Global Government Certifications: Why they are Important, and How the Certifications Process Must Continue to Evolve

Governments worldwide require certification and/or evaluation of IT products before allowing equipment to be deployed in their networks. It is not uncommon for different organizations within the same government to have different requirements. Product requirements also vary based on product type. There are many reasons for these requirements. The most common include:

- Assurance that the products meet a minimum set of functional criteria
- Verification of product feature and performance claims made by vendors
- Demonstration of interoperability with existing network equipment
- Demonstration of product performance under specific conditions in specific configurations

Security products are at the top of the required products list for certification and evaluation. Because network security is tantamount, governments must work to ensure the products being deployed perform as desired. The level of evaluation required depends on the sensitivity of the information being transported across the network. While “basic” evaluation may be sufficient for most networks, increasing levels of evaluation are required for equipment in networks transporting confidential information, and additional levels of evaluation, including analysis and/or inspection of source code, are required for equipment in networks transporting classified information.

In many countries, product evaluation falls into three distinct types: functional evaluation, cryptographic algorithm evaluation, and interoperability demonstration. Functional evaluation verifies the product behaves as expected. Categories of functional requirements are defined based on product type. These include firewall, virtual private network (VPN), intrusion detection system/intrusion protection system (IDS/IPS), etc. Cryptographic algorithm evaluation ensures the algorithms meet minimum requirements and are implemented correctly. Interoperability demonstration ensures products are compatible with the existing network infrastructure and, in some cases, validates vendor claims of performance.

Common Criteria

As IT becomes more pervasive, vendors and government organizations have recognized the need to define a common process to evaluate security products. Vendors are motivated to find a common process in an effort to reduce the costs involved in getting a product certified or evaluated. Governments, especially of smaller countries, are motivated because of the difficulty vendors have justifying the cost of custom certification efforts if market size is small.

History

Common Criteria originated from three standards:

- TCSEC: The U.S. Department of Defense's DoD 5200.28 Std, called the Orange Book, and parts of the Rainbow Series. The Orange Book originated from Computer Security work including the Ware Report, done by the National Security Agency and the National Bureau of Standards (the NBS eventually became NIST) in the late 1970s and early 1980s. The central thesis of the Orange Book follows from the work done by Dave Bell and Len Lapadula for a set of protection mechanisms.
- ITSEC: The European standard, developed in the early 1990s by France, Germany, the Netherlands, and the United Kingdom. It too was a unification of earlier work, such as the two U.K. approaches (the CESG U.K. Evaluation Scheme aimed at the defense/intelligence market and the DTI Green Book aimed at commercial use), and was adopted by some other countries, such as Australia.
- CTCPEC: The Canadian standard followed from the U.S. DoD standard and was used jointly by evaluators from both the United States and Canada. The CTCPEC standard was first published in May of 1993.

Common Criteria was produced by unifying these pre-existing standards, predominantly so that companies selling computer products for the government market (mainly for defense or intelligence use) would only need to have them evaluated against one set of standards. The Common Criteria was developed by the governments of Canada, France, Germany, the Netherlands, the United Kingdom, and the United States.

Mutual Recognition Arrangement

As well as the Common Criteria standard, there is also a sub-treaty-level Common Criteria Mutual Recognition Arrangement (MRA), whereby each party recognizes evaluations against the Common Criteria standard done by other parties. Originally signed in 1998 by Canada, France, Germany, the United Kingdom, and the United States, Australia and New Zealand joined in 1999, followed by Finland, Greece, Israel, Italy, the Netherlands, Norway, and Spain in 2000. The Arrangement has since been renamed **Common Criteria Recognition Arrangement** (**CCRA**) and membership continues to expand.

CCRA membership falls into two groups: authorizing members and consuming members. Authorizing members are countries that have established labs to evaluate and certify products. Currently, there are 12 authorizing members. All authorizing members are also consuming members. A consuming member is a country that agrees to recognize products certified by authorizing members. Today, there are 12 consuming (non-authorizing) members. A list of CCRA members is provided in Table 1. Any certification of a product issued by an authorizing member is recognized by all other CCRA members.

Table 1. List of CCRA Members

Authorizing Members	Consuming Members
Australia	Austria
Canada	Czech Republic
France	Denmark
Germany	Finland
Japan	Greece
Netherlands	Hungary
New Zealand	India
Norway	Israel
Republic of Korea	Italy
Spain	Malaysia
Sweden	Singapore
United Kingdom	Turkey

Process Overview

Under the Common Criteria, classes of products are evaluated against the security functional and assurance requirements of protection profiles. Protection profiles have been developed to apply to operating systems, firewalls, smart cards, and other products that can be expected to meet security requirements. The Common Criteria specifies a series of Evaluation Assurance Levels (EALs) for evaluated products. A higher EAL certification specifies a higher level of confidence that a product's security functions will be performed correctly and effectively. All test labs must comply with ISO 17025. Within the CCRA only evaluations up to EAL 4 are mutually recognized (including augmentation with flaw remediation). The European countries within the former ITSEC agreement typically recognize higher EALs as well. Evaluations at EAL 5 and above tend to involve the security requirements of the host nation's government.

Benefits

The nations that have embraced the Common Criteria have done so because they recognize that their common endorsement of a uniform set of IT security standards:

- Improves the availability of evaluated, security-enhanced IT products
- Contributes to higher levels of consumer confidence in IT product security
- Improves the efficiency and cost-effectiveness of the evaluation and certification process

It is important to note the benefits of Common Criteria are not limited to government customers. The Common Criteria certification provides a certain level of quality assurance through allowing customers to apply a consistent, stringent, and independently verified set of evaluation requirements to their IT purchases. Although Common Criteria certification does not ensure that a product is free of security vulnerabilities, it does provide a higher level of security assurance through an objective process to ensure the product performs as documented, and the vendor supports the product in the marketplace with processes to remediate flaws when, and if, they are

discovered.

The Common Criteria program provides customers with a wealth of information that helps to enable higher security in their implementation, and deployment of, evaluated products. Although Common Criteria certification is just one of many factors that can contribute to providing effective security, the Common Criteria allow vendors to help customers build more secure IT systems.

The Common Criteria help customers make informed security decisions on several levels:

- Customers can compare their specific requirements against the Common Criteria's consistent standards to determine the level of security they require.
- Customers can more easily determine whether particular products meet their security requirements. Because the Common Criteria require certification bodies to prepare detailed reports about the security features of successfully evaluated products, consumers can use those reports to judge the relative security of competing IT products.
- Customers can depend on Common Criteria evaluations because they are not performed by the vendors, but by independent test labs. The Common Criteria are increasingly used as a purchasing benchmark.
- Because the Common Criteria are an international standard, they provide a common set of standards that customers with worldwide operations can use to help choose products that meet their local and global operations' security needs.

By providing a detailed set of security standards, the Common Criteria effectively create an IT product security "language" that both vendors and consumers can understand. Vendors can draw upon this language to describe the security features included in their products by describing which Common Criteria evaluations their products have passed. Similarly, consumers can use this language to identify and communicate their security needs, which enables vendors to design products that meet customer needs.

The Common Criteria language enables vendors to build their IT products in such a way that they can more easily demonstrate that their products meet specified security requirements, and the evaluation process allows them to have their product security evaluated in a consistent and meaningful way by an impartial third party.

Cryptographic Algorithm Evaluation

Unfortunately, governments have not been as willing to define a common process for cryptographic algorithm evaluation. Because of the dependency on cryptography to protect nations' secrets, governments are less trusting when it comes to allowing other countries to determine whether or not cryptographic algorithms have been implemented properly. While there is some cooperation for validation of commercial algorithms such as Advanced Encryption Standard (AES) and Data Encryption Standard (DES), there is little, if any, cooperation for validation of algorithms used for encrypting classified information.

While most countries use similar processes for evaluating cryptographic algorithms, few formally recognize the validation results from other countries. The U.S. government requirements for cryptography are documented in the Federal Information Process Standard (FIPS) 140 series of publications. FIPS 140-2, issued on May 25, 2001 is the most current version of the standard. The U.S. Government's National Institute of Standards and Technology (NIST) issued the 140 Publication Series to coordinate the requirements and standards for cryptographic modules, which include both hardware and software components for use by departments and agencies of the U.S. Federal Government. The requirements cover not only the cryptographic modules themselves but also their documentation and (at the highest security level) some aspects of the comments contained in the source code. FIPS 140-2 defines four levels of security, simply named "Level 1" to "Level 4."

The Cryptographic Module Validation Program (CMVP) is operated jointly by the NIST's Computer Security Division and the Communications Security Establishment (CSE) of the Government of Canada. The use of validated cryptographic modules is required by the U.S. Government for all unclassified uses of cryptography. The Government of Canada also recommends the use of FIPS 140 validated cryptographic modules in unclassified applications of its departments.

The Communications Electronics Security Group (CESG) is the branch of Government Communications Headquarters (GCHQ) that works to secure the communications and information systems of the government and critical parts of the U.K. national infrastructure. CESG provides the CESG Assisted Products Service or CAPS. CAPS enables products to be cryptographically verified by CESG to U.K. Government cryptographic standards and formally approved for use by the U.K. Government and other appropriate organizations.

In Australia, the Defence Signals Directorate (DSD) has the responsibility for cryptography.

There are direct benefits of cryptographic algorithm evaluation to the governments that perform the validation, but there are widespread benefits to non-government customers as well, independent of what country performs the validation. Benefits include assurance that the cryptographic algorithms have been implemented properly. A cryptographic system can only be as strong as the encryption algorithms, digital signature algorithms, one-way hash functions, and message authentication codes it relies on. Break any of them, and you have broken the system. And just as it's possible to build a weak structure using strong materials, it's possible to build a weak cryptographic system using strong algorithms and protocols.

Cryptography is an increasingly important part of securing every corporate network. Most people are familiar with using encryption to protect wireless infrastructure or as part of VPNs for remote and/or teleworker access. They may not be aware that encryption is also used for:

- Site-to-site VPNs to connect branch offices
- Securing communications for managing the network
- Securing IP-based voice and video communications and signalling, and data storage

Interoperability Demonstration

Most governments have one or more large-scale IT networks to support their operations, ranging from healthcare to education to public services to military to intelligence. Depending on the nature and criticality of the networks and the services provided, many governments require vendors to perform some level of interoperability demonstration on their products before they can be deployed in these networks. The demonstrations can range from basic interoperability demonstrations to more sophisticated feature/functionality evaluations to performance evaluations to combinations of all three. These evaluations typically result in the product being placed on an Approved Products List (APL). Depending on the evaluation, government customers are either encouraged to, or required to, limit their equipment purchases to equipment listed on the APL.

The motivation for these demonstrations is to ensure a level of confidence in network operation and continuity of service. They also provide customers with an assurance that the equipment they are purchasing performs as advertised without each and every customer having to perform their own product evaluations.

The government evaluation process typically results in benefits for non-government customers. Non-government customers that take the time to learn about government evaluation and certification activities can gain increased confidence in product purchases by either directly or indirectly obtaining the results of the testing performed by the government labs. Examples range from deployment guides documenting how to deploy equipment in a more secure manner to validating vendor claims regarding product performance and reliability.

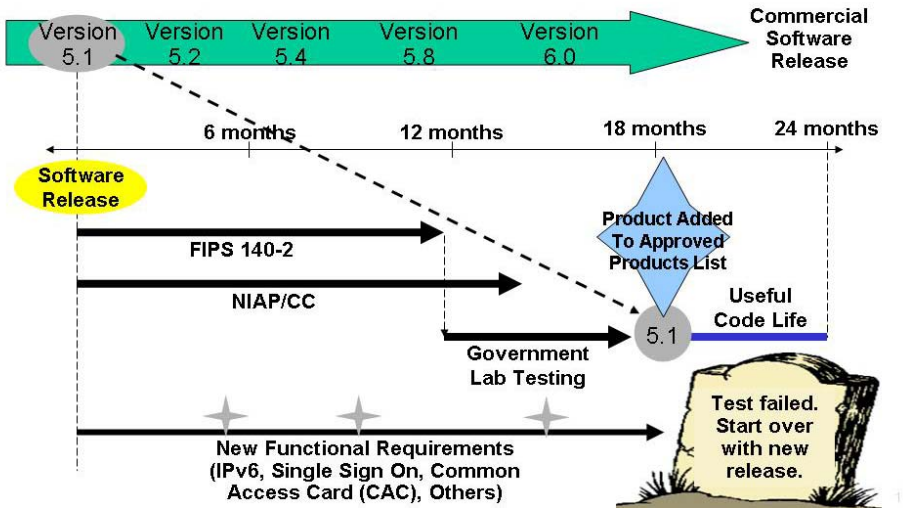
Certification Challenges

In today's environment of rapidly changing technology, there are several industry challenges with product certification. These include:

- Lack of requirements for certifying new technology
- The need to have the same features evaluated by more than one lab
- "Nested Requirements" Testing dependencies (or prerequisites) that gate entry into a lab
- Requirement to provide support for and/or interoperate with legacy technology
- Cost (documentation, equipment, personnel, lab fees)
- Time (preparation, test, post-test activities)

The result is a significant delay in the ability of government customers to field new technology. There are examples where the technology is practically obsolete before it is even fielded. This is illustrated in Figure 1.

Figure 1. Impact of Nested Requirements



The example in Figure 1 illustrates a product with a software release cycle of roughly every 3–4 months with each release being available for purchase by customers for 24 months. For this particular certification, a FIPS certificate is required to enter government testing. In addition, the product must be in process for Common Criteria evaluation.

In a typical scenario, the software will be able to enter government testing approximately 12 months after it is released and then it would be available for fielding 6 months after that. The result is a 6-month window for customers to buy the software. Obviously, durations will change depending on various factors, but this scenario is fairly typical and assumes no changes to the process as well as a fairly mature product. Policies and requirements are constantly evolving. In some cases, vendors have a “grace period” in which to comply. In other cases, they don’t. Couple that with challenges that all vendors encounter with taking a new product through certification or an existing product through a new certification process and it’s easy to see how a software release could reach end of sale before it gets certified.

In the past, this delay did not introduce a significant level of risk because the technology was expensive and available only to government customers. In today’s world where commercial-off-the-shelf (COTS) products, in many cases, offer greater capability at a much lower cost, risks are increased when an adversary has access to new technology that takes months, or even years, for the government to field.

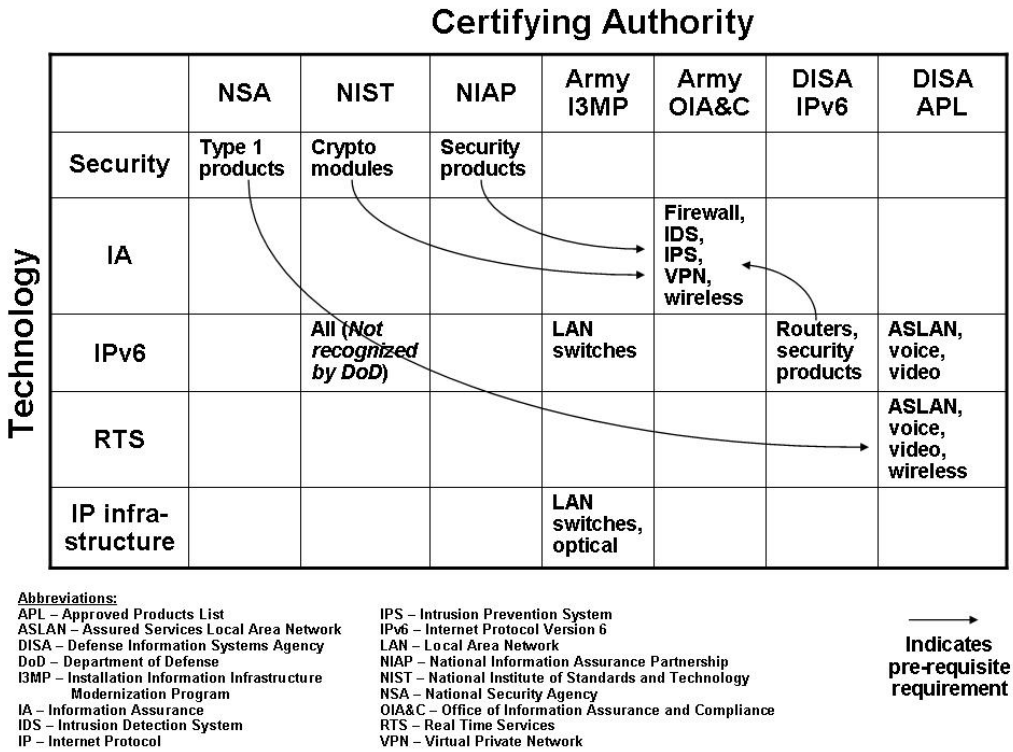
The adoption and deployment of COTS products leads to a new paradigm for government customers. In the past, government customers focused on mitigating risk. A product or system security evaluation was performed and a risk assessment produced. Then, the vendor and/or customer had to develop a mitigation plan and obtain approval to proceed. Until very recently, few, if any, customers included the risk of delaying the fielding of new technology as part of the risk

assessment. Because there is no quantitative measure of that risk, the old process for assessing and mitigating risk needs to be changed.

A process that includes risk management must be developed and adopted. While this requires more reliance on judgment than in the past, it is the only way to effectively address risks that are more intangible. Risk management is not new. It's common in tactical situations where commanders must evaluate the risk of allowing the use of new equipment versus the risk of delaying the use of that equipment. In the new paradigm, this process will also need to be integrated into strategic system evaluations.

In order to prevent the certification process from delaying the introduction of new technology, it is imperative that we first understand how we got to where we are today. Most of the certification policies have evolved over a long period of time. These policies came about out of necessity as technologies were developed to meet specific needs. For example, policies around cryptographic technology have been around since World War I. The level of certification required is a function of the sensitivity of the information being protected. The evolution of certification policies reflected the technology of the time. The best way to describe both the policies and the technology is to say they are "stove-piped." This is illustrated in Figure 2.

Figure 2. U.S. Government Certifications



Initially, the stove-piped approach worked. It was much easier to assign responsibility for certification to organizations that were most familiar with the technology. What has happened, however, is that most, if not all, of these technologies are now converging onto a single

infrastructure, specifically IP. This results in new dependencies that were never considered. As a result of these unforeseen dependencies, the process is now difficult at best, and impossible at worst.

Technology is evolving rapidly, and industry and government must find ways to transform the certification process. Just like technology that is converging onto single infrastructures, certification policies and processes must keep pace with the changes, and they must adapt if they are to remain viable. It is no longer acceptable to have a sequential certification process that delays product fielding for up to two (or even more) years. There are several things that should be considered.

Solutions

The first is to increase collaboration between government and industry. Currently, industry works for years to develop and introduce new technology. This is followed by a period of time in which the government defines policy and generates evaluation requirements for the new technology. This is often done without industry or test lab involvement. The first product then enters the certification process and vendors find out that the evaluation requirements are not consistent with the functionality and capabilities of the product. Once those issues are resolved, the test lab completes its evaluation and generates a test report. The policy people review the report and often discover that the test lab did not understand what needed to be evaluated. The end result is a duplication of effort and a protracted period of policy- and requirement-definition refinement that could have been avoided, and streamlined by involving industry and the test labs early in the process. This collaboration could also prove beneficial in providing clarification and resolving issues in a timely fashion through the evaluation process.

Government agencies must also define a workable process for dealing with new technology. While the concept of “pilot” deployments is not new, the problem is these deployments are typically customer focused, and not agency focused. The certifying authority has not been involved, and as a result, has not gained the information necessary to define the functional and evaluation requirements for certification. When the pilot is complete, the customer is often stuck because the certifying authority has not made any progress toward being able to certify the product/system. The critical thing here is to not create an R&D type mentality that provides for product or system evaluation in anything but a representative operational environment. Too often, products and systems are evaluated and are then determined to not meet the needs of the end user.

Concurrent processes must also be considered. While it may be prudent to require an FIPS certificate prior to beginning government certification testing, there may also be value to allowing the vendor an opportunity to perform “assessment” testing ahead of time. Many government labs are fee for service (i.e., vendors must pay a fee to the lab). If a vendor wants to mitigate risk by performing assessment testing prior to official certification testing, this provides an opportunity to increase the probability of success. Also worth considering for testing that requires other certifications as prerequisites is to allow testing to start once the product gets to the final stage of the process, which typically involves coordination and finalization.

The requirement to interoperate and support legacy technology is another area that often hinders the timely introduction of new technologies. In the past, it was important to ensure customer investment in legacy technology was protected. While this is still a consideration, it is also important to realize that vendors of new technology cannot afford to invest in legacy technology that non-government customers do not want to purchase. If these vendors must invest in the legacy technology, the associated costs must be passed on to government customers. The reality is that customers need to make purchasing decisions based on their needs.

Basic economics will determine whether or not vendors of new technology believe there is a good financial reason to invest in the development of legacy technology. If customers don't want to pay for it, vendors will not develop it. If vendors must have the support in order to be certified, government customers ultimately suffer because technology vendors will not enter the government market. There comes a time in every technology when it becomes cheaper to replace the legacy equipment than to incur the ongoing cost of support. An excellent example of this is video conferencing. The cost differential for an H.320 video teleconferencing (VTC) unit is many times the cost of an equivalent H.323 unit. Yet, vendors selling telecommunications equipment to the U.S. Department of Defense (DoD) must continue to support H.320 equipment. This is delaying the introduction of new Unified Communications products and capabilities into the U.S. DoD.

The time and financial resources required to enter into the certification process is a barrier of entry for small vendors. It would seem to best-serve the market to develop a system of reciprocity. One way to reduce cost is to eliminate redundant testing and leverage the test results from one or more labs across all organizations. While an organization like the U.S. Defense Information Systems Agency (DISA) Joint Interoperability Test Command (JITC) is already performing this role for telecommunications equipment, other service organizations are widely recognized for the type of testing they perform. The challenge is how to identify the "best-in-class" and eliminate redundancy. But, that is exactly what must be done to streamline the certification process and increase relevancy while at the same time reducing cost.

Conclusion

The certification process is critical to ensuring that government customers get the equipment they need and that the equipment performs as advertised, and that it is compatible with existing infrastructure. The missing component is that the customers need to know that the certification process does not limit the other part of the equation, which is being able to deploy the equipment they need when they need it, without unnecessary delays created by an archaic process. This point is made even more critical if government customers are to take advantage of the many benefits of COTS products. Without a transformation of the certification process, there will be reduced incentive for commercial equipment vendors to certify their products, government customers will not have timely access to the latest technology, and adversaries will gain a tactical advantage in cyber terrorism.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA

CXX-XXXXXX-XX 05/08