Product Assurance in the UK - Common Criteria, Commercial Product Assurance and CESG Claims Tested Mark - is there any convergence?

Simon Milford
SiVenture
Contents

- History
  - UK CC Scheme
  - UK Product Evaluation Schemes
- Current Status
  - UK CC Scheme
  - UK Product Evaluation Schemes
- CPA
  - What is CPA
  - Security Characteristics
- Convergence
UK Common Criteria Scheme History

- Mid 1980s – creation of UK Scheme, evaluating against UK Levels
- Early 1990s – adoption of ITSEC methodology, jointly developed between UK, France, Germany and the Netherlands
- Late 1990s – adoption of Common Criteria within UK IT Security Evaluation and Certification Scheme
  - Spin offs included Sys N for system evaluations and Fast Track for product assessments (both now defunct)
UK Product Assurance History

DTI

CESG

UK Scheme (pre-ITSEC)

CESG Assisted Products Scheme (crypto)

ITSEC

Common Criteria

Commercial Product Assurance

CESG CTM

Central Sponsor for Information Assurance

CCTM
UK CC Scheme – current status

- Certificate authorizing nation
- Member of JHAS, hence able to certify smartcard and chip evaluations
- Member of JTEMS, hence able to certify payment terminal evaluations

- Currently only certifying up to EAL2, unless evaluating against a PP from a technical community (e.g. JHAS/JTEMS)
UK CC Scheme – Lab Status

- 3 labs:
  - SiVenture
  - Plus two others
Commercial Product Assurance

http://www.cesg.gov.uk/products_services/iacs/cpa/index.shtml
What is Commercial Product Assurance?

- Product Assurance scheme including:
  - Standardised sets of product security requirements (Security Characteristics)
  - Requirements for developer security (Build Standard)

- May be thought of as being similar to CC with
  - Protection Profiles
  - ALC_DVS, ALC_CMC, ALC_CMS
Commercial Product Assurance (CPA)

CPA for Developers - Current Test Labs

This page will include a list of all currently approved CPA Test Laboratories, including Points of contact. It will also state which Test Labs have successfully tested against which Security Characteristics.

<table>
<thead>
<tr>
<th>Test Lab</th>
<th>Status</th>
<th>Security Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enex Test Lab</td>
<td>Provisional</td>
<td>Software Full Disk Encryption</td>
</tr>
<tr>
<td>SiVenture</td>
<td>Provisional</td>
<td>✓ VPNs for remote working - In Pilot</td>
</tr>
</tbody>
</table>

The Table above indicates which Test Labs have successfully tested against which Security Characteristics. However, any Test Lab is permitted to test against any of the Security Characteristics listed in the table. However the first evaluation of a particular Security Characteristic by a particular Test Lab may require extra CESG oversight.

Provisional Test Labs are ones which have completed the relevant pre requisite activities and qualifications and are currently waiting to undertake or complete an initial CPA Trial Test.

Further Clarification

If you have any comments or queries on the comments above please E-Mail them to cpa@cesg.gsi.gov.uk
Security Characteristics (short term)

- Security Characteristics under development:
  - Software Full Disk Encryption (at v1-0)
  - IPsec VPN Gateway and Client (at v1-0)
  - Software media encryption (draft)
  - Server Virtualisation (draft)
  - Email encryption between gateways (draft)
  - IP filtering Firewall (draft)
  - Hardware media encryption (draft)
  - Data destruction (draft)
  - Desktop email encryption (draft)
  - Network authentication (draft)
Security Characteristics (medium term)

- WPA-2 wireless client/network devices (planned)
- Web Application Firewall (planned)
- Self-encrypting hard drives (planned)
- Data sanitisation (planned)
- Endpoint lockdown and control (planned)
- SSL-VPN (planned)
- One-time password generator (planned)
- Desktop virtualisation (planned)
- SAN segregation (planned)
Security Characteristics (longer term)

- Security Characteristics dreamed of:
  - Session border controller as part of VOIP solution.
  - Intrusion Detection System
  - Client AV product
  - Database separation
  - Bootable media for remote working
  - Data export guard
CPA Evaluation Process

- Select Test Lab (SiVenture …)
- Select SC relevant to product
- Submit application to Scheme
- Evaluate product against requirements in SC
- Perform Build Standard evaluation (if required)
- Lab submits Test Report to Scheme for approval
- Certification
Convergence ...?

- CPA Evaluation Process
  - Select Test Lab (SiVenture ...)
  - Select SC relevant to product
  - Submit application to Scheme
  - Evaluate product against requirements in SC
  - Perform Build Standard evaluation (if required)
  - Lab submits Test Report to Scheme for approval
  - Certification

- CC Evaluation Process
  - Select Test Lab (SiVenture ...)
  - Select PP relevant to product
  - Submit application to Scheme
  - Evaluate product against ST (check compliance with PP)
  - Development Environment Assessment if required
  - Lab submits Test Report to Scheme for approval
  - Certification
Convergence (2)

- **CPA**
  - SC Requirements informed by threat knowledge
  - SC includes assurance requirements specific to product type
  - SC development influenced by vendors and end users

- **CC**
  - New PPs informed by threat knowledge
  - New PP includes assurance activities specific to product type
  - Tech community includes vendors and end users
Convergence (3)

- **Best Case**
  - New PP exists
  - SC exists
  - PP and SC are consistent

- **Perform CPA and CC in the same evaluation**
  - Needs lab who is both CPA and CC
Convergence (4)

- Worst case
  - Either SC or new PP don’t exist, or
  - They are largely inconsistent

- Perform both in same lab will still gain some efficiencies
  - Again lab needs to be both CC and CPA
Summary

- For best convergence we need to co-ordinate the development of Security Characteristics (in the UK) and Protection Profiles – a current example of this is for encrypted USB devices.

- CESG supports the formation of these technical communities and is providing inputs to each of them. The input of vulnerability, mitigation and assessment evidence is particularly important in this regard, and CESG is working to have this aligned with the 'security characteristics' being used in the Commercial Product Assurance (CPA) process at the 'Foundation' grade.

- The evaluation methodologies overlap widely – enabling two certifications from a single evaluation project.
Questions?

For further information on SiVenture services please go to www.siventure.com or call +44 (0) 1628 651366
SiVenture
A division of NDS

SiVenture
A division of NDS

Simon Milford
Head of SiVenture
Unit 6, Cordwallis Park, Clivemont Road, Maidenhead
Berkshire, SL6 7BU, United Kingdom
T: +44 (0) 1628 651 366  F: +44 (0) 1628 651 365
M: +44 (0) 7881 918 199  E: simon.milford@siventure.com
www.siventure.com