122

# CERTIFICATION REPORT No. CRP269

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

**SW2008A-USB-EAL SW4008A-USB-EAL**
**SW2006A-USB-EAL SW4006A-USB-EAL**

Issue 1.0

September 2012



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

# CERTIFICATION STATEMENT

| | | | |
|---|---|---|---|
| The product detailed below has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and has 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 | Developer: | Adder Technology Limited |
| Product and Version: | Black Box Secure Analogue and Digital KVM Switches Version 1.0 | | |
| Models: | SW2008A-USB-EAL, SW4008A-USB-EAL, SW2006A-USB-EAL, SW4006A-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, video monitor and mouse (and also, for the SWn008A models, a shared loudspeaker). | | |
| CC Version: | Version 3.1 Release 3 | | |
| CC Part 2: | Extended | CC Part 3: | Augmented |
| EAL: | EAL2 augmented by ALC_FLR.2 | | |
| PP Conformance: | Peripheral Sharing Switch (PSS) For Human Interface Devices Protection Profile, IAD, Version 2.1, 7 September 2010 | | |
| CLEF: | Logica (N.B. Logica is now part of CGI) | | |
| CC Certificate: | P269 | Date Certified: | 25 September 2012 |

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 Parts 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 the product identified below (and on Page 2 'Certification Statement'). It is addressed to the Sponsor of the evaluation, Black Box Corporation, and it is also intended to assist prospective consumers in judging the suitability of the product's IT security features to meet their particular requirements.

2. Prospective consumers of the product should understand the specific scope of the certification by reading this report in conjunction with the Security Target [ST], which specifies the functional, environmental and assurance requirements that the product was evaluated against.

## Evaluated Product and TOE Scope

3. The following Black Box Secure KVM Switch models completed evaluation to CC **EAL2** augmented by ALC_FLR.2, on 30 August 2012:

- **SW2008A-USB-EAL, SW4008A-USB-EAL, SW2006A-USB-EAL, and SW4006A-USB-EAL.**

4. Hereinafter, the above models are collectively referred to as the 'Black Box Secure KVM Switches' or 'the set of TOEs'. A statement in this report about the 'TOE' (Target of Evaluation) or 'the product' applies to each of the above models (unless stated otherwise). The Developer of the TOE is Adder Technology Limited.

5. The TOE enables a user to interact with multiple computers (that may be operating at different levels of classification) using a shared keyboard, video monitor and mouse (and also, for the SWn008A models, a shared loudspeaker). Further details are given in Chapter IV 'Product Architecture' of this report.

6. Details of the TOE Scope, and the TOE's assumed environment and evaluated configuration, are given in Chapter III 'Evaluated Configuration' of this report. Configuration requirements are specified in Section 2 of [ST].

## Protection Profile Conformance

7. The Security Target [ST] is certified as achieving demonstrable conformance to the following Protection Profile:

- Peripheral Sharing Switch (PSS) For Human Interface Devices Protection Profile, IAD, Version 2.1, 7 September 2010 [PP].

## Security Target

8. 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. The other SFRs are from [PP], see [ST] Section 6.

9. The TOE security policies are detailed in [ST]; they do not include any organisational security policies (OSPs).

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

## Evaluation Conduct

11. The set of TOEs had previously been certified by the UK IT Security Evaluation and Certification Scheme to the CC EAL4 (augmented by ALC_FLR.2 and ATE_DPT.2) assurance level, see [CR]. The set of TOEs, the security environment, and most of the supporting evaluation deliverables were unchanged from what was reported on in [CR]; what had changed was the Security Target [ST], which conforms to [PP] rather than to [PPv1.2]. For the evaluation of the set of TOEs that is the subject of this report, the Evaluator re-used the previous evaluation results where appropriate.

12. The CESG Certification Body monitored the evaluation, which was performed by the Logica[2] Commercial Evaluation Facility (CLEF). The evaluation addressed the requirements specified in the Security Target [ST]. The results of this work, completed in August 2012, were reported in the Evaluation Technical Report [ETR] and the Supplement [SUPP].

## Evaluated Configuration

13. The TOE should be used in accordance with the environmental assumptions specified in the Security Target [ST]. 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.

14. The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration (see Chapter II 'TOE Security Guidance' of this report).

## Conclusions

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

[2] Logica is now part of CGI.

**Recommendations**

16. Chapter II 'TOE Security Guidance' of this report includes a number of recommendations regarding the secure delivery, receipt, installation, configuration and operation of the TOE.

17. In addition, the Evaluator's comments and recommendations are as follows:

- Users of the TOE should ensure that the shared keyboard and mouse 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;

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

- The Developer should ensure that the labels attached to all instances of the TOE manufactured in the future include the TOE's version number (as well as the switch model and unique serial number).

**Disclaimers**

18. This Certification Report and associated Certificate applies only to the specific version of the product in its evaluated configuration. This is specified in Chapter III 'Evaluated Configuration' of this report. The ETR on which this Certification Report is based relates only to the specific items tested.

19. 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.

20. Existing and prospective consumers should check regularly for themselves whether any security vulnerabilities have been discovered since the date of the penetration tests (as detailed in Chapter V Section 'Evaluator Testing') and, if appropriate, should check with the Vendor to see if any patches exist for the product and whether those patches have further assurance.

21. The installation of patches for security vulnerabilities, whether or not those patches have further assurance, should improve the security of the TOE but should only be applied in accordance with a consumer's risk management policy. 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.

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

23. Note that the opinions and interpretations stated in this report under 'Recommendations' and 'TOE Security Guidance' are based on the experience of the Certification Body in performing similar work under the Scheme.

# II. TOE SECURITY GUIDANCE

## Introduction

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

## Delivery and Installation

25. It is recommended that, upon receipt of the TOE, the purchaser should check that the evaluated version has been supplied, and that the TOE's serial number corresponds with the details on both the packing slip (which will accompany the TOE) and the relevant invoice (which will be delivered separately from the TOE/packing slip).

26. Specific advice on how to install the TOE is given in the Section 'Installation' of Black Box Secure User Guide [UG]. In particular, the consumer should not use the unit if the TOE's tamper-evident seals are damaged, or if there are any other signs of damage to the TOE.

## Guidance Documentation

27. The User and Administration Guidance documentation is provided by [UG], which includes (on Page 2) the following security-specific recommendations:

- 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:

  (a) 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.

  (b) Operational procedures (e.g. regarding staff vetting and training) must 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.

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

- Additionally, the security office in the organisation purchasing the TOE should be aware that the TOE is not responsible for security vulnerabilities in computers, IT components or peripherals outside its physical boundary. The security of other system components connected to the TOE will require separate management to ensure IT security best practice.

# III. EVALUATED CONFIGURATION

## TOE Identification

28. The set of TOEs consists of the following Black Box Secure KVM Switch models:

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

## TOE Documentation

29. The relevant guidance documentation for the evaluated configuration is identified in Chapter II Section 'Guidance Documentation' of this report.

## TOE Scope

30. 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:

- Unidirectional flow of keyboard and mouse data;
- Dedicated DDC (Display Data Channel) bus and EDID (Extended Display Identification Data) memory emulation;
- Active erasing of USB host controller circuit RAM at each channel change;
- Unambiguous channel selection;
- Dedicated keyboard and mouse peripheral ports;
- Non-upgradeable firmware.

31. Other security-related features of the TOE are defined in [ST] Section 2.4.4; such features have not necessarily been examined during the evaluation to the same extent as the main security features (provided it is not essential to do so in order to satisfy the functional and assurance requirements specified in [ST] Section 7).

## TOE Configuration

32. The evaluated configuration of the TOE is defined in [ST] Section 2.3. Once the TOE has been installed, as described in the Section 'Installation' of [UG], no specific configuration is necessary before the TOE can be used securely.

## Environmental Requirements

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

34. The TOE is entirely self-contained (apart from requiring an external power supply), i.e. it does not require a particular IT environment in which to operate. (Note that for the SWn006A models some non-standard cables - supplied with the switch - are needed in order to attach computers to the switch.)

**Test Configurations**

35. The Developer and the Evaluator both tested the SW4008A-USB-EAL and the SW4006A-USB-EAL models with a variety of computers and shared peripherals. (These two models are sufficiently representative of the set of TOEs, as explained in [ST] Section 2.4.1.)

# IV. PRODUCT ARCHITECTURE

## Introduction

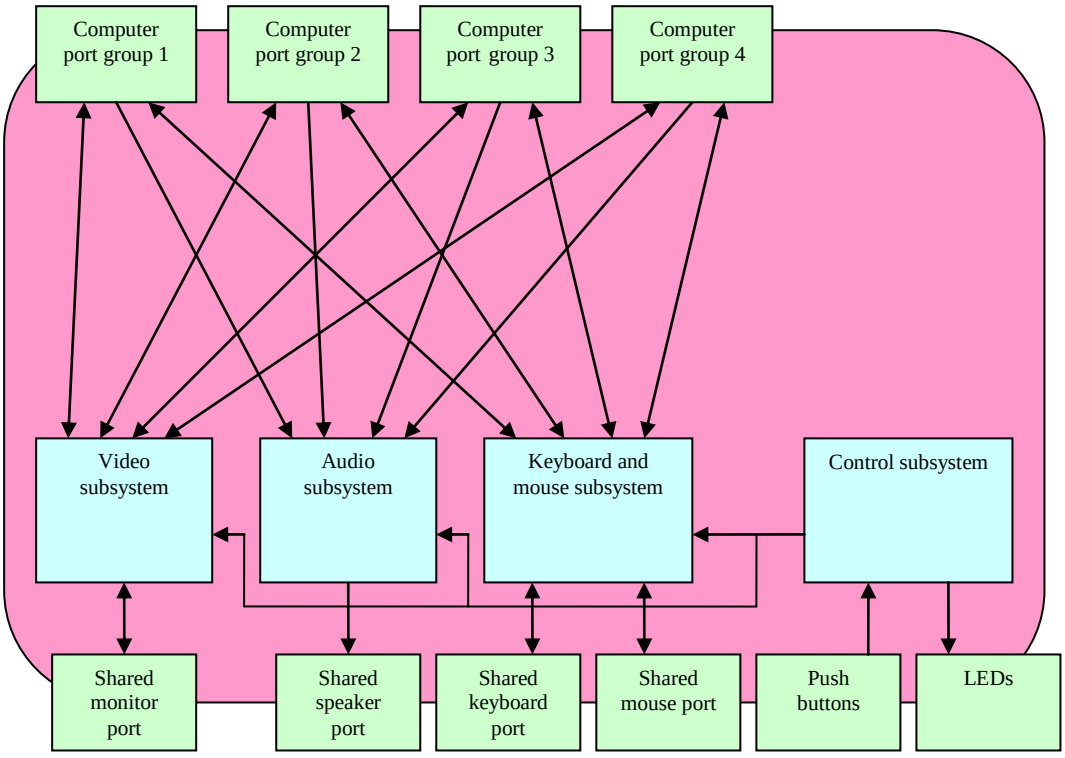
36. This Chapter gives an overview of the TOE's main architectural features. Other details of the scope of evaluation are given in Chapter III 'Evaluated Configuration' of this report.

## Product Description and Architecture

37. The TOE enables a user to interact with multiple computers (that may be operating at different levels of classification) using a shared keyboard, video monitor and mouse (and also, for the SWn008A models, a shared loudspeaker).

38. The SWn008A models handle dual link DVI-I (Digital Video Interface - Integrated) video traffic, i.e. both digital and analogue traffic; the SWn006A models handle analogue video traffic only. The SWn008A models also handle computer audio output signals, i.e. they are actually KVMA (Keyboard-Video-Mouse-Audio) switches to which loudspeaker(s) may be attached; the SWn006A models are not KVMA switches.

39. The diagram below shows the product architecture for the four port *digital* model (SW4008-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).



40. The architecture for the four port *analogue* model (SW4006-USB-EAL) is similar to the four port *digital* model (SW4008-USB-EAL) except that the audio subsystem and shared speaker port are not present.

**TOE Design Subsystems**

41. The high-level 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 an appropriate channel selection control signal to the other subsystems. It also provides feedback (via a LED) to the user of the selected channel. 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 and configures keyboard and mouse devices attached to the shared USB ports (other types of USB device, once recognised, are un-configured and prevented from functioning). The subsystem also 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 switches only): This routes stereo audio signals from the selected computer port to the shared audio output port.

**TOE Dependencies**

42. The TOE has no external security-related dependencies.

**TOE Interfaces**

43. The external TOE Security Functionality Interface (TSFI) is described as follows:

- One push button for each selectable channel.
- One LED (each of a different colour) per selectable channel. The LED that is lit indicates the currently selected channel.
- Full speed USB host ports, one for the shared keyboard and one for the shared mouse.
- Analogue (for SWn006A models) or DVI-I (for SWn008A models) video output for the shared video monitor.

- Stereo audio output port (on SWn008A models).

- On SWn006A models: a combined connector (‘computer port group’ in the diagram above) for each selectable channel; this connector effectively provides a low-speed USB device port (which emulates a combined keyboard and mouse device to the attached computer), a PS/2 keyboard port and a PS/2 mouse port (which respectively emulate a PS/2 keyboard and a PS/2 mouse to the attached computer), and an analogue video input port.

- On SWn008A models: the following three ports (‘computer port group’ in the diagram above) for each selectable channel: a low-speed USB device port (which emulates a combined keyboard and mouse device to the attached computer), a DVI-I video input port, and a stereo audio input port.

# V. TOE TESTING

**Developer Testing**

44. The Developer's security tests covered:

- all SFRs;
- all TOE high-level subsystems, as identified in Chapter IV Section 'TOE Design Subsystems' of this report;
- the TSFI, as identified in Chapter IV Section 'TOE Interfaces' of this report.

45. The configuration used for the Developer's security tests is specified in Chapter III Section 'Test Configurations' of this report.

**Evaluator Testing**

46. The Evaluator devised and ran a total of five independent security functional tests, different from those performed by the Developer. The Evaluator also witnessed a repeat run of approximately 15% of the Developer's security tests. No anomalies were found.

47. The Evaluator also repeated approximately 25% of the security penetration tests referenced in [CR]; he did not identify anything during the evaluation that suggested any additional penetration tests.

48. The configuration used for the Evaluator's independent functional and penetration tests is specified in Chapter III Section 'Test Configurations' of this report.

49. The Evaluator completed his functional and penetration testing on 22 August 2012. He concluded that, within the constraints of [ST], in the TOE, there are no errors, and no exploitable or identified residual vulnerabilities.

**Vulnerability Analysis**

50. The Evaluator's vulnerability analysis, which preceded penetration testing and is reported in [ETR], was based on public domain sources and the visibility of the TOE provided by the evaluation deliverables. It also re-used the results of the vulnerability analysis referenced in [CR].

# 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 Components, 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 Components, 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.

[CR] Common Criteria Certification Report No. CRP260, Black Box Secure Analogue and Digital KVM Switches, Version 1.0, UK IT Security Evaluation and Certification Scheme, Issue 1.0, January 2011.

[ETR] Evaluation Technical Report, Re-evaluation of Adder Secure KVM Switches[3], Logica CLEF, LFL/T265R/ETR, Issue 1.0, 30 August 2012.

[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).


[3] This ETR also covers the Black Box Secure KVM Switches.

[PP] Peripheral Sharing Switch (PSS) for Human Interface Devices
Protection Profile, IAD,
Version 2.1, 7 September 2010.

[PPv1.2] Peripheral Sharing Switch (PSS) for Human Interface Devices
Protection Profile, IAD,
Version 1.2, 21 August 2008.

[ST] Security Target, Secure Analogue and Digital KVM Switches,
Adder Technology Limited,
Version 1.1, 17 September 2012.

[SUPP] Supplement to LFL/T265R [ETR],
CB/120903/LFL/T265R, Version 1.0 (Final CB Update), 18 September 2012.

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

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

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

[UG1] Black Box Network Services ServSwitch Secure USB SW2006A-USB-EAL SW4006A-USB-EAL SW2009A-USB-EAL SW4009A-USB-EAL,
Black Box Corporation,
rev 1.2 (DOC-ASP-110v1-2, December 2010).

[UG2] Black Box Network Services ServSwitch Secure USB SW2008A-USB-EAL SW4008A-USB-EAL,
Black Box Corporation
rev 1.2 (DOC-DSP-0007v1-2, December 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 4.3, October 2010.

[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 Common Criteria abbreviations (e.g. TOE, TSF) covered in CC Part 1 [CC1]; and UK Scheme abbreviations and acronyms (e.g. CLEF, CR) covered in [UKSP00].

| | |
|---|---|
| DVI-I | Digital Video Interface – Integrated |
| DDC | Display Data Channel |
| 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) |
| KVMA | Keyboard-Video-Mouse-Audio |
| NCS | Num-lock, CAPS-lock and Scroll-lock |

*This page is intentionally blank.*