SiVenture
A division of Cisco

A CPA Update

(Supporting the development of CC)

A Test Lab Perspective

Simon Milford

Head of SiVenture

SiVenture
A division of Cisco

Revision – CPA, what is it?

- Commercial Product Assurance
  - A UK specific product assurance scheme
  - Based on evaluation of products against specified requirements (called Security Characteristics)
  - Use qualified labs and defined methodology
  - Certificates issued by CESG

Revision (2) – what was the state in Paris

- Pilot Evaluations were complete
- Methodology was published
- Security Characteristics were more numerous
- Build Standard was published
- 3 labs (one Fully approved, two interim)

SiVenture
A division of Cisco

Current Description

- Commercial Product Assurance. CESG's new scheme for the evaluation and certification of commercial security-enforcing products for use in the UK Public Sector.
- Build Standard. A standard which describes properties of a developer's security engineering approach which is assessed as part of a CPA evaluation. This is used to gain confidence in the product developer's processes and to give assurance that the quality of a security product is not expected to decrease over the duration of a CPA certificate

SiVenture
A division of Cisco

Available SCs (Part 1)

Product Category	Security Characteristic	Published Date
Data at Rest Encryption	Enterprise Management of Data at Rest Encryption v1.0 Allows the remote administration of key components of data at rest encryption products, including policy management, user account management, device encryption key management, device recovery and device purging.	Jan 2013
Data at Rest Encryption	Hardware Media Encryption v1.2 Maintains the confidentiality of data on mass storage devices through the addition of cryptographic hardware.	Apr 2012
Data at Rest Encryption	Software Full Disk Encryption v1.23 Protects the confidentiality of data at rest.	Mar 2013
Data at Rest Encryption	Software Media Encryption v1.1 Maintains the confidentiality of data on mass storage devices through the addition of cryptographic hardware.	Aug 2011
Data Sanitisation	Data Sanitisation: Degaussers v2.5 Sanitises data on magnetic media forms such as hard disk drives and tapes such that confidentiality is maintained.	May 2012
Data Sanitisation	Data Sanitisation: Flash based Media v0.3 Sanitises all flash-based storage media such as solid-state hard drives, USB 'Thumb' drives and SD cards.	Aug 2011
Data Sanitisation	Data Sanitisation: Overwriting Tools For Magnetic Media v1.6 Overwrites information from a piece of magnetic media prior to reuse.	May 2012
Endpoint Lockdown and Control	Software Execution Control v2.1 Limits the software applications and services that are able to run on an Operating System	Jan 2013

SiVenture
A division of Cisco

Available SCs (Part 2)

Email Encryption	Desktop Email Encryption v1.0 Protects the confidentiality and integrity of emails in addition to providing the recipient with authentication of the sender, for email messages sent to and received by a user endpoint.	Apr 2012
Email Encryption	Gateway Email Encryption v1.0 Protects the confidentiality and integrity of emails in addition to providing the recipient with authentication of the sender, for email messages as they transit the boundary of a secure network.	Mar 2012
Firewall	IP Filtering Firewall v1.1 Protects network boundaries or specific areas of networks by permitting only traffic from certain hosts to reach certain destinations (and vice versa).	Oct 2011
Firewalls	Stateful Traffic Filter Firewall *(SC-CC Mapping Document)* v1.0 Devices capable of filtering IP and TCP/UDP network traffic based on administrator-configured rules.	Mar 2013
Firewalls	Web Application Firewall v1.3 Prevents a range of malicious communications from reaching a protected web server and the applications running on it.	May 2012
Remote Desktop	Remote Desktop v1.0 Allows basic user control of machines running a remote desktop server located within another security domain.	Jul 2012

Available SCs (Part 3)

Secure Voice over IP - Client	Secure VoIP Client v2.0 Used to make secure voice calls over an untrusted network. The client aims to provide an encrypted and mutually authenticated channel for VoIP calls to be made between mobile or fixed devices.	Feb 2013
Virtualisation	Desktop Virtualisation v1.21 Provides the ability to run multiple instances of a commercial operating system on a single piece of hardware, distinguished by frequent interactive use by a single user.	May 2012
Virtualisation	Server Virtualisation v2.21 Provides the ability to run multiple instances of a commercial operating system on a single piece of hardware, distinguished by a need for unattended running and remote access by multiple users.	May 2012
VPN	IPSec Security Gateway v2.3 Provides an endpoint for an IPsec Virtual Private Network (VPN) tunnel, from either a VPN client or another Security Gateway.	Apr 2013
VPN	IPsec VPN for Remote Working Software Client v2.3 Provides secure corporate network connectivity over a less-trusted network	Apr 2013
VPN	TLS VPN for Remote Working - Software Client v1.0 Provides secure corporate netwrok connectivity over a less-trusted network.	Jul 2013
VPN	TLS VPN Security Gateway v1.0 Provides an endpoint for an IPsec Virtual Private Network (VPN) tunnel, from either a VPN client or another Security Gateway.	Jul 2013

In Development SCs

The following Security Characteristics are currently in development.

Product Category	Security Characteristics
Data at Rest Encryption	Data at Rest Encryption: Always on Aims to maintain the confidentiality of data stored within a device which is powered on in an enviroment where the risk of loss, theft or physical attack is elevated. Includes devices kept in low powered states often covering terms such as 'locked' and' sleep'.
Data Sanitisation	Data Sanitisation: Overwriting Tools for Magnetic Media Overwrites information from a piece of magnetic media prior to reuse.
Mobile Device Management	Mobile Device Management (Client) Enforces lockdown policy on handset, tablet or mobile device, prescribed from a Mobile Device Management (MDM) Server.

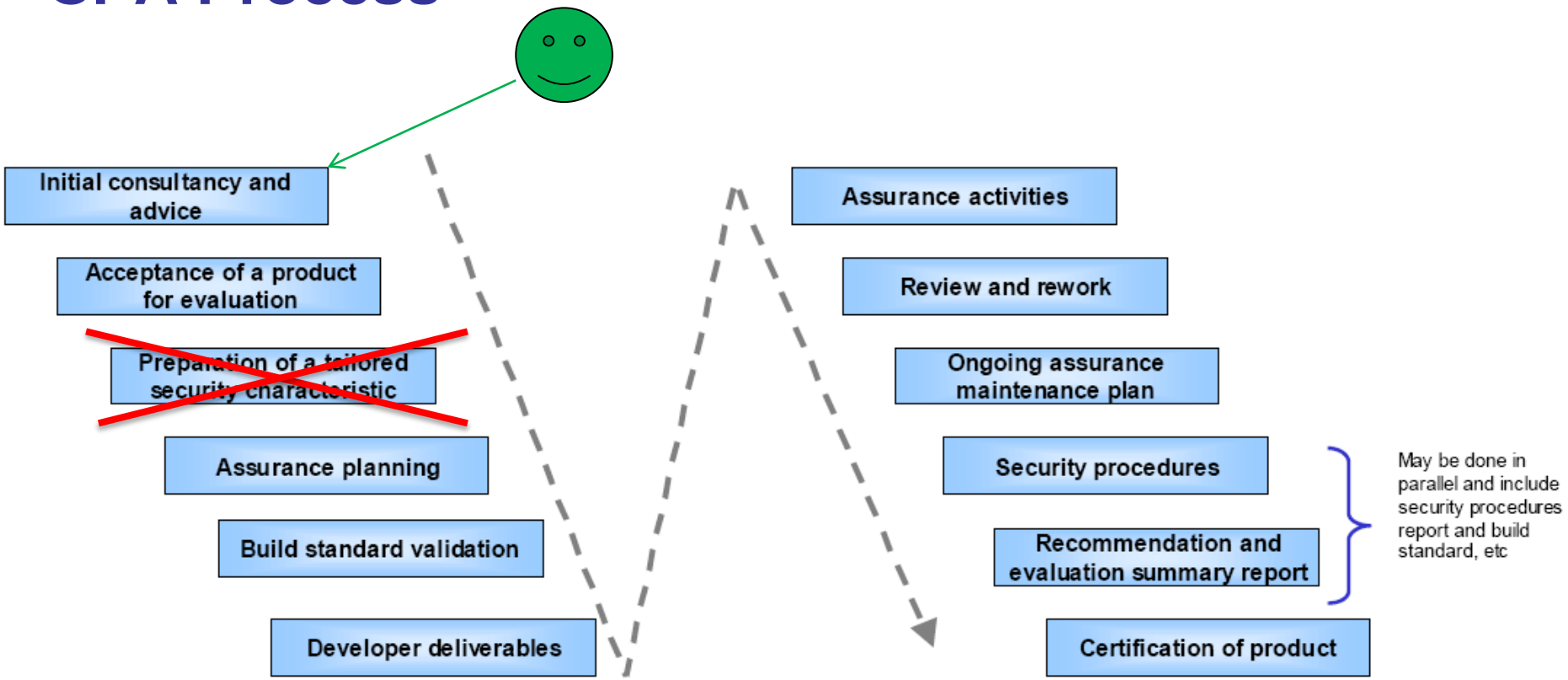
Archived SCs

The following table lists previously published version of Security Characteristics.

Product Category	Security Characteristics	Published Date
Data at Rest Encryption	Software Full Disk Encryption v1.22 (PDF, 318KB)	Aug 2012
	Software Full Disk Encryption v1.21 (PDF, 326KB)	Mar 2012
	Software Full Disk Encryption v1.1 (PDF, 320KB)	Sep 2011
	Software Full Disk Encryption v1.0 (PDF, 204KB)	Apr 2011
	Products designed to protect the confidentiality of date at rest.	
Data at Rest Encryption	Hardware Media Encryption v1.0 (PDF, 342KB) Removable media device (such as a USB thumb drive) with in-built hardware encryption functionality).	Apr 2011
Virtualisation	Client Virtualisation v1.1 (PDF, 349KB) Product that provide the ability to run multiple instances of a commercial operating system on a single piece of hardware.	Sep 2011
VPN	IPSec Security Gateway v1.1 (PDF, 396KB) Products that provide secure network connectivity over a less-trusted network.	Mar 2012
VPN	IPSec VPN for Remote Working - Software Client v1.1 (PDF, 412KB) Products that provide secure network connectivity over a less-trusted netwrok.	Mar 2012

SiVenture
A division of Cisco

CPA Process



SiVenture
A division of Cisco

Certified Products

Vendor	Product	Security Characteristic	Awarded	Expires
BeCrypt	DISK Protect 7.0.1	Software Full Disk Encryption 1.1 (PDF, 325KB)	29/02/2012	28/02/2014
Cisco Systems	ISR/ASR 1.2	IPSEC Security Gateway 1.2 (PDF, 405KB)	17/01/2013	31/01/2014
Juniper Networks	SRX Series 10.4	IPSEC Security Gateway 1.2 (PDF, 405KB)	15/05/2013	31/01/2014

SiVenture
A division of Cisco

Products In Evaluation

The following products are currently being evaluated by CPA Test Labs.

Vendor	Product	Security Characteristic	Test Lab
Cryptify	Call Version 3	Call Version 3	Roke
Egress	Switch 3.0	Gateway Email Encryption v1.0 Desktop Email Encryption v1.0	Context IS
iStorage	diskAshur Secure USB 3 Hard Drive Version 1 and diskAshur DT USB 3 Secure Hard Drive Version 1	Data at Rest Encryption - Hardware Media Encryption v1.2	SiVenture
iStorage	datAshur Secure USB Flash Drive firmaware Version 12	Data at Rest Encryption - Hardware Media Encryption v1.2	SiVenture
Microsoft	Windows Server 2012	Server Virtualisation v1.21	CGI
Tabernus	Enterprise Erase v6.3	Data Sanitisation - Overwriting Magnetic Media v1.6	SiVenture
Ultra Electronics	X-Kryptor PRIME Gateway	IPSec Security Gateway v2.3	Roke

CPA Labs

Was

Test Lab	Enex Test Lab	Logica UK limited	SiVenture
Status	Provisional - Interim	Provisional	Full

Is now

Test Lab	CGI	Context Information Security	KPMG LLP	NCC GROUP plc	Roke Manor Research Limited	SiVenture
Status	Provisional	Provisional	Provisional	Provisional	Provisional	Full

SiVenture
A division of Cisco

CPA Process Document

PROCESS FOR PERFORMING CPA
FOUNDATION GRADE EVALUATIONS

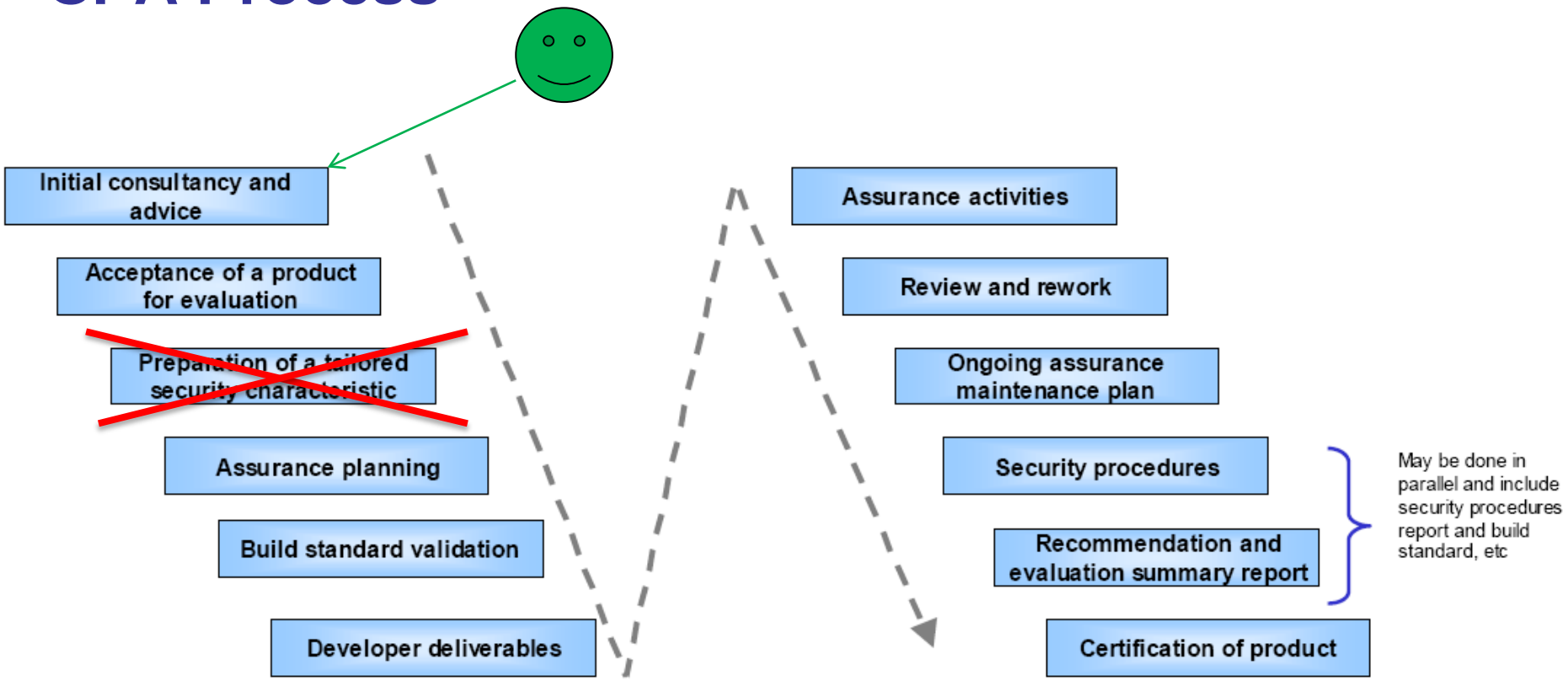
Version 2.1

Document History

Version	Date	Description
1.0	April 2011	Version 1.0 for release
1.1	July 2011	Added support for Cryptographic Interoperability, Cryptographic Testing and Product Families
1.2	August 2011	Minor changes following internal review
1.3	August 2011	Clarification text added on assurance activities and fuzzing
2.0	September 2011	Approved and issued
2.1	June 2012	Updates for bespoke protocols and network robustness testing, clarification around mitigation interpretation and revision of document templates.

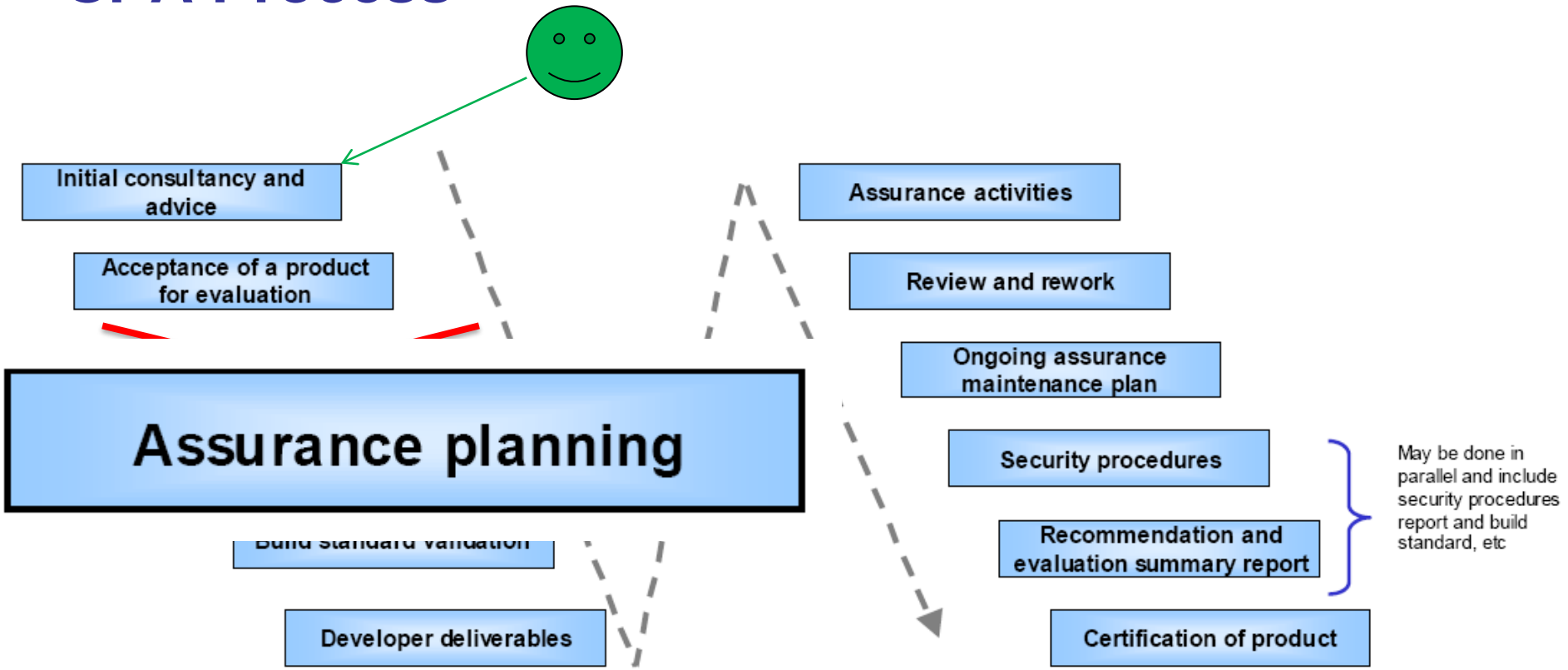
SiVenture
A division of Cisco

CPA Process



SiVenture
A division of Cisco

CPA Process



The Assurance Plan

- Each mitigation
  - DEV
  - VER
  - DEP
- How will Lab evaluate the product's compliance with the mitigation?
- Must be agreed with CESG – before:
  - Continuing with the evaluation
  - Product being listed as "In Evaluation"

Recent Developments

- Publication of SCs with Common Criteria Protection Profile Mappings

B.1 Protection Profile selections

There are a number of specific selections which must be made by the author of a Security Target derived from the above Protection Profile to ensure overlap with the Security Characteristic:

1. FCS_COP.1.1(1) CBC mode must be selected. Other modes may also be acceptable, please discuss with CESG.
2. FCS_CKM.1.1(Y) The selection must be using 'NIST SP 800-132 with a salt generated using a Random Bit Generator as specified in FCS_RBG_EXT.1'. Other selections within this option can be made at the developer's discretion.
3. If the product supports protecting hibernation mode (a power-saving mode in which the contents of memory are saved to disk) then the requirements in section C.5.1 must have been included in the assessment.

Recent Developments

- Publication of SCs with Common Criteria Protection Profile equivalence

1.1 Introduction

The NIAP[1] *Network Device Protection Profile (NDPP) Extended Package: Stateful Traffic Filter Firewall (v1.0)* document describes a set of requirements for Stateful Traffic Filtering Firewalls which can be assessed through the Common Criteria scheme.

The document you are now reading is a CPA Security Characteristic that directly translates its requirements onto those for the *NDPP*.

CESG believe that a product assessed against these requirements via Common Criteria meets the technical requirements for a CPA Foundation Grade Stateful Traffic Filtering Firewall.

SiVenture
A division of Cisco

CPA and CC

Should you just use CC?

Ideally, yes. However, at the current time, CC does not always represent a necessary or sufficient level of product assurance for the UK public sector due to the way the scheme has been employed internationally. Many products are assessed against Security Targets which bear little relationship to the likely threats that they will face, and which do not allow like-for-like comparisons of similar products. For clarity, the CC methodology is reasonable, but the way use of it has evolved over the years has led to unfortunate and ineffective outcomes.

Through our engagements with the international CC community, we are working to help rectify this; bringing our experiences from CPA to the discussion.

The (a) Fundamental Difference …

THE CPA BUILD STANDARD

Version 1.2

Rqt		
1	**CC Relationship:**	[1]: ALC_CMC.1.1C, ALC_CMC.3.7C, ALC_CMC.5.11C.
2	**CC Relationship:**	[1]: ALC_FLR.3.1C to ALC_FLR.3.11C.
3	**CC Relationship:**	[1]: ALC_CMC.2.3C.
4	**CC Relationship:**	[1]: ALC_CMC.3.4C.
5	**CC Relationship:**	[1]: ALC_CMC.4.7C, ALC_CMC.4.8C, ALC_CMC.4.9C, ALC_CMC.5.3C, ALC_CMC.5.9C.
6	**CC Relationship:**	[1]: ALC_DVS.1.1C, ALC_DVS.2.2C.
7	**CC Relationship:**	[1]: ALC_CMC.4.5C.

The (a) Fundamental Difference …

Rqt		
8	**CC Relationship:**	[1]: ALC_FLR.1.1C, ALC_FLR.1.2C, ALC_FLR.1.3C, ALC_FLR.3.8C.
9	**CC Relationship:**	[1]: ALC_FLR.3.6C.
10	**CC Relationship:**	[1]: ATE_COV.1.1D, ATE _COV.2.2C, ATE _DPT.1.1D, ATE_FUN.1.3C, ATE_FUN.1.4C.
11	**CC Relationship:**	[1]: ATE_FUN.1.4C.
12	**CC Relationship:**	[1]: ALC_FLR.3.11C.
13	**CC Relationship:**	[1]: ALC_FLR.3.11C.

SiVenture
A division of Cisco

Next steps

- Alignment of SCs with cPPs (e.g. encrypted USB stick)
- Development of further SC to CC PP mappings
- Develop further SCs where no cPP exists (e.g. Cross Domain Solutions; UK smart metering programme)

Problems with CPA (from a Test Lab …)

- It is still a new Scheme
  - Process documents iterating, so scoping an evaluation is difficult
  - Interpretations being made, sometimes inconsistently
  - No formal method of informing Labs and/or Vendors of “interpretations”
  - Demand from end users is patchy
  - Vendors are unsure of benefits

SiVenture
A division of Cisco

CPA FAQs (just for Orlando …)

- How long has CPA been around?
  - 1906
  - Fantasia 2000
  - The Thirteenth Year

CPA FAQs (just for Orlando …)

- Other names for CPA?
  - Bedtime Stories
  - The Black Hole
  - Blank Cheque
  - Can of Worms
  - Geek Charming
  - Go Figure
  - The Greatest Game Ever Played
  - The Haunted Mansion
  - Hocus Pocus
  - The Incredible Journey
  - Magic Kingdom
- Continued …
  - Monsters Inc.
  - Monsters University
  - Never a Dull Moment
  - Now You See Him, Now You Don't
  - Read It and Weep
  - Return to Never Land
  - Shipwrecked
  - Something Wicked This Way Comes
  - You Wish!

SiVenture
A division of Cisco

CPA FAQs (just for Orlando …)

- CPA Stakeholders?
  - An Absent Minded Professor
  - Alice in Wonderland
  - The Barefoot Executive
  - Beauty and the Beast
  - Dinosaur
  - Dumbo
  - My Favourite Martian
  - Unidentified Flying Oddball
  - The Muppets
  - Sleeping Beauty

SiVenture
A division of Cisco

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