Certification Authorities for Trusted Computing in Military and Avionics Products

Trusted Computing: The COTS Perspective Series

Read About

Introduction

In the world of security and Trusted Computing, there are many different disciplines involved, from cybersecurity to safety certification. With a constantly evolving set of standards and possible certifications, it can be confusing to understand what certifications might apply to your system, which of those are worthwhile, and what the important aspects are when considering certification or certified products.

An example of a system designed for use in Trusted Computing applications, Curtiss-Wright's Data Transport System (DTS1) Network Attached Storage (NAS) storage device is the embedded industry's first commercial off-the-shelf (COTS) data-at-rest (DAR) storage solution designed to support CSfC, with two layers of full disk encryption (FDE) in a single device.

This white paper provides an overview of some of the certification authorities that are involved in Trusted Computing, explores which disciplines they oversee, and gives guidance on when to get these certification authorities involved. While this white paper will focus specifically on the US market, it will also discuss ways in which these bodies are relevant (or not) in some international markets.

National Institute of Standards and Technology (NIST)

The NIST manages multiple standards across many industries. Some of these standards include areas of Trusted Computing, including cryptographic algorithms and documents used to define the Risk Management Framework (RMF). Some of the certification programs related to Trusted Computing that are administered by NIST are specified below.

Cryptographic Module Validation Program (CMVP)

The CMVP is a program jointly administered by NIST and the Canadian Centre for Cyber Security (CCCS). This program performs independent testing of cryptographic modules at independent labs for conformance to FIPS 140-2 Security Requirements for Cryptographic Modules. For standalone cryptographic modules this certification can show thorough testing, providing confidence to customers on the security and implementation of cryptographic algorithms. FIPS 140-2 provides for multiple security levels (1 to 4) mainly related to physical security capabilities, so vendors need to ensure that they apply for the appropriate level of certification, and customers need to verify that products are certified to meet their required level of security.

Cryptographic Algorithm Validation Program (CAVP)

As opposed to the CMVP, the CAVP just ensures that cryptographic algorithms have been faithfully implemented, either in hardware or software. The CAVP is a prerequisite to the CMVP. Subsets of algorithms can be selected for validation and the NIST maintains the list of certified testing laboratories, and validated algorithm implementations.

Risk Management Framework (RMF)

The RMF is a process for assessing risk and is designed specifically for Federal Information Systems. In addition to assessing risks, the RMF provides guidance on selecting controls to mitigate risk, and then authorizing and monitoring those systems. While the framework itself is maintained by the NIST in a series of special publications (SP 800-53, SP 800-34, SP 800-61, SP 800-53A, SP 800-37, SP-800-137, SP 800-60, and others), the latter does not perform assessment or certification of systems under RMF. Programs should be assessed under guidance of the SP 800-53A Guide for Assessing the Security Controls in Federal Information Systems and Organizations. Different departments and agencies will determine who provides the oversight needed to give approval after appropriate assessments are completed in order to allow systems to operate.

Common Criteria (CC)

CC is a standard administered by the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). It serves as a framework that allows products to be evaluated against a defined Security Target (ST) and Security Functional Requirements (SFR). Normally, products will pull much of their ST from an already defined Protection Profile (PP) for a given set of products. Products are then evaluated against their defined ST and SFR at an independent lab.

Furthermore, when being evaluated, the Evaluated Assurance Level (EAL) can also be selected from level 0 to level 7. The EAL dictates the strictness of the evaluation, with higher levels looking at the entire development process of the product, and the highest level requiring formal verification of security claims. It is important to remember that higher EAL levels do not imply higher security, they simply show that there is a higher level of confidence in the verification of the security claims. Because CC certification by itself only states that the evaluated product meets its defined ST and SFR, vendors must clearly select/define, and customers must closely evaluate, the ST and SFR of any product to ensure that the defined capabilities meet the security needs for their system and have been evaluated to the appropriate confidence.

National Information Assurance Partnership (NIAP)

The NIAP is the group within the US that manages the certification of COTS components to CC certification. NIAP works with certified testing laboratories to perform CC certification and maintains the list of validated products.

Commercial Solutions for Classified (CSfC)

CSfC is a program run under the NSA that takes CC certified security solutions, layers those solutions to produce a product, and certifies that the resulting product can securely protect National Security Systems (NSS) that operate on classified data. The NSA may put additional requirements on a product, or require that certain CC protection profile selections for products are included on the CSfC list. For that reason, for any product intended to be included as part of a CSfC solution in an NSS, the designer should start discussions on CSfC with the NSA prior to going through CC certification for individual portions of that CSfC product. CSfC provides an alternative to using Type-1 NSA certified cryptography on US NSS. Its use does present tradeoffs that should be considered that can affect product lifecycle, key management requirements, and product classification when determining whether Type-1 or CSfC is most appropriate for a given program or product.

Defense Information Systems Agency (DISA)

The DISA is part of the US DoD and helps ensure continued operation and security of the US DoD Global Information Network. DISA also manages a repository of Security Technical Implementation Guides (STIG) that can be used as guidance to help secure computing systems. STIGs can range from very general to product version specific. While the DISA does not perform certification, they do maintain the set of STIGs used to secure systems, and they approve submitted STIGs prior to including them in the list. Vendors who want to generate and provide specific STIGs for their own products can submit them to the DISA for approval and inclusion.

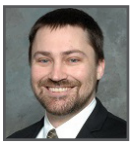
RTCA DO-178C/EUROCAE ED-12C

This standard, regarding Software Considerations in Airborne Systems and Equipment Certification, is used as a design assurance guideline in the US by the Federal Aviation Administration (FAA) (as well as by the European Aviation Safety Agency [EASA] and Transport Canada) to approve the airworthiness of software that will be used in aviation systems and can impact flight safety. It details the requirements for software development, testing, test coverage, and reliability. There are multiple design assurance levels (DALs) based on the level of criticality of the system failing, with “A” indicating catastrophic danger and “E” indicating no impact on safety. While the DoD performs self-certification, for commercial systems that might be used in commercial aviation markets, DO-178C certification of software elements would be critical. Since the DO-178C specification can heavily influence the entire software development process, ensuring that the requirements are well understood prior to starting development is essential.

RTCA DO-254/EUROCAE ED-80

The DO-254 standard (Design Assurance Guidance for Airborne Electronic Hardware) is the hardware counterpart to DO-178C used by the FAA, as well as EASA and Transport Canada. DO-254 is meant to provide design assurance guidance for certification for complex electronic components that are used in avionics equipment and can impact flight safety. As with DO-178C, levels of criticality exist (A to E), and the DO-254 guidelines can impact the entire development process for hardware. For this reason, requirements to meet DO-254 certification should be fully understood before beginning development of a new complex hardware avionics component.

Author(s)



David Sheets
Architect
Curtiss-Wright Defense Solutions

Conclusion

It's important to fully understand which security protections, safety standards, and certification authorities are relevant to your technology and program, as well as the process and requirements necessary to attain them. See below for more information about DO-254/178 and the safety certification process.

Learn More

Curtiss-Wright Products

- Data-at-Rest (DAR) Protection
- Security Enabled Curtiss-Wright Single Board Computers and Digital Signal Processing

Curtiss-Wright Case Study

- Building a Truly Trusted Computing Solution with COTS Hardware and Intel Security Capabilities

Curtiss-Wright White Papers

- The Many Faces of Trusted Computing: What You Need to Know to Protect Critical Platforms and Data
- Getting Secure, Intel-Based Solutions to Market Faster - Why the Hardware Vendor's Boot Security Implementation Is So Important
- Beyond Trusted Computing: Extending Protection Capabilities to Deliver TrustedCOTS Solutions
- Trusted Computing: The COTS Perspective Series
  1. Introduction to COTS-based Trusted Computing
  2. Trusted Boot
  3. Hardware Features for Maintaining Security During Operation
  4. Considering the Role of Hardware in Securing OS and Hypervisor Operation
  5. Application Development, Testing, and Analysis for Optimal Security
  6. Developing a Secure COTS-Based Trusted Computing System
  7. The Impact of Protecting I/O Interfaces on System Performance
  8. Decomposing System Security Requirements
  9. Establishing a Trusted Supply Chain
  10. Certification Authorities for Trusted Computing in Military and Avionics Products