions

Energy | Environment | National Security | Health | Critical Infrastructure

Other factors considered

- Scheme size
  - Number of labs
  - Number of certifiers
  - Number of product in evaluation
- Scheme Assurance maintenance requirements and policies
- Scheme Requirements for Testing and Site Visits
  - When
  - Where
  - Who

Conclusions

- There are many similarities between the Schemes in the process for conducting evaluations
  - Initial review of the security target (ST) to determine suitability
  - Evaluation milestones
  - Rules to determine when an evaluation must be stopped

- There are also many differences between the Schemes in the process for conducting evaluations
  - The state of the ST at the start of the evaluation
  - Policies and other requirements additional to the CC
  - Level of interactions between certifier/validator and evaluators
  - Government mandates that require product to be evaluated

Contacts

Name	Contact Information
James Arnold	SAIC Accredited Testing & Evaluation Laboratories, james.l.arnold.jr@saic.com http://www.saic.com/infosec/common-criteria
Tony Boswell	SiVenture, tony.boswell@siventure.com
Richard Boyns	BT CLEF, BT Global Services, richard.boyns@bt.com
Erin Connor	EWA-Canada IT Security Evaluation & Testing Facility, econnor@ewa-canada.com
Gerald Krummeck	Atsec Information Security GmbH, gerald@atsec.com
Jean Pierre Lacoustille	SERMA Technologies, jp.lacoustille@serma.com
Aleks Lubiejewski	STRATSEC, aleks.lubiejewski@stratsec.net
Eve Pierre	SAIC Accredited Testing & Evaluation Laboratories marie.e.pierre@saic.com