

BITS

FINANCIAL SERVICES
R O U N D T A B L E

BITS Product Certification Program (BPCP) Frequently Asked Questions (includes Common Criteria Alignment)

Why should I have my product certified?

The *BITS Tested Mark* product certification demonstrates to customers that your company is aware of and cares about security issues. When your product earns the *BITS Tested Mark*, your company improves safety and security for everyone. Certification helps build consumer confidence, leads to more widespread use of technology and promotes the growth of e-commerce.

The BITS certification process is a consistent, objective means of evaluating and testing for security standards. Seeking out certification helps reduce the real and perceived risks that can be a barrier to purchasing technology products.

How can my company prepare for product certification? What are the first steps?

Technology companies should approach testing with a high degree of confidence that their product will meet all necessary criteria. Therefore, the first step in preparing for product certification is to download the appropriate criteria for which the product under consideration applies, and perform an internal assessment of the product against the criteria. BITS can be consulted for any specific questions that come up during this period. Once the product is ready, a testing facility can be contacted for testing service contracts.

What does BITS suggest for vendors that have not yet tested against the Common Criteria?

For those technology providers not yet testing with the Common Criteria, the BITS requirement package can be used as a starting point for building a Security Target or Protection Profile. We encourage vendors that are in the process of Common Criteria testing, or that have achieved Common Criteria certification on a product, to begin an internal comparison of the BITS requirement package with their existing testing specifications to get an idea of the level of incremental testing, if any.

What happens when other industries establish their requirements—will vendors be expected to meet multiple requirements? Are there agreements in place or discussions taking place with other industries that will accept BITS certification?

This could be something the industry has to address in the future. For now, the financial services industry is leading the efforts to define requirements. Now that the BITS Product Certification Program is established with the Common Criteria, BITS intends to work with the National Institute of Standards and Technology (NIST) and the National Information Assurance Partnership (NIAP), as well as the new U.S. Department of Homeland Security and the White House's Office of Cyberspace Security to educate other industries and user groups about our security packages.

A lot of programs already exist that are not certified by BITS. Is BITS bringing existing programs up to speed and in compliance with the BITS criteria before looking toward new products to meet the criteria?

Improving product security must start somewhere. Therefore, the BITS Product Certification Program is targeted at the procurement cycle. BITS member companies realize the dilemma of existing or implemented products potentially not meeting the BITS security criteria. However, procurement and development cycles are relatively constant and therefore, a first step is to make sure that products meet a base-level requirement. Business risk decisions in any given financial institution may in fact lead to actions that affect existing products or programs.

What is included in the BITS Product Certification Program that is not in the Common Criteria?

Essentially, nothing. All of the BITS criteria were translated into security functional requirements under the Common Criteria. The Common Criteria provides a catalog of security functional requirements. BITS simply selected and defined, where necessary, the requirements that are important for financial institutions as minimum baseline requirements and then packaged them by product class.

What Evaluation Assurance Level (EAL) does BITS require?

The BITS Tested Mark certification focuses on the presence or absence of security functional requirements as a starting point for improving product security. The BITS packages of requirements that must be met to achieve a BITS Tested Mark do not stipulate an EAL requirement but rather leave the assurance testing level to be determined by the author of a Security Target or Protection Profile. An assurance level is contingent on the environment in which the product operates, its function in that environment, and the threats to the environment/product. These items are articulated in Security Targets and Protection Profiles. BITS does, however, recognize the importance of assurance levels and understands that most products testing for Common Criteria certification will be testing at an assurance level of EAL 3 or higher. In addition, testing at an EAL of 3 or higher could help facilitate meeting all of the security functional requirements set forth in the BITS packages.

What is the depth of the compliance specification and how do the specifications embrace emerging standards?

The BITS security criteria do not specify specific types of technologies or languages. Our security requirements are selected from a pre-defined catalog of security features under the Common Criteria. The BITS specifications do not mandate specific technologies or languages but rather outline common feature sets. There may be several different technology mechanisms that can be used to show the presence of a particular feature or comply with a particular requirement.

Will BITS provide a list of certified products and status on continued compliance?

Yes, BITS will provide a current list of certified products on its Web site, www.bitsinfo.org. BITS will monitor compliance with the security criteria as detailed in the requirements of the seal-use contract agreement, including collecting an annual attestation statement from the vendors of certified products.

Please clarify the seal usage fees. How much is the fee and how is it applied?

The seal use fee is an annual fee of \$2,500, which covers administration costs associated with issuing and maintaining the *BITS Tested Mark* certification seal. It applies per certification seal or per certified product, with a reduced incremental fee for multiple seals. A maximum fee of \$5,000 would be assessed for three or more products.

How can I estimate the cost of testing? How will my company be charged by a testing facility?

The duration of a product evaluation will be determined during the test preparation process. The total cost and time depends upon many factors, including product breadth and complexity, the criteria being tested against, and how well the product meets the criteria. Therefore, it is difficult to estimate testing costs. Testing services contracts between a testing facility and a technology vendor will address charges per hour and cost estimates. One of the reasons that we maintain an independent testing option is to offer a potentially faster and more affordable method for smaller firms to complete testing.

What is considered a product for testing? Under the independent testing route, who is making the decision for which criteria/profile the vendor should meet? If product has components that fall into several categories, which category should be selected? If a product supports multiple platforms, will it be necessary to certify each?

The *BITS Tested Mark* certification seal is issued to a particular product version. The technology vendor selects the environment, underlying systems/platforms, and boundaries for which the product will be tested. These should be reflected in testing documentation, which financial services companies may request to review. The selection of these items should consider the most representative environment of its financial services customers. If the technology vendor has a separate product version for each operating platform, each product version is eligible to be certified. A vendor should look at the product descriptions in the product class example matrix (see the BITS Web site at www.bitsinfo.org) or in each individual product profile (see the product description and subclasses, also on the Web site) to determine where a product “fits.” It may be that products simply don't qualify for testing because they do not fit into any of the current categories (e.g., operating systems).

If a vendor finds that the product fits in multiple categories or if the product is multi-functional, the vendor should select the most appropriate category under which to test, i.e., the one most closely aligned to the primary product functionality. Vendors are also encouraged to read through the criteria that will be applied in testing to make sure it is appropriate for the product. If the vendor thinks the product could meet all criteria in multiple categories and still has trouble identifying which category matches the product's primary functionality, the vendor should chose the category it would most like to see associated with its certification. Keep in mind, however, that BITS will not grant more than one certification per product.

Who determines the security criteria for testing? Has BITS compared its criteria to existing protection profiles?

A financial services working group led by a Profile Leader develops the criteria. After an initial, industry-defined profile is complete, the financial services working group holds criteria development workshops with outside information security experts from key technology providers, the regulatory community and select government agencies such as the Department of the Navy. The criteria are then presented publicly to the financial services industry and all stakeholders during an open comment period. Under the Common Criteria testing option, the BITS security criteria do not specify specific types of technologies or languages. Our security requirements are selected from a pre-defined catalog of security features under the Common Criteria. The BITS specifications do not mandate specific technologies or languages but rather outline common feature sets. There may be several different technology mechanisms that can be used to show the presence of a particular feature or comply with a particular requirement. In addition, within the Common Criteria,

differences exist not only in the choice of requirements but also in the assignment, refinement, selection and iteration tied to each requirement. For instance, BITS reviewed the Firewall Protection Profiles and determined that the financial services industry needs security requirements beyond those profiles. Accordingly, we developed the BITS product certification criteria. All future development of new product categories will begin with an analysis and consideration of those Protection Profiles and Security Targets already established for the respective product category. BITS does not intend to create additional requirements when existing protection profiles are adequate.

Will BITS create Protection Profiles?

No. Because BITS' requirements are intended to be broadly applied, we chose not to define threat statements and objectives, which are necessary items in a protection profile. Rather, BITS allows financial services companies and/or vendors to tailor the use of the packages in Security Targets and Protection Profiles to their needs.

Did BITS involve government agencies in vetting the requirements packages? Did BITS seek endorsement from financial regulators such as SEC?

Development of the original security criteria was a collaborative effort involving several financial services regulatory agencies and government bodies: the Office of the Comptroller of the Currency, Federal Reserve Board of Governors, Department of Navy and NIST. While BITS briefs the regulatory agencies periodically, these agencies are prohibited from formally endorsing the criteria. Although it's important that the regulatory community looks favorably upon the certification program, it is more important that the industry believes that the criteria are valuable.

Do you envision BITS members going beyond the stated BITS packages and developing additional packages under the Common Criteria?

Yes, eventually. The current packages do not cover the entire spectrum of product categories. They do, however, represent priority product categories at this time. All future development activities will consider the adoption of existing Protection Profiles in full or part.

How will BITS member organizations and the financial services industry use the *BITS Tested Mark*?

The *BITS Tested Mark* provides assurance that a technology product has been tested by an unbiased and professional facility and was found to have met the minimum-security criteria. The validity of the certification is maintained by the BITS Security Lab through its seal use, compliance and maintenance program. Each financial institution will decide how to apply test results in product selection decisions for their specific organization. Financial institutions will likely give favorable consideration to products with the *BITS Tested Mark* because of their known security features. Security testing has always been a component of the product implementation process; the *BITS Tested Mark* makes that process more efficient.

When do BITS members expect to be incorporating the *BITS Tested Mark* requirements into proposals and RFPs?

Many already have. Others have been provided with sample language to address compliance with the BITS criteria and will include language addressing the *BITS Tested Mark* within the next few months.

Will products be evaluated at the source-code level?

Source-code reviews will not be performed, nor will any on-site reviews of the development process. The testing process focuses on the security functionality of the product.

Can all Common Criteria-accredited labs perform BITS evaluations? Including international labs?

Yes. BITS certification requirements stipulate that a product may successfully test against the applicable BITS packages of security functional requirements with any Common Criteria accredited lab, including the international labs.

What is BITS doing to make sure there is not a “bottleneck” for vendors at the Common Criteria labs?

We trust that NIAP is monitoring the U.S. testing capacity and the demand for Common Criteria certification. While achieving certification is the end goal, BITS member companies will be looking at those products and vendors that are in the testing queue. In addition, the BITS Product Certification Program allows for testing independent of the Common Criteria; vendors are not required to go through Common Criteria testing for the certification.

NIAP and other agencies grant waivers because of the lengthy time it can take to get through their testing process. Does BITS offer such a waiver?

In certain cases, the government is required to issue waivers against its own mandate for certain government agencies to limit the procurement of products to those that are Common Criteria certified. However, U.S. antitrust laws prohibit private industry from imposing similar community-wide mandates.

Given the value of the BITS Product Certification Program, BITS member companies and other financial services organizations are making the certification a major factor in their software product purchasing decisions. Some firms have included certification testing requirements in sales contracts and procurement policies. Moreover, some may consider imposing individual deadlines for testing of existing or new products. Certification is an issue of critical infrastructure protection and the landscape of product testing requirements is likely to evolve rapidly.

What is the life of the product certification seal? Will I be required to retest product changes?

The *BITS Tested Mark* is good for the life of the specific version of the product tested as long as;

- the product remains in compliance with the security criteria,
- the company remains in compliance with the seal use rules,
- the company pays the annual seal use fee, and
- the product is not materially modified.

Material modification to a product includes,

- a product name change or any higher order digit numeric descriptor (e.g., a change from Product 5.XX to 6.YY would be deemed a material modification, but a change from Product 5.XX to 5.YY would not be deemed a material modification),
- a requirement that the customer re-license or make additional payment, or
- a change that would have adversely affected the ability of the tested product to successfully meet the security criteria.

The seal Sublicense Agreement should be reviewed for specific terms for using and complying with the certification seal.

What is the level of incremental testing to achieve a *BITS Tested Mark* with the Common Criteria certification?

The level of incremental testing is entirely dependent upon the set of security functional requirements—selected by the vendor or set forth in a Protection Profile—that are otherwise being tested for the Common Criteria certification. In some cases, there may not be any additional security functional requirements, while other situations will depend on the product and the comprehensiveness of the Common Criteria testing.

How will BITS enforce the certification?

The certification seal contract stipulates the contractual obligations for certification, including an annual attestation from the vendor stating continued compliance with the security criteria and seal use rules. Please refer to the seal use agreement and operating procedures manual on the BITS Web site at www.bitsinfo.org for further detail.

Where can I go for more information?

For more information about the BITS Security Lab and the *BITS Tested Mark*, visit www.bitsinfo.org/fslab.html, or contact BITS:

202.289.4322
bitslab@fsround.org
1001 Pennsylvania Avenue
Suite 500 South
Washington, DC 20004