International Certification Authorities for Trusted Computing

Trusted Computing: The COTS Perspective Series

Read About

- Importance of international agreements for security and Trusted Computing
- Relevant certification authorities around the globe
- Processes applied to NATO member nations

Introduction

In our previous white paper, Certification Authorities for Trusted Computing in Military and Avionics Products, we provided an introduction to the North American government agencies that serve as certification authorities for security and Trusted Computing. As a follow up, this white paper provides an overview to the international government agencies that perform security accreditation for equipment such as network switches, storage devices, and ruggedized computers used in military applications.

The UK's Ministry of Defence (MoD) and NATO are among the many certification authorities present worldwide that perform security accreditation for a wide range of equipment used in commercial and military applications.

International Agreements

International agreements exist to recognize North American certifications; for example, the National Information Assurance Partnership (NIAP) recognizes Common Criteria (CC) schemes and Protection Profiles (PP). The goal of such agreements is to reduce the level of re-assessment for use on a particular international military program. Nevertheless, applicants are generally required to submit a Security Target document that describes the Target Of Evaluation (TOE) and the relevant protection features built around the critical security areas, such as hard drive encryption, key management, and secure boot that

cryptographically verifies executable code on power-up. The extent of these features depends on the type of program. For example, secure boot can range from validating checksums prior to loading code, to verifying cryptographic signatures, and decrypting all boot artifacts. Government agencies will issue high-level requirements that specify the protection levels.

International Certification Authorities

Below we look at specific agencies and protection schemes for individual countries.

United Kingdom

The UK Ministry of Defence (MoD) issues a Security Aspects Letter (SAL) on a new military program. In turn, the National Cyber Security Centre (NCSC) determines the assessment process level, the highest grade being the CAPS (CESG Assisted Product Service), with official-level programs following the CPA (Commercial Product Assurance) Certification route.

CAPS assessments are performed directly by the NCSC, whereas CPA approvals are outsourced to licensed evaluation facilities.

Companies performing development work in this field also need to meet facility-level IT and access security requirements, which flow down from Defence Condition DEFCON 658 (Cyber) and Defence Standard DEFSTAN 05-138 (Cyber Security for Defence Suppliers). The MoD sponsors a scheme known as Cyber Essentials Plus, whereby potential suppliers can seek accreditation against these requirements.

France

The French government agency Agence nationale de la sécurité des systèmes d'information (ANSSI), which is equivalent to the NCSC, provides two certification schemes dependent on the security level, which are assessed by Centres d'évaluation de la sécurité des technologies de l'information (CESTI) approved facilities.

The CESTI schemes are:

+ Critères communs (CC) = Common Criteria
  - Applicable to products already accredited in another country that is a signatory to the ITSEC accord (includes US, UK & Canada)
  - Based on ISO15408 (IT Security) and focused on network, enterprise-level computing
+ Certification sécuritaire de premier niveau (CSPN) = First Level Security Certification
  - Note that CSPN accreditation is not normally recognized outside of France

Germany

Equally, the German Federal Office for Information Security, known as Bundesamt fur Sicherheit in der Informationstechnik (BSI), offers similar accreditation schemes for its country's providers.

Italy

The Italian Ministry of Economic Development is the regulatory agency for security and integrity for electronic communication systems.

Spain

The Spanish Government Agency for certifying cryptographic equipment is the Organismo de Certificación - Centro Criptológico Nacional (OC-CCN).

Turkey

Part of the Tubitak organization, the Turkish National Research Institute of Electronics and Cryptology is referred to locally as Ulusal Elektronik ve Kriptoloji Arastırma Enstitüsü (UEKAE).

South Africa

In South Africa, COMSEC Electronics Communications Security, a company owned by the South African Government, is tasked with securing government communications against unauthorized access. It provides verification services for electronics communications security systems, products, and services used by the government.

South Korea

The Korea Internet & Security Agency (KISA) is the South Korean government agency responsible for international cybersecurity. It is managed by KrCERT/CC within KISA. South Korea has an NCSC within the National Intelligence Service that coordinates with KrCERT/CC.

Australia

The Australian DoD State Security Agency provides cryptographic evaluations under the Australian Signals Directorate (ASD).

European Union (EU)

For the EU, the European Union Agency for Network and Information Security (ENISA) is the certification organization for Trusted Computing.

NATO

Cryptographic products which are developed and produced in a NATO member nation and which are evaluated and approved in accordance with the INFOSEC Technical and Implementation Directive on Cryptographic Security and Cryptographic Mechanisms, by the developing nations National Communications Security Authority, are eligible to be submitted for inclusion to the NATO Information Assurance Product Catalogue (NIAPC). The list of cryptographic products and cryptographic mechanisms is updated and maintained by the NATO Communications and Information (NCI) Agency Cyber Security on behalf of input provided by the National Communications Security Authority of the NATO member nation. The NCI Agency develops interoperable C4ISR capabilities, operates the NATO Information Assurance Product Catalog (NIAPC), and recognizes “Collaborative Protection Profiles” under the NATO Common Criteria. The NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) is based in Tallinn, Estonia.

Conclusion

In order to effectively sell Trusted Computing and security products and systems into North American and international markets, companies need to ensure that the correct certification authorities and processes are identified, understood, and adhered to. To simplify the process of bringing certified content into new countries, international agreements exist to recognize foreign certifications and should be explored.

Author(s)

David Sheets
Senior Principal Security Architect
Curtiss-Wright Defense Solutions

Paul Hart
Chief Technology Officer
Curtiss-Wright Defense Solutions

Learn More

Curtiss-Wright Products

- Curtiss-Wright TrustedCOTS™
- DTS1: 1-slot Rugged Network Attached File Server
- Data-at-Rest (DAR) Encryption
- DO-254 & DO-178 Safety-Certifiable COTS Solutions

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
- Accelerate Time-To-Market With Safety-Certifiable Airborne Electronics Hardware
- Understanding Your Safety-Certifiable COTS Options: A Closer Look at the Subsystem Level
- Why Dissimilar Redundant Architectures Are a Necessity for DAL A
- 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
  11. International Certification Authorities for Trusted Computing