
This presentation will provide some background on the history of the Common Criteria Recognition Arrangement (CC RA), including its implementation, and will discuss its future expansion. The CC RA has been in operation for almost 2 years now. I will share with you my thoughts on the successes of the CC RA and the challenges that we still have to face.

# International Recognition of Test Results

***Motivating Factors…***

- Eliminate or reduce duplicate evaluations of IT products and protection profiles
- Improve global market opportunities for the IT industry
- Encourage formal security testing of IT products
- Increase the availability of evaluated, security-enhanced IT products and protection profiles for national use

The next two slides indicate the many reasons why recognition of CC evaluation results are beneficial to users, developers, and evaluation laboratories. Perhaps the most important motivating factor was the desire on the part of developers to have “one evaluation, accepted everywhere”, in order to maximize their return-on-investment in getting their products evaluated.

# International Recognition of Test Results

***Motivating Factors…***

- Ensure that evaluations of 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
- Improve the efficiency and cost-effectiveness of security evaluations and the certification/validation process for IT products and protection profiles

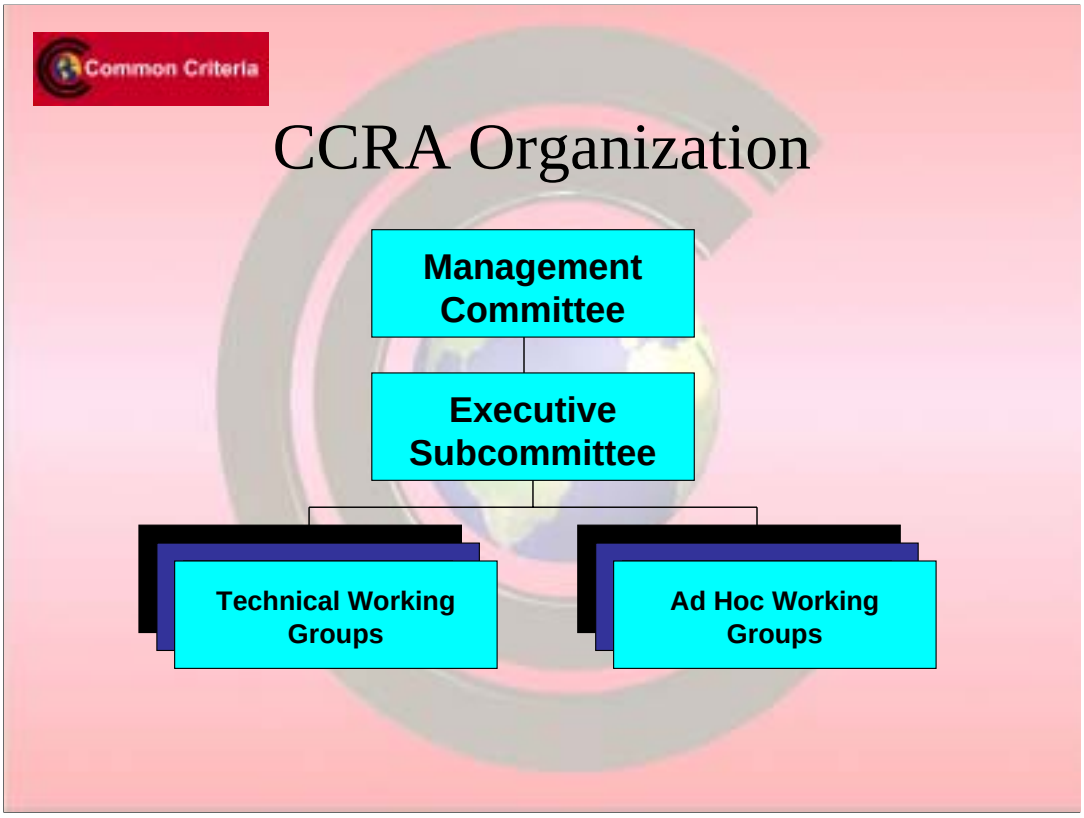
These two motivating factors are particularly important since the CC RA provides a forum where CC RA members can raise complaints if they think a particular member is not upholding the spirit of the CC RA and a forum where members can agree on detailed or specific evaluation methods for specific technical areas (e.g. specific evaluation techniques for smartcards)

# CC RA History

- Interim Arrangement (October 1997)
  **Canada, United Kingdom, United States**
- Interim Arrangement (March 1998)
  **Canada, France, Germany, United Kingdom, United States**
- Full Arrangement (October 1998)
  **Canada, France, Germany, United Kingdom, United States**
  October 1999: **Australia, New Zealand**
- Harmonized Arrangement (May 2000)
  **Australia, Canada, Finland, France, Germany, Greece, Italy, The Netherlands, New Zealand, Norway, Spain, United Kingdom, United States**
  **November 2000: Israel**
  **February 2002: Sweden**

This slide shows the temporal order of arrangements that led up to the full harmonized CC RA in May 2000. The May 2000 CC RA was significant in that it merged the members of two prior arrangements: members of the Full CC Arrangement (October 1998) with members of the ITSEC arrangement that existed in Europe prior to the Full CC Arrangement.

This February, Sweden was admitted as a certificate consuming member.




The CC RA specifies that each signatory of the CC RA is a member of the Management Committee (MC) , with one vote on the MC. Decisions in the MC are by majority vote, except in cases where the CC RA calls for unanimous consent. These are:

Admitting new certificate consumer participants

Admitting a new certificate producer participant (following a shadow certification)

Accepting a certification body as being compliant (following a shadow certification)

Changing the CC RA.

The MC meets once a year, unless it is necessary to hold meetings in between annual meetings.

The Executive Subcommittee (ES) carries out the day-to-day activities of the CC RA and meets 3-4 times per year. It is composed of all certificate producer members and a few certificate consumer members. Decisions in the ES are taken by majority vote. Disagreements are resolved at the MC level.

There is one standing working group, the CC Interpretations Management Board (CCIMB) which addresses Requests for Interpretation, development of CC methodology, resolution of methodology issues, resolution of technical issues, and development of new versions of the CC and the Common Evaluation Methodology (CEM)


The MC responsibilities are contained on the next two slides. In almost all cases, the ES performs the required tasks and background work for the MC.

As an example, the ES is currently working on several procedures that supplement the CC RA document. These include:

*Process for shadow certification.*

*Procedures for admitting new CC Recognition Arrangement (RA) members.*

*Procedures for voluntary periodic assessment.*

*Procedures for handling supporting documents* (i.e., documented evaluation methods that are utilized in at least two CC RA member schemes)

*Procedures for maintaining a Centralized Certified Product List and Protection Profile List*

*Procedures for handling internal disagreements*

*Guidance to sponsors on reuse of evaluation results for reevaluation and certificate maintenance.*

# Committee Responsibilities

- Resolve technical disagreements about the terms and application of the Arrangement
- Manage the promotion and development of IT security evaluation criteria and evaluation methods
- Manage the maintenance of historical databases for criteria and methodology interpretations and any resultant decisions that could affect future versions of either the criteria or methodology


The CC RA requires that signatories to the CC RA must be government members.

As indicated before, there are two types of participants:

1. Certificate Consumer: those participants that agree to accept CC certificates issued by certificate authorizing participants
2. Certificate Producer: those participants that issue CC certificates under the conditions indicated in the slide.

# Admission Requirements

- All prospective participants must agree to uphold the general provisions of the Recognition Arrangement
- In addition, if seeking to become a certificate producer, a prospective participant must satisfy rigorous technical requirements by demonstrating competence in conducting IT security evaluations

This slide indicates the conditions for admission to the CC RA.


Many countries have expressed interest in joining the CC RA.

We are very pleased to see large amount of interest in the CC RA, and are looking forward to Japan joining the arrangement in the future.


This slides indicates current certificate consumer CC RA participants that are planning to transition to certificate producer status in the future.


Since some prospective participants may not want it know they are planning to join the CC RA, I didn't include references to specific nations in the slide. However, the slide does indicate the parts of the world the inquires came from.

However, a number of nations have publicly announced their intent to join the CC RA. These include:

Japan

Korea

Russia


Using the metric of "international interest in joining the CC RA", the CC RA appears to be very successful.

However, as the remainder of the slides in this presentation will show, there are issues that need to be addresses within the CC RA by the CC RA members to ensure its continued success and growth.

# International Experience: The CC RA in Practice

- To provide information on how the Common Criteria Recognition Arrangement is functioning in practice to include:
  - ✓ Experiences to-date in the day-to-day operation and administration of the Arrangement
  - ✓ Key issues that still need addressing
  - ✓ Challenges for the future

This slide begins the discussion of issues that still need to be addressed by current CC RA members and of challenges for the future.

The rest of the presentation will elaborate on these issues and challenges

# Key Issues and Challenges

- Non-Binding Arrangement
- Achieving Relative Parity (Intra-scheme and Inter-scheme)
- Confidence Building Activities
- Resource Requirements
- Common Criteria Interpretations
- Partnership with ISO
- Working with External Groups
- Commercial Sector Acceptance
- International Outreach Activities
- Extending the Arrangement

This slide contains a listing of the issues and challenges that will be discussed in slides that follow.


The current CC RA is a non-binding agreement. That means that all signatories agree that the CC RA is a voluntary arrangement (i.e., not mandatory) and cannot be enforced in a court of law. It also means that if a participant does not abide by the arrangement, the participant cannot be thrown out of the arrangement. It also requires each member to respect the national sovereignty of other members.

This type of agreement (called an "arrangement" rather than an "agreement") was negotiated because it was faster to get approval by all of the original signatories. A binding agreement would have taken several years to negotiate and would have had a low probability of being approved by the respective governments. Consequently, we chose the easier path of a non-binding agreement.

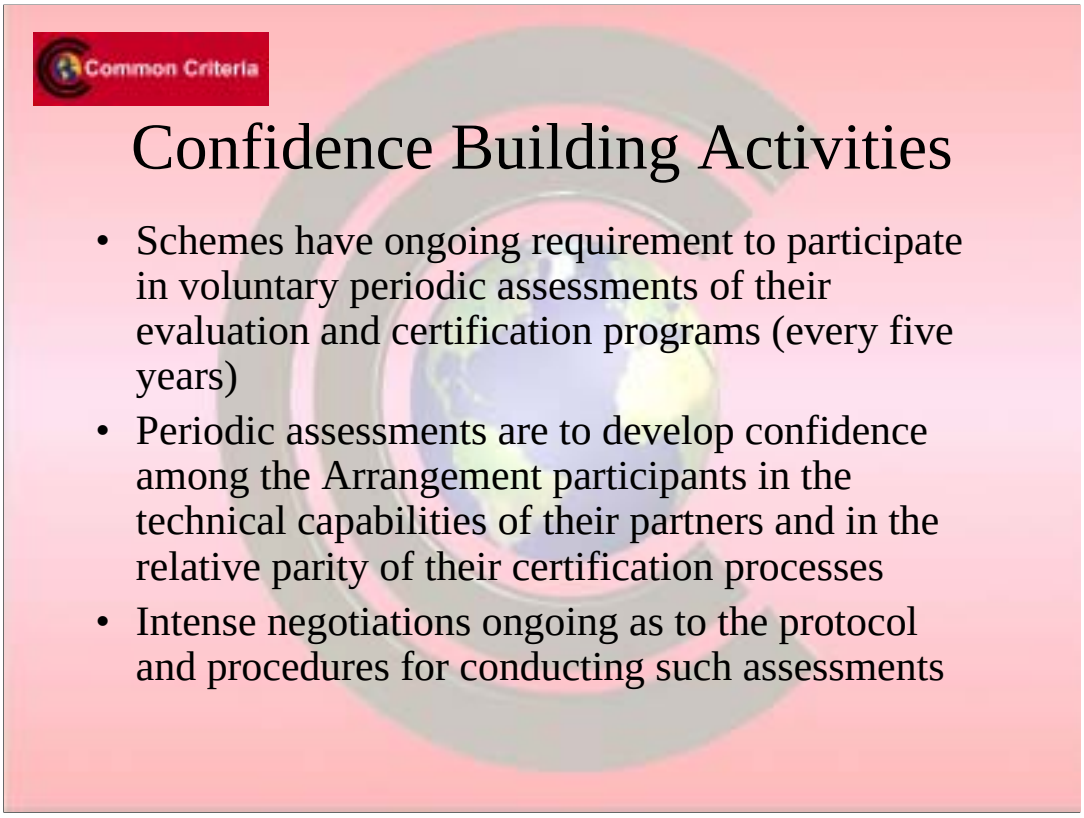
This has some draw backs. A major one is that it does not allow an "official or formal" membership fee. To be able to function in professional business like manner, an information infrastructure is required (e.g., website for external parties and an internal one for documents, archives, communication) and technical editors are needed to support to the ES, MC, CCIMB, and other working groups. This takes funding and resources. The original CC RA has no provision for requiring each member to provide funding and other resources. Consequently, it is not mandatory for a member to provide any funding/resources—it is voluntary. However, without adequate funding/resources the CC RA can not meet CC RA goals and external expectations. The MC/ES is currently investigating an equitable way to obtain funding from members.

# Achieving Relative Parity

**(Intra-scheme and Inter-scheme)**

- Natural competition among national schemes and among testing and evaluation facilities within schemes—the "business case aspects"
- Schemes implement terms of the Recognition Arrangement differently but must still satisfy overall requirements
- Differences in testing and evaluation costs can be due to labor rates and currency exchange rates

The credibility of the CC RA is only as good as the relative parity of the schemes. If there are large differences in comparability, repeatability, and consistency of evaluations among the different schemes, the credibility of the CC RA will be questioned. These differences occur in two areas: cost-time of evaluation and technical results. While some of the differences in cost-time of evaluation can be attributed to labor and currency exchange rates, it is the differences in technical results that potentially can cause the largest, most significant problems. The CC RA members have to strive to make sure differences in technical results are minimal and that the differences do not undermine the CC RA. The confidence building activities discussed on the next slide are intended to address the technical parity issue.

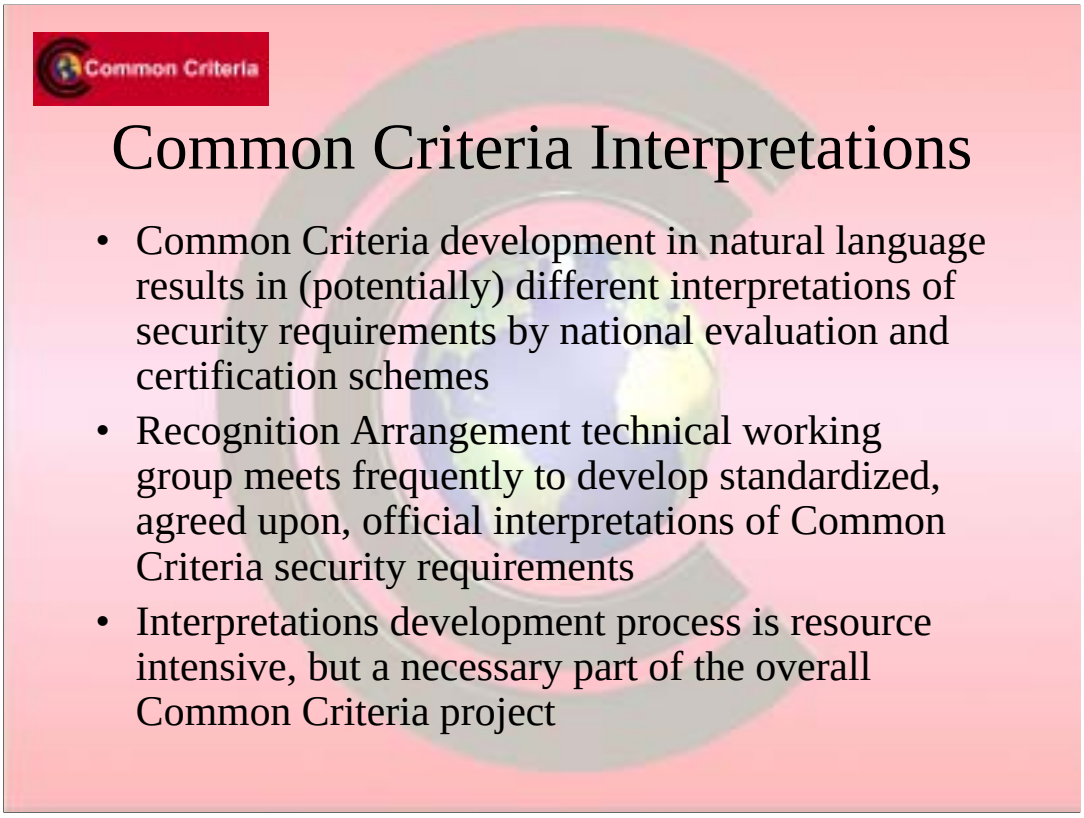



Although all producer participants in the CC RA agreed to follow the CEM, the CEM is at a high level of specificity. This allows schemes some variation in the specific methods they use to meet CEM requirements.

Because each scheme does things a little bit differently, it is necessary to be sure that evaluation results in the schemes are comparable even though evaluation methodology and approaches of the schemes may differ. Confidence building activities are intended to build confidence among the schemes that all schemes' evaluations are resulting in evaluations of comparable technical quality.

A key component of confidence building is requiring that each scheme go through a voluntary periodic assessment every 5 years or less. The ES has just completed the procedure that specifies the requirements for the voluntary periodic assessment, including the shadow certification process that is performed as part of the voluntary periodic assessment.


As mentioned previously, funding and staffing/human resources are needed to conduct day-to-day business of the CC RA (e.g., the support information infrastructure, the ES, the MC) and to support the technical working group activities (e.g., CCIMB). In addition, the producer participants need human resources to staff their schemes. This demand coupled with the lack of available trained professionals in this area has resulted in a shortage of human resources. The shortage of human resources has had a negative impact on the ability of the schemes and the CC RA project to meet desired goals. We do not see this situation changing in the future. As an example, it is very difficult for scheme to find competent validators/certifiers to oversee evaluations. Likewise, laboratories are having difficulty find staff that have experience performing evaluations.




Since the CC & CEM are written in a natural language, their use has resulted in numerous Request for Interpretation (RI). These RIs often point out errors in the CC & CEM or areas that need clarification. Often it takes months to process a RI. The unusually long length of time to process a RI is due, in part to the:

Shortage of human resources to apply to resolving the RIs

Inability to obtain consensus within the CCIMB on a solution

Complexity of the CC & CEM


A major goal of the CC project has been to work with ISO SC 27 WG3 to make the CC an international ISO standard. This goal has been achieved.

The CC project still believes it is important to work with ISO on other CC-related activities (e.g., making the CEM a standard) but, as described previously, lacks the human resources to provide significant coordination with and contributions to ISO. The CC RA project recently met with the Chair of SC 27 WG 3 to explore how both organizations can work together to meet each others expectations.


The CC RA does not contain any provisions for the CC RA project to work with external CC RA non-members. The CC RA requires the consistency of all official CC RA project working groups to be made up of representatives from the CC RA participants. However, the CC RA members have recognized the need to allow external technical consultation between outside groups/individuals and the CC project. Consequently, a procedure is being developed to allow this technical consultation in the future. The new procedure would still not permit external groups/individuals to be part of the CC RA (or its working groups) but it would define a process of cooperation/coordination/technical input if these support the goals of the CC RA.


The CC was originally developed by governments because they wanted their agencies to use evaluated products in government systems. To support this goal, the governments established evaluation schemes to ensure there were commercial laboratories available to perform the evaluations. However, it was recognized by many, including this author, that government demand for and use of evaluated products might not be large enough to sustain a healthy evaluation infrastructure. Thus, in order for the CC and the CC RA project to succeed, there needs to be commercial sector acceptance of the value of evaluated products and the commercial sector's desire to use evaluated products in their systems. Consequently, the CC RA project members and their respective schemes need to address the concern of the commercial sector that are on this slide. The commercial sector will be reluctant to embrace the evaluated product concept until these concerns are eliminated.


Information about the CC, the national schemes, and the goals of the CC RA project are spreading. As I mentioned previously, many nations have indicated a desire to join the CC RA. In 10 years, the CC has become a widely recognized standard and the benefits of using evaluated products in building critical infrastructure systems

has been recognized. However, there are many communities that could benefit from the use of the CC to define their requirements in the form of a protection profile but these communities do not know about the CC or understand how to apply it. Those of us that understand the CC and how to use it have a responsibility to evangelize its use to communities that know little about IT security and that do not understand the power of the CC.

As an example, I initiated discussions with key members of the process control community that led to establishment of a working group focused on defining security requirements for process control real-time systems. Such systems include: electric power generation & distribution, control of nuclear power plants, control of manufacturing plants, control of building environmental controls including safety/fire. Many of these systems are part of the critical infrastructures of many nations and, as such, are vulnerable to terrorist and other types of attacks. We need to engage other communities in order to educate them and to activate them to develop their security requirements.

This type of outreach is necessary for the continued success and growth of the CC.

# Extending the Arrangement

- Modifying the Arrangement to include higher levels of assurance requires:
  - ✓ The development of Common Evaluation Methodology for Evaluation Assurance Levels 5 through 7
  - ✓ Additional confidence-building activities to include shadow certifications of all certificate-producing participants in the Arrangement
  - ✓ Consensus vote by all participants to include new assurance components in the scope of the Arrangement

The current CC RA allows for changes by unanimous consent of its members. It is anticipated that in the future the current scope of the CC RA may need to be extended beyond EAL4. There are two key conditions that will have to be met prior to extending the scope of the CC RA beyond EAL4:

1. Methodology would have to developed and adopted for the extensions
2. All original members (US, UK, Canada, France, Germany) would undergo voluntary periodic assessments for confidence building purposes to ensure that they have a common technical base and comparable evaluation capability.


The future of the CC RA looks promising but there are still challenge that need to be overcome. It takes a lot of work to maintain the health of the CC RA – and, as more members join, the level of effort will increase and the ability to get consensus will become more difficult. I believe the CC will not succeed if the CC RA does not succeed since there will be no incentive for developers to get evaluated. While developers are not excited about the cost-time aspects of evaluation, they will "accept" it if they can have "one evaluation, accepted everywhere". If they have to go back to the situation where they need to have separate evaluations to meet the requirements of regional/national schemes, they will not go for evaluation.

To leave on a positive note, we have come a long way in 10 years, from multiple criteria to one, from multiple evaluations with no recognition to the CC RA, from no standard way to express security requirements to security targets and protection profiles. As I look back at the progress we have made, on balance, I believe there is an excellent chance the CC & CC RA will succeed. I look forward to having Japan contribute in and share in its success.

# Summary

- Anticipate continued expansion
  - Current member transitions to certificate authorisers
  - Increased membership since full Arrangement
  - New inquiries from Europe & Asia-Pacific
- Ongoing oversight and quality control required by CCRA committees
- Continuous improvements needed in:
  - Evaluation methods and their effectiveness
  - Promotion, outreach, and education

# Contact Information


**100 Bureau Drive  Mailstop 8930**
**Gaithersburg, MD USA 20899-8930**

***Director***
Dr. Ron S. Ross
**NIST-ITL**
**(301) 975-5390**
**rross@nist.gov**

***Deputy Director***
Terry Losonsky
**NSA-V1**
**(301) 975-4060**
**tmloson@missi.ncsc.mil**

***Senior Advisor***
Dr. Stuart Katzke
NIST-ITL
(301) 975-4768
**skatzke@nist.gov**

***Chief Scientist***
R. Kris Britton
NSA-V1
(410) 854-4384
**britton@radium.ncsc.mil**

**Email:** niap-info@nist.gov
**World Wide Web:** http://niap.nist.gov