

Senetas encryptors are certified to the most rigorous independent standards for cryptographic product design including FIPS140-2 and EAL4+. These standards are designed to provide an independent assessment of a products security and give an assurance of trust other than the one provided by the vendor.

Value of Certification

Governments and organizations worldwide use these assessments as a mark of trust for the security products they choose to encrypt their data.

Common Criteria

The Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria or CC) is an international standard (ISO/IEC 15408) for computer security certification. Common Criteria provides assurance that the process of specification, implementation and evaluation of a product has been conducted in a rigorous and standard manner.

The product or system that is evaluated is referred to as the 'Target Of Evaluation' (TOE) - the product or system that is the subject of the evaluation. Details of cryptographic implementation within the TOE are outside the scope of the CC. Instead, national standards, like FIPS 140-2 (see below) give the specifications for cryptographic modules, and various standards specify the cryptographic algorithms in use.

Evaluation Assurance Level (EAL) - the numerical rating (1 - 7) describing the depth and rigor of an evaluation. Each EAL corresponds to a package of security assurance requirements which covers the complete development of a product, with a given level of strictness. Higher EALs do not necessarily imply "better security", they only mean that the claimed security assurance of the TOE has been more extensively validated.

The Common Criteria Recognition Agreement (CCRA) is an arrangement that ensures that evaluations of Information Technology (IT) products and protection profiles are performed to high and consistent standards. Almost all countries where Senetas sells its encryptors are CCRA members. A list of member countries is at:

www.commoncriteriaportal.org/members.html

FIPS 140-2

The U.S. Federal Government and many other organisations looking to purchase a cryptographic product require that it be validated to FIPS 140-2. The FIPS validation process is long and expensive and knowing that some customers treat the FIPS requirement as a



check box, some vendors take the path of least resistance to achieve certification. So how do you verify that a product is really accredited?

First you must verify that the product really is FIPS validated or at least contains a FIPS validated module. Sometimes you will see the word “FIPS” used in statements like, “FIPS compliant”, or “implements FIPS approved algorithms”, however these statements don’t mean validated. Validated modules must have a certificate. If it is not clear then ask the vendor for the certificate number and verify it on the NIST web site:

<http://csrc.nist.gov/groups/STM/cmvp/validation.html>.

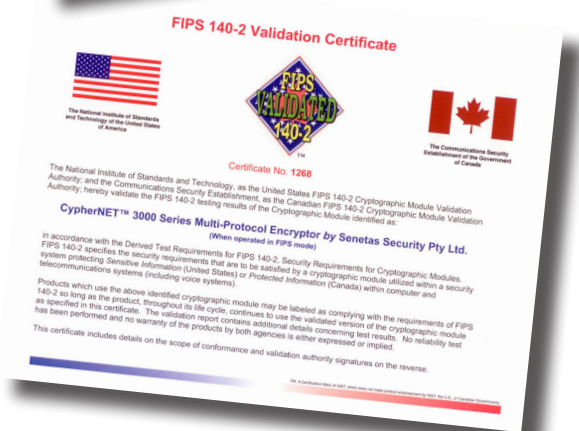
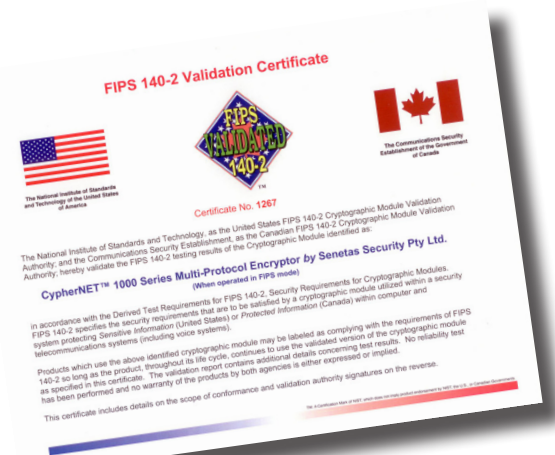
The next (easy) step is to look at the overall validation level. The 4 levels of validation cover a wide range of security requirements and are summarized as follows:

- Level 1: The lowest level - provides basic assurance that algorithms are correct - no physical security or authentication requirements – can be software only
- Level 2: Adds physical security with tamper evidence – at least role based operator authentication
- Level 3: Stronger physical security with tamper detection and response for covers and doors - identity based operator authentication
- Level 4: Strongest physical security with tamper detection and response for the entire enclosure

Senetas encryptors are accredited to **FIPS 140-2 level 3**, and therefore provide the level of physical protection and intrusion detection required to secure your network. The certificate numbers are 1267 for the CN1000 Series and 1268 for the CN3000 Series.

As a final check you may want to check out the products Security Policy on the <http://csrc.nist.gov/> website to ensure that your deployment would be in a FIPS approved mode. Although this may appear paranoid, there have been instances where a product claims accreditation because it contains an accredited module. In these cases the product itself is not validated and there is no public document like the Security Policy that clearly states what you need to know. Given this, you must first check that the product is utilizing the module correctly, and then check that the product is actually meeting your security requirements.

If you are in the market to buy a FIPS validated solution it is wise to do more than look for “FIPS” as a check box item. The security of your information is at stake.



Acknowledgement

Please refer to Wikipedia on the Internet for additional detail on the certification of security products and the value that this delivers to users. Senetas acknowledges Wikipedia as a source of content.