122-B

CERTIFICATION REPORT No. CRP260

Black Box Secure Analogue and Digital KVM Switches, Version 1.0,

SW2008A-USB-EAL SW4008A-USB-EAL
SW2006A-USB-EAL SW4006A-USB-EAL
SW2009A-USB-EAL SW4009A-USB-EAL

Issue 1.0

January 2011

CESG Certification Body
IACS Delivery Office, CESG
Hubble Road, Cheltenham
Gloucestershire, GL51 0EX
United Kingdom

CERTIFICATION STATEMENT

The products detailed below have been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and have met the specified Common Criteria requirements. The scope of the evaluation and the assumed usage environment are specified in the body of this report.			
Sponsor:	Black Box Corporation		
Products:	Black Box Secure Analogue and Digital KVM Switches		
Models:	SW2008A-USB-EAL, SW4008A-USB-EAL, SW2006A-USB-EAL, SW4006A-USB-EAL, SW2009A-USB-EAL and SW4009-USB-EAL.		
Description:	A range of secure KVM switches for controlling multiple computers that may be operating at different levels of classification using a common keyboard, mouse and display.		
CC Version:	Version 3.1 Release 3		
CC Part 2:	Extended	CC Part 3:	Augmented
EAL:	EAL4 augmented by ALC_FLR.2 and ATE_DPT.2		
PP Conformance:	Peripheral Sharing Switch (PSS) For Human Interface Devices Protection Profile, Version 1.2, 21 August 2008		
CLEF:	Logica		
CC Certificate:	CRP260	Date Certified:	4 January 2011

The evaluation was performed in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in UK Scheme Publication 01 [UKSP01] and 02 [UKSP02P1], [UKSP02P2]. The Scheme has established the CESG Certification Body, which is managed by CESG on behalf of Her Majesty's Government.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [ST], which prospective consumers are advised to read. To ensure that the Security Target gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 1 [CC1] and 3 [CC3], the Common Evaluation Methodology [CEM] and relevant Interpretations.

The issue of a Certification Report is a confirmation that the evaluation process has been performed properly and that no *exploitable* vulnerabilities have been found in the evaluated configuration of the TOE. It is not an endorsement of the product.

ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY

The CESG Certification Body of the UK IT Security Evaluation and Certification Scheme is a member of the above Arrangement [CCRA] and, as such, this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement.

The judgements[1] contained in the certificate and in this report are those of the Qualified Certification Body which issued them and of the Evaluation Facility which performed the evaluation. There is no implication of acceptance by other Members of the Arrangement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed by a third party upon those judgements.

MUTUAL RECOGNITION AGREEMENT OF INFORMATION TECHNOLOGY SECURITY EVALUATION CERTIFICATES

The SOGIS MRA logo which appears below confirms that the conformant certificate has been authorised by a Participant to this Agreement and it is the Participant's statement that the certificate has been issued in accordance with the terms of this Agreement.

The judgments[1] contained in the certificate and this Certification Report are those of the compliant Certification Body which issued them and of the Evaluation Facility which carried out the evaluation. Use of the logo does not imply acceptance by other Participants of liability in respect of those judgments or for loss sustained as a result of reliance placed upon those judgments by a third party.

CCRA logo **CC logo** **SOGIS MRA logo**

[1] All judgements contained in this Certification Report, are covered by the CCRA [CCRA] and the MRA [MRA].

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria (CC) security evaluation of Black Box Secure Analogue and Digital KVM Switches (Models SW2008A-USB-EAL, SW4008A-USB-EAL, SW2006A-USB-EAL, SW4006A-USB-EAL, SW2009A-USB-EAL and SW4009A-USB-EAL) to the Sponsor, Black Box Corporation, as summarised on page 2 'Certification Statement' of this report, and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

2. Prospective consumers are advised to read this report in conjunction with the Security Target [ST], which specifies the functional, environmental and assurance requirements.

Evaluated Product and TOE Scope

3. The following Black Box Secure KVM Switch models completed evaluation to CC **EAL4** augmented by ALC_FLR.2 and ATE_DPT.2 on 4 January 2011:

SW2008A-USB-EAL, SW4008A-USB-EAL, SW2006A-USB-EAL, SW4006A-USB-EAL, SW2009A-USB-EAL and SW4009-USB-EAL

4. Hereinafter, the above models are referenced as the "Black Box Secure KVM Switches". The Developer was Adder Technology Limited.

5. The evaluated configuration of these products is described in this report as the Target of Evaluation (TOE). Details of the TOE Scope, its assumed environment and the evaluated configuration are given in Chapter III 'Evaluated Configuration' of this report.

6. An overview of the TOE and its product architecture can be found in Chapter IV 'Product Architecture' of this report. Configuration requirements are specified in Section 2 of [ST].

Protection Profile Conformance

7. The Security Target [ST] is certified as achieving conformance to the following protection profile:

- Peripheral Sharing Switch (PSS) For Human Interface Devices Protection Profile, Version 1.2, 21 August 2008 [PP].

8. The Security Target [ST] also includes objectives and Security Functional Requirements (SFRs) additional to those of [PP].

Security Claims

9. The Security Target [ST] fully specifies the TOE's Security Objectives, the Threats which these Objectives counter and the Security Functional Requirements (SFRs) that refine the

Objectives. Most of the SFRs are taken from CC Part 2 [CC2]; use of this standard facilitates comparison with other evaluated products.

10. The TOE security policies are detailed in ST [ST].

11. The environmental assumptions related to the operating environment are detailed in Chapter III (in 'Environmental Requirements') of this report.

Evaluation Conduct

12. The CESG Certification Body monitored the evaluation which was performed by the Logica Commercial Evaluation Facility (CLEF). The evaluation addressed the requirements specified in the Security Target [ST]. The results of this work, completed in December 2010, were reported in the Evaluation Technical Reports [ETR1] and [ETR2], and the Supplement [SUPP].

Conclusions and Recommendations

13. The conclusions of the CESG Certification Body are summarised on page 2 'Certification Statement' of this report.

14. Prospective consumers of the Black Box Secure KVM Switches should understand the specific scope of the certification by reading this report in conjunction with the Security Target [ST]. The TOE should be used in accordance with the environmental assumptions specified in the Security Target. Prospective consumers are advised to check that the SFRs and the evaluated configuration match their identified requirements, and to give due consideration to the recommendations and caveats of this report.

15. The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration. Chapter II 'TOE Security Guidance' of this report includes a number of recommendations regarding the secure receipt, installation, configuration and operation of the TOE.

16. In addition, the Evaluators' comments and recommendations are as follows:

    a) Users of the TOE should ensure that the shared keyboard, mouse and smartcard (if applicable) are connected *directly* to the TOE on installation. A check that this remains the case should be performed periodically throughout the operational life of the TOE especially during times of heightened security risk.

    b) Users of the TOE should ensure that the keyboard and mouse are not being used when switching from one channel to another.

    c) A prospective user of the TOE should ensure that the following objectives are satisfied by the environment in which the TOE is to be used:

        (i) The operational environment procedures must ensure that all users are duly authorized and possess the necessary privileges to access the information

transferred via the TOE. This should be implemented physically and in terms of supporting IT infrastructure.

(ii) Operational procedures must (e.g. re staff vetting and training) ensure that, as far as is reasonably possible, the TOE is received, installed and managed in accordance with the manufacturer's directions. This should also ensure that users are not malicious or hostile.

(iii) The TOE should be installed in an environment that is physically secure.

(iv) Vulnerabilities associated with shared peripherals or switched computers, or their connection to the TOE, are a concern of the application scenario; they are outside the scope of the TOE.

Disclaimers

17. This report is only valid for the evaluated TOE. This is specified in Chapter III 'Evaluated Configuration' of this report.

18. Certification is *not* a guarantee of freedom from security vulnerabilities. There remains a small probability (smaller with higher Evaluation Assurance Levels) that exploitable vulnerabilities may be discovered after an evaluation has been completed. This report reflects the CESG Certification Body's view at the time of certification.

19. Existing and prospective consumers should check regularly for themselves whether any security vulnerabilities have been discovered since the ETR was issued and, if appropriate, should check with the Vendor to see if any patches exist for the product and whether those patches have further assurance.

20. The installation of patches for security vulnerabilities, whether or not those patches have further assurance, should improve the security of the TOE. However, note that unevaluated patching will invalidate the certification of the TOE, unless the TOE has undergone a formal re-certification or is covered under an approved Assurance Continuity process by a CCRA certificate-authorising Scheme.

21. All product or company names used in this report are for identification purposes only and may be trademarks of their respective owners.

II. TOE SECURITY GUIDANCE

Introduction

22. The following sections provide guidance that is of particular relevance to purchasers of the TOE.

Delivery

23. On receipt of the TOE, via a known and trusted courier, the consumer is recommended to check that one or more of the evaluated platforms has been supplied in accordance with the invoice that was raised, and to check that the security of the TOE has not been compromised during delivery.

Installation and Guidance Documentation

24. The Installation and Secure Configuration documentation is provided by [UG]. This also provides the User Guide and Administration Guide documentation.

III. EVALUATED CONFIGURATION

TOE Identification

25. The TOE comprised the following models of Black Box Secure KVM Switches:

SW2008A-USB-EAL, SW4008A-USB-EAL, SW2006A-USB-EAL, SW4006A-USB-EAL, SW2009A-USB-EAL and SW4009-USB-EAL.

TOE Documentation

26. The relevant guidance documentation for the evaluated configuration is identified in Chapter II (in 'Installation and Guidance Documentation') of this report.

TOE Scope

27. The TOE Scope is defined in the Security Target [ST] Section 2.4.2. The main security features are described in the Security Target [ST] Section 2.4.3 and are briefly summarised as follows:

a) Unidirectional flow of keyboard and mouse data;

b) Dedicated DDC bus and EDID memory emulation;

c) Active erasing of USB host controller circuit RAM at each channel change;

d) Unambiguous channel selection.

28. Functionality that is outside the TOE Scope is defined in [ST] paragraphs 46, 48, 49, 52 – 57, which are briefly summarised as follows:

a) No common power supply;

b) High port to port electrical isolation;

c) Low radiated emissions profile;

d) Tamper-evident seals (certain models only);

e) Active authentication verification (certain models only)

f) Active tamper detection (certain models only):

g) Dedicated smartcard reader port (certain models only):

h) Bidirectional communication of USB smartcard reader devices (certain models only)

TOE Configuration

29. The evaluated configuration of the TOE is defined in [ST] Section 2.3.

Environmental Requirements

30. The environmental assumptions for the TOE are stated in [ST] Section 4.3.

Test Configuration

31. The Developers used the following configuration for their testing:

- SW4008A-USB-EAL;
- SW4009-USB-EAL.

32. The Evaluators used the same configuration for their testing.

IV. PRODUCT ARCHITECTURE

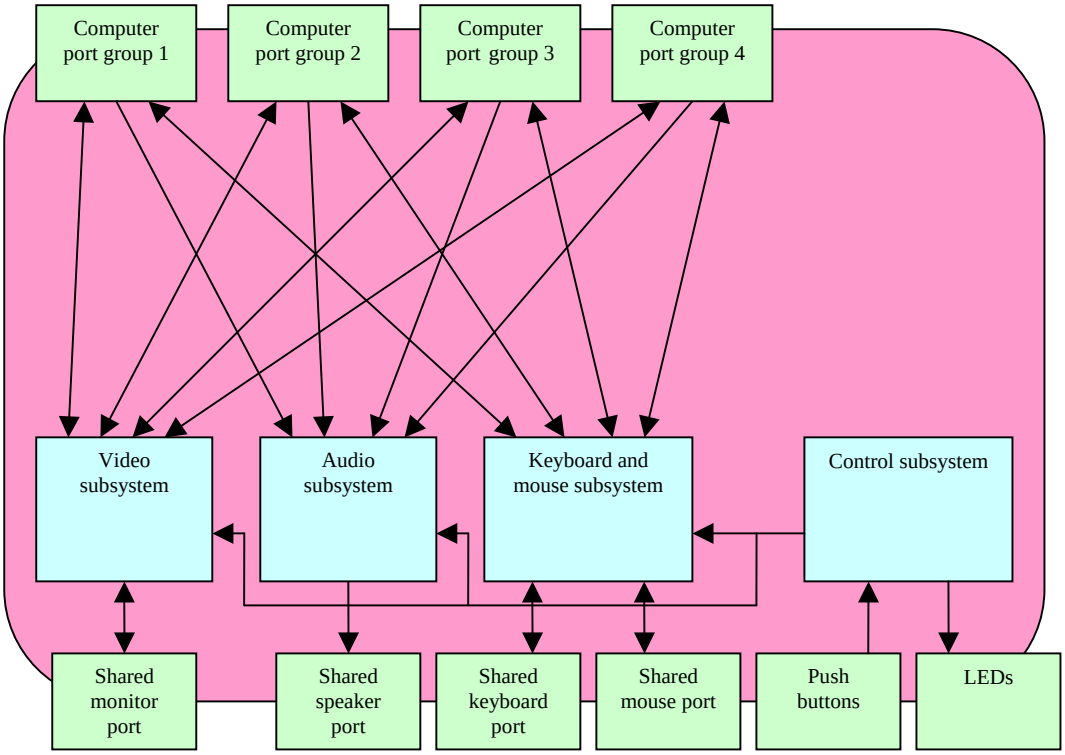
Introduction

33. This Chapter gives an overview of the main TOE architectural features. Other details of the scope of evaluation are given in Chapter III 'Evaluated Configuration' of this report.

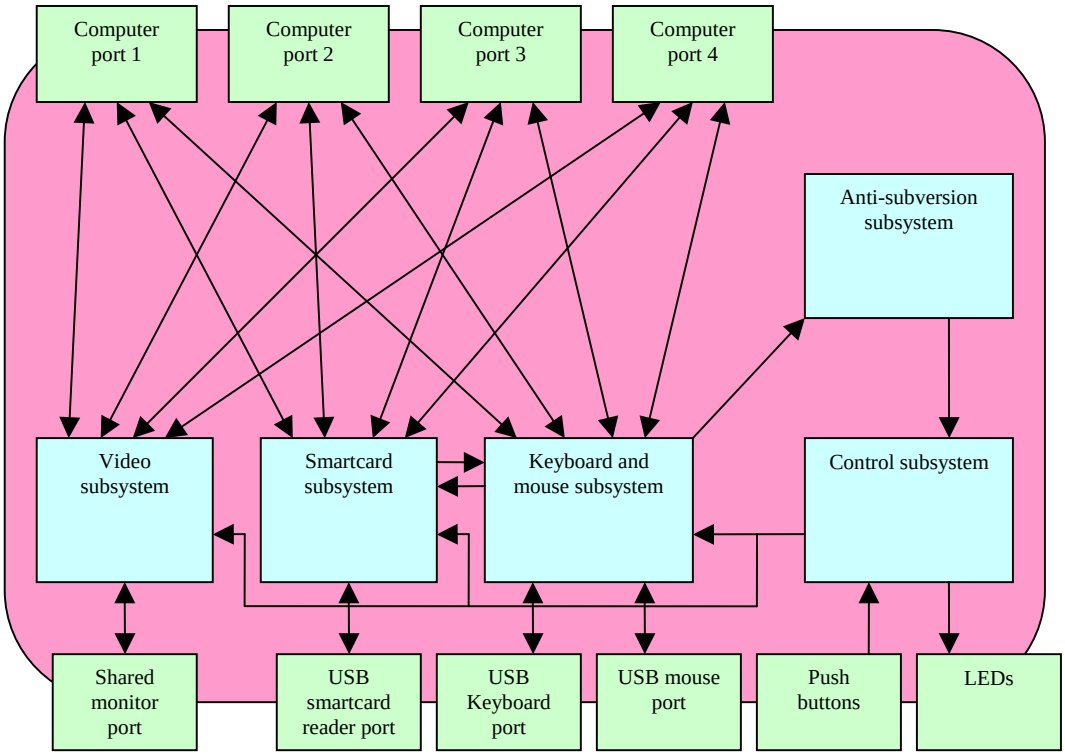
Product Description and Architecture

34. The Black Box Secure KVM Switches comprises a range of secure KVM switches for controlling multiple computers that may be operating at different levels of classification using a shared keyboard, mouse and display.

35. The diagram below shows the product architecture for the four port *digital* switch (SW4008A-USB-EAL). It depicts the switch's internal security architecture in terms of its sub-systems (each constructed from hardware/firmware sub-components and circuitry).



36. The following diagram (overleaf) shows the product architecture for the four port *analogue* switch (SW4009A-USB-EAL). This is much the same as the digital switch except that instead of an audio subsystem it offers a smartcard subsystem and additionally an anti-subversion subsystem. The features provided by the latter are outside the scope of the evaluation.



TOE Design Subsystems

37. The TOE subsystems, and their security features/functionality, are as follows:

a) Control Subsystem: this decodes any input from a channel select push button and passes appropriate channel selection control signal to the other sub-systems. It also provides feedback to the user of which channel is selected. This ensures that only one channel is selected at a time, and only the current channel is connected to the shared peripherals.

b) Keyboard and Mouse Subsystem: this enumerates keyboard and mouse on the shared USB ports. Other devices are not recognised; emulates a combined keyboard and mouse to each of the connected computer ports; routes keyboard and mouse data from the shared keyboard and mouse devices to the selected computer port; and maintains the state of the keyboard num lock, caps lock and scroll lock (NCS) per channel.

c) Video Subsystem: this routes video signals and digital synchronisation signals from the selected computer port to the shared video output port; and clones and emulates the EDID from the display device attached to the video output port to each computer port.

d) Audio Subsystem (digital device only): this routes stereo audio signals from the selected computer port to the shared audio output port.

e) Smartcard Subsystem (analogue device only): enumerates and controls the shared peripheral USB CCID class smartcard reader device; emulates a USB CCID class smartcard reader device to the selected computer port; and passes keyboard data from a combined keyboard and smartcard reader device (if connected) to the USB subsystem.

f) Anti-subversion (analogue device only): product authentication and tamper detection and response. These features are out of scope of the evaluation.

TOE Dependencies

38. The TOE has no external dependencies for security, although the TOE requires connection to at least two computers and one set of shared peripherals in operational use.

TOE Interfaces

39. The external TOE Security Functions Interface (TSFI) is described as follows:

a) One push button for each selectable channel.

b) One LED for each selectable channel. The channel with a lit LED is the active one.

c) Full speed USB host port for the shared peripherals.

d) Analogue or digital video output depending on the TOE platform.

e) Stereo audio output on the digital TOE.

f) For an analogue TOE: combined connector consisting of Low speed USB device, PS/2 keyboard, PS/2 mouse, full speed smartcard device and analogue video input. This connector is provided on a per channel basis.

g) For a digital TOE: a low-speed USB device, DVI-I digital and analogue video input and Stereo audio input. Each connection is provided on a per channel basis.

V. TOE TESTING

TOE Testing

40. The Developer's tests covered:

    a) all SFRs;

    b) all TOE high-level subsystems, as identified in Chapter IV (in 'TOE Design Subsystems') of this report;

    c) the TSFI, as identified in Chapter IV (in 'TOE Interfaces') of this report.

41. The test configuration used for developer tests is specified in Chapter III (in 'Test Configuration') of this report.

42. The Evaluators devised and ran a total of 5 independent functional tests, different from those performed by the Developer. No anomalies were found.

43. The Evaluators also devised and ran a total of 17 penetration tests to address potential vulnerabilities considered during the evaluation. No exploitable vulnerabilities or errors remained in the TOE at the end of this process.

44. The test configuration used for evaluator functional and penetration tests is specified in Chapter III (in 'Test Configuration') of this report.

45. The Evaluators finished running their penetration tests on 11th November 2010.

Vulnerability Analysis

46. The Evaluators' vulnerability analysis, which preceded penetration testing and was reported in [ETR1] and [ETR2], was based on public domain sources and the visibility of the TOE provided by the evaluation deliverables, in particular the developer's vulnerability analysis.

Platform Issues

47. The two models tested comprised digital and analogue TOE platforms at the largest capacity (4 channel compared with 2), and with smartcard connectivity (rather than without). The other TOE platforms are functional subsets of the TOE platforms tested, and therefore, the results derived are directly applicable to them.

VI. REFERENCES

[CC] Common Criteria for Information Technology Security Evaluation (comprising Parts 1, 2, 3: [CC1], [CC2], [CC3]).

[CC1] Common Criteria for Information Technology Security Evaluation, Part 1, Introduction and General Model, Common Criteria Maintenance Board, CCMB-2009-07-001, Version 3.1 R3, July 2009.

[CC2] Common Criteria for Information Technology Security Evaluation, Part 2, Security Functional Requirements, Common Criteria Maintenance Board, CCMB-2009-07-002, Version 3.1 R3, July 2009.

[CC3] Common Criteria for Information Technology Security Evaluation, Part 3, Security Assurance Requirements, Common Criteria Maintenance Board, CCMB-2009-07-003, Version 3.1 R3, July 2009.

[CCRA] Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security, Participants in the Arrangement Group, May 2000.

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Common Criteria Maintenance Board, CCMB-2009-07-004, Version 3.1 R3, July 2009.

[UG] Applicable platform user guide [UG1] or [UG2] depending on platform as follows:

[UG1] SW2006A-USB-EAL, SW4006A-USB-EAL, SW2009A-USB-EAL, SW4009A-USB-EAL

[UG2] SW2008A-USB-EAL, SW4008A-USB-EAL

[UG1] Black Box Network Services SW2006A-USB-EAL SW4006A-USB-EAL SW2009A-USB-EAL SW4009A-USB-EAL ServSwitch Secure USB, Black Box Corporation, DOC-ASP-0011v1-2, revision 1.2, December 2010

[UG2] Black Box Network Services SW2008A-USB-EAL SW4008A-USB-EAL ServSwitch Secure USB, Black Box Corporation, DOC-DSP-0007v1-2, revision 1.2, December 2010

[ETR1] Evaluation Technical Report,
Logica CLEF,
LFL/T265/ETR, 310.EC231228:5.1.1, Issue 1.0, 21 October 2009.

[ETR2] Evaluation Technical Report 2,
Logica CLEF,
LFL/T265/ETR, 310.EC231228:5.3.1, Issue 0.9, 3 December 2010.

[SUPP] Supplement to LFL/T265 [ETR2],
CB/101210(2)/LFL/T265, (final update) 22 December 2010.

[MRA] Mutual Recognition Agreement of Information Technology Security Evaluation Certificates,
Management Committee,
Senior Officials Group – Information Systems Security (SOGIS),
Version 3.0, 8 January 2010 (effective April 2010).

[PP] Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile, IAD,
Version 1.2, August 2008.

[ST] Security Target,
Black Box Corporation,
DOC-SSP-0011, Issue 1.2, November 2010.

[UKSP00] Abbreviations and References,
UK IT Security Evaluation and Certification Scheme,
UKSP 00, Issue 1.6, December 2009.

[UKSP01] Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 6.3, December 2009.

[UKSP02P1] CLEF Requirements - Startup and Operations,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part I, Issue 4.2, December 2009.

[UKSP02P2] CLEF Requirements - Conduct of an Evaluation,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part II, Issue 2.4, December 2009.

VII. ABBREVIATIONS

This list of abbreviations is specific to the TOE. It therefore excludes: general IT abbreviations (e.g. GUI, HTML, LAN, PC); standard CC abbreviations (e.g. TOE, TSF) covered in CC Part 1 [CC1]; and UK Scheme abbreviations (e.g. CESG, CLEF) covered in [UKSP00].

CCID	Chip (Smart) Card Interface Device
DVI	Digital Video Interface
DVI-I	Digital Video Interface – Integrated
EDID	Extended Display Identification Data - a data structure provided by a monitor to describe its capabilities to a graphics card (part of a computer in this context)
IAD	Information Assurance Directorate (part of the NSA)
KVM	Keyboard-Video-Mouse
LED	Light Emitting Diode
NCS	Num-lock, CAPS-lock and Scroll-lock
PS/2	Personal System/2
USB	Universal Serial Bus
VGA	Video Graphics Array