National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Dell 5535dn Multi-Function Printer

Report Number: CCEVS-VR-VID10476-2012
Dated: 18 May 2012
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Mike Allen (Lead Validator)
Jerome F. Myers (Senior Validator)
Aerospace Corporation
Columbia, Maryland

Michelle Brinkmeyer
Darren King
National Security Agency
Fort Meade, Maryland

Common Criteria Testing Laboratory

COACT CAFÉ Laboratory
Columbia, Maryland 21046-2587

Table of Contents

List of Figures

List of Tables

1 Executive Summary

This report is intended to assist the end-user of this product and any security certification Agent for that end-user in determining the suitability of this Information Technology (IT) product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Clarification of Scope in Section 4 and the Validator Comments in Section 10.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Dell 5535dn Multi-Function Printer. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This Validation Report applies only to the specific version and configuration of the product as evaluated and documented in the Security Target.

The evaluation of the Dell 5535dn Multi-Function Printer was performed by the CAFÉ Laboratory of COACT Incorporated, the Common Criteria Testing Laboratory, in Columbia, Maryland USA and was completed in April 2012.

The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR) and associated test report. The ST was written by Common Criteria Consulting LLC for Lexmark International, Inc. The ETR and test report used in developing this validation report were written by COACT. The evaluation was performed to conform to the requirements of the Common Criteria for Information Technology Security Evaluation, Version 3.1 R2, dated September 2007 at Evaluation Assurance Level 2 (EAL 2) augmented with ALC_FLR.2 and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 3.1 R2, dated September 2007. The product, when configured as specified in the installation guides, user guides, and Security Target satisfies all of the security functional requirements stated in the Dell 5535dn Multi-Function Printer Security Target. The evaluation team determined the product to be both Part 2 extended and Part 3 augmented compliant, and meets the assurance requirements of EAL 2 augmented by ALC_FLR.2. All security functional requirements are derived from Part 2 of the Common Criteria. The TOE is conformant to the U.S. Government Protection Profile for Hardcopy Devices (IEEE Std. 2600.2™-2009), dated February 26, 2010, version 1.0, including the augmentations specified by Attachment A of *CCEVS Policy Letter #20* dated 15 November 2010.

The printer that makes up the TOE is a multi-functional printer system with scanning, fax, and networked capabilities. The capabilities extend to walk-up scanning and copying, scanning to fax, scanning to email, and servicing print jobs through the network. This MFP features an integrated touch-sensitive operator panel.

The major security features of the TOE are:

1. All Users are identified and authenticated as well as authorized before being granted permission to perform any restricted TOE functions.
2. Administrators authorize Users to use the functions of the TOE.
3. User Document Data are protected from unauthorized disclosure or alteration.
4. User Function Data are protected from unauthorized alteration.
5. TSF Data, of which unauthorized disclosure threatens operational security, are protected from unauthorized disclosure.
6. TSF Data, of which unauthorized alteration threatens operational security, are protected from unauthorized alteration.
7. Document processing and security-relevant system events are recorded in an audit log, and such records are protected from disclosure or alteration by anyone except for authorized personnel.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation conduct security evaluations.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology (IT) products, desiring a security evaluation, contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- The Protection Profile to which the product is conformant (if any); and
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	Dell 5535dn Multi-Function Printer
Protection Profiles	U.S. Government Protection Profile for Hardcopy Devices (IEEE Std. 2600.2™-2009), dated February 26, 2010, version 1.0, including the augmentations specified by Attachment A of CCEVS Policy Letter #20 dated 15 November 2010, also 2600.2-PP, Protection Profile for Hardcopy Devices, Operational Environment B," "2600.2-PRT, SFR Package for Hardcopy Device Print Functions, Operational Environment B, also 2600.2-SCN, SFR Package for Hardcopy Device Scan Functions, Operational Environment B, also 2600.2-CPY, SFR Package for Hardcopy Device Copy Functions, Operational Environment B, also 2600.2-FAX, SFR Package for Hardcopy Device Fax Functions, Operational Environment B, also 2600.2-SMI, SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment B
Security Target	*Dell 5535dn Multi-Function Printer Security Target*, Version 1.6, April 3, 2012
Dates of evaluation	August 2009 through April 2012
Evaluation Technical Report	*Dell 5535dn Evaluation Technical Report*, Document No. F2-0312-005, May 16, 2012

Conformance Result	Part 2 extended and EAL2 Part 3 augmented with ALC_FLR.2
Common Criteria version	Common Criteria for Information Technology Security Evaluation Version 3.1R2, September 2007 and all applicable NIAP and International Interpretations effective on August 20, 2009
Common Evaluation Methodology (CEM) version	CEM version 3.1R2 dated September 2007and all applicable NIAP and International Interpretations effective on August 20, 2009
Sponsor	Dell Inc., 501 Dell Way, Round Rock, TX 78682
Developer	Lexmark International, Inc., 740 New Circle Road, Lexington, KY 40550
Common Criteria Testing Lab	COACT Inc. CAFÉ Labs, Columbia, MD
Evaluators	Greg Beaver, Dave Cornwell, Rory Saunders, Jonathan Alexander and Brian Pleffner
Validation Team	Dr. Jerome Myers and Mike Allen of the Aerospace Corporation, Michelle Brinkmeyer and Darren King of the National Security Agency

2.1 Applicable Interpretations

The following NIAP and International Interpretations were determined to be applicable when the evaluation started.

NIAP Interpretations

None

International Interpretations

None

3 Security Policy

The security requirements enforced by the Dell 5535dn Multi-Function Printer were designed based on the following overarching security policies:

3.1 Audit

The TOE generates audit event records for security-relevant events. A severity level is associated with each type of auditable event; only events at or below the severity level configured by an administrator are generated. The time field is supplied by the TOE if internal time is configured by an administrator or by an NTP server if external time is configured. As audit event records are generated, they are forwarded to a remote syslog IT system configured by an administrator.

3.2 Identification and Authentication

Users are required to successfully complete the I&A process before they are permitted to access any restricted functionality. The set of restricted functionality is under the control of the administrators, with the exception of submission of network print jobs which is also allowed.

The I&A process is controlled by security templates that are associated with functions and menus. Each security template specifies two building blocks – one for authentication and the second for authorization. The security template also includes a list of groups that are authorized to perform the function or access the menu with which the security template is associated. When I&A is necessary, the TOE examines the authentication building block in the security template to determine what authentication mechanism should be used. The general purpose mechanisms supported in the evaluated configuration are PKI authentication, Internal Accounts and LDAP+GSSAPI.

In the case of failed authentications, an error message is displayed on the touch panel, and then the display returns to the previous screen for further user action. An audit record for the failed authentication attempt is generated.

If authentication is successful, the TOE binds the username, password, account name, email address, group memberships (for Internal Accounts only) and name of the building block used for authentication to the user session for future use (only the username and group memberships are security attributes). An audit record for the successful authentication is generated. The user session is considered to be active until the user explicitly logs off, removes the identification card or the administrator-configured inactivity timer for actions on the Home screen of the touch panel expires. If the inactivity timer expires, an audit record is generated.

If a user locks the touch panel, the user session is terminated immediately. Similarly, after a user unlocks the touch panel, the user session is terminated immediately.

3.3 Access Control

Access control authenticates the user access request against the authorizations configured by administrators for specific functions. On a per-item basis, authorization may be configured as "disabled" (no access), "no security" (open to all users), or restricted (via security templates).

Authorization is restricted by associating a security template with an item. The security template assigned to each item may be the same or different as the security template(s) assigned to other items. Each security template points to an authentication building block as well as an authorization building block; the two building blocks may be the same or different.

The following summarizes the access controls and configuration parameters used by the TOE to control user access to the MFP functions provided by the TOE:

A) Printing – Submission of print jobs from users on the network is always permitted. Jobs that do not contain a PJL SET USERNAME statement are discarded. Submitted jobs are always held on the TOE until released or deleted by a user authorized for the appropriate access control and whose userid matches the username specified when the job was submitted.

B) Scanning - may be performed as part of a fax or email function. Only authorized users may perform scans. Scanning for fax is allowed if the Enable Fax Scans configuration parameter is "On" and the user is authorized for the Fax Function access control. Scanning for email is allowed if the user is authorized for the E-mail Function access control.

C) Copying - allowed if the user is authorized for the Copy Function access control. A user may view or delete their own copy jobs queued for printing.

D) Incoming faxes - allowed if the "Enable Fax Receive" (for analog fax mode) or "Enable Fax Receive" (for fax server mode) configuration parameter is "On". Incoming faxes are always held in the queue (until released) in the evaluated configuration. Only users authorized for the Release Held Faxes access control may release or delete the faxes.

3.4 Management

The TOE provides the ability for authorized administrators to manage TSF data from remote IT systems via a browser session or locally via the touch panel. Authorization is granular, enabling different administrators to be granted access to different TSF data. When an administrator modifies TSF data, an audit record is generated.

The security reset jumper provides an alternate mechanism to manage some TSF data. The TOE contains a hardware jumper that can be used to:

- erase all security templates, building blocks, and access controls that a user has defined (i.e. the factory default configuration); OR
- force the value of each function access control to "No Security" (all security templates and building blocks are preserved but not applied to any function).

3.5 Fax Separation

The Fax Separation security function ensures that the information on the TOE, and the information on the network to which the TOE is attached, is not exposed through the phone line that provides connectivity for the fax function. This function ensures that only printable documents are accepted via incoming fax connections, and that the only thing transmitted over an outgoing fax connection (in the evaluated configuration) is a document that was scanned for faxing.

3.6 D.Doc Wiping

The TOE overwrites RAM with a fixed pattern upon deallocation of any buffer used to hold user data.

3.7 Secure Communications

IPSec with ESP is required for all network datagram exchanges with remote IT systems. IPSec provides confidentiality, integrity and authentication of the endpoints. Supported encryption options for ESP are TDES, AES and DES. Both SHA-1 and MD5 are supported for HMACs. ISAKMP and IKE are used to establish the Security Association (SA) and session keys for the IPSec exchanges. Diffie-Hellman is used for key agreement, using Oakley Groups 1, 2, 5 or 14. During the ISAKMP exchange, the TOE requires the remote IT system to provide a certificate and the RSA signature for it is validated. If an incoming IP datagram does not use IPSec with ESP, the datagram is discarded.

3.8 Self Test

During initial start-up, the TOE performs self tests on the hardware. The integrity of the security templates and building blocks is verified by ensuring that all the security templates specified in access control exist and that all building blocks referenced by security templates exist. If any problems are detected with the hardware, an appropriate error message is posted on the touch screen and operation is suspended. If a problem is detected with the integrity of the security templates or building blocks, the data is reset to the factory default, an audit log record is generated, an appropriate error message is posted on the touch screen, and further operation is suspended. In this case, a system restart will result in the system being operational with the factory default settings for the data.

4 Assumptions and Clarification of Scope

The assumptions, threats and policies in the following paragraphs were considered during the evaluation of the Dell 5535dn Multi-Function Printer.

4.1 Assumptions

Table 2: Assumptions

Assumption	Definition
A.ACCESS.MANAGED	The TOE is located in a restricted or monitored environment that provides protection from unmanaged access to the physical components and data interfaces of the TOE.
A.ADMIN.TRAINING	Administrators are aware of the security policies and procedures of their organization, are trained and competent to follow the manufacturer's guidance and documentation, and correctly configure and operate the TOE in accordance with those policies and procedures.
A.ADMIN.TRUST	Administrators do not use their privileged access rights for malicious purposes.
A.USER.TRAINING	TOE Users are aware of the security policies and procedures of their organization, and are trained and competent to follow those policies and procedures.

4.2 Threats

The threats identified in the following section are addressed by the TOE and/or Operating Environment. The following threats are addressed by the TOE and IT environment.

Table 3: Threats

Threat	Definition
T.CONF.ALT	TSF Confidential Data may be altered by unauthorized persons
T.CONF.DIS	TSF Confidential Data may be disclosed to unauthorized persons
T.DOC.ALT	User Document Data may be altered by unauthorized persons
T.DOC.DIS	User Document Data may be disclosed to unauthorized persons
T.FUNC.ALT	User Function Data may be altered by unauthorized persons
T.PROT.ALT	TSF Protected Data may be altered by unauthorized persons

4.3 Organizational Security Policies

This section describes the Organizational Security Policies (OSPs) that apply to the TOE.

Table 4: Organizational Security Policies

Name	Definition
P.AUDIT.LOGGING	To preserve operational accountability and security, records that provide an audit trail of TOE use and security-relevant events will be created, maintained, and protected from unauthorized disclosure or alteration, and will be reviewed by authorized personnel
P.INTERFACE.MANAGEMENT	To prevent unauthorized use of the input-output interfaces of the TOE, operation of the interfaces will be controlled by the TOE and its operational environment.
P.SOFTWARE.VERIFICATION	To detect unintentional malfunction of the TSF, procedures will exist to self-verify TSF data
P.USER.AUTHORIZATION	To preserve operational accountability and security, Users will be authorized to use the TOE only as permitted by the TOE Owner

4.4 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation and how the TOE needs to be configured to ensure it operates in the evaluated configuration.

Note that the following configuration options apply to the evaluated configuration of the TOE:

1. The TOE includes the single Ethernet interface that is part of the standard configuration of every printer. No optional network interfaces are installed.
2. No optional parallel or serial interfaces are installed. These are for legacy connections to specific IT systems only.
3. All USB ports on the printer that perform document processing functions are disabled. In the operational environments in which the Common Criteria evaluated configuration is of interest, the users typically require that all USB ports are disabled. If PKI authentication is used, the card reader is physically connected to a specific USB port during TOE installation; in the evaluated configuration this USB port is limited in functionality to acting as the interface to the card reader. If a card reader is installed, the PKI authentication functionality is the only I&A mechanism that can be used.

4. All management functions are performed via the touch screen panel and the HTTP(S) server (for remote management) is disabled. This is done to align the TOE with the P2600 protection profile. In addition, this mechanism is preferred over remote management capability because it requires physical access to the TOE, is more resistant to brute force password attacks, and precludes network-based attacks on the management functions.
5. Access controls are configured for all TSF data so that only authorized administrators are permitted to manage those parameters.
6. All network communication is required to use IPSec with ESP to protect the confidentiality and integrity of the information exchanged, including management sessions that exchange D.CONF and D.PROT. Certificates presented by remote IT systems are validated.
7. Support for AppleTalk, NetWare (IPX) and LexLink are disabled since it does not provide confidentiality and integrity protection.
8. I&A may use Internal Accounts and/or LDAP+GSSAPI on a per-user basis. The Backup Password mechanism may be enabled at the discretion of the administrators. If PKI authentication is used for touch panel users, no other I&A mechanisms are included in the evaluation because they provide significantly lower strength than the supported mechanisms.
9. LDAP+GSSAPI and PKI authentication require integration with an external LDAP server such as Active Directory. This communication uses default certificates; the LDAP server must provide a valid certificate to the TOE. Binds to LDAP servers for LDAP+GSSAPI use device credentials (not anonymous bind) so that the information retrieved from Active Directory can be restricted to a specific MFP. Binds to LDAP servers for PKI authentication use user credentials from the card (not anonymous bind) so that the information retrieved from Active Directory can be restricted to a specific user.
10. Internal Accounts require User ID and password (rather than just User ID).
11. The Enable Audit parameter must be set to "Yes".
12. Audit event records are transmitted to a remote IT system as they are generated using the syslog protocol.
13. User data sent by the MFP in email messages is sent as an attachment (not as a web link).
14. No Java applications are loaded into the MFP by Administrators. These applications are referred to as LES applications in end user documentation. The following LES applications are installed by Lexmark before the TOE is shipped: "PKI Authentication", "PKI Held Jobs", and "CAC Smartcard Authentication Token".
15. No option card for downloadable emulators is installed in the TOE.
16. Some form of credential (device or user) is required to authenticate to the SMTP server.
17. Fax forwarding is disabled to limit the destinations for incoming faxes to the local printer only.
18. NPAP, PJL and Postscript have the ability to modify system settings. The capabilities specific to modifying system settings via these protocols are disabled.
19. All administrators must be authorized for all document processing functions (print, copy, scan, fax).
20. All network print jobs are held until released via the touch panel. Every network print job must include a PJL SET USERNAME statement to identify the userid of the owner of the print job. Held print jobs may only be released by an authenticated user with the

same userid as specified in the print job.

21. All incoming fax jobs are held until released via the touch panel. Held print jobs may only be released by an authenticated user with the U.ADMINISTRATOR role.
22. Administrators are directed (through operational guidance) to specify passwords adhering to the following composition rules for Internal Accounts and the Backup Password:
    a. A minimum of 8 characters
    b. At least one lower case letter, one upper case letter, and one non-alphabetic character
    c. No dictionary words or permutations of the user name
23. All unnecessary network ports are disabled.

5 Architectural Information

The following identifies the minimum hardware and software requirements for components provided by the IT Environment:

The TOE is a complete MFP, including the firmware and hardware. To be fully operational, any combination of the following items may be connected to the TOE:

A) A LAN for network connectivity. The TOE supports IPv4 and IPv6.
B) A telephone line for fax capability.
C) IT systems that submit print jobs to the MFP via the network using standard print protocols.
D) IT systems that send and/or receive faxes via the telephone line.
E) An IT system acting as the remote syslog recipient of audit event records sent from the TOE.
F) LDAP server to support Identification and Authentication (I&A). This component is optional depending on the type(s) of I&A mechanisms used.
G) Card reader and cards to support PKI authentication using Common Access Card (CAC) or Personal Identity Verification (PIV) cards. This component is optional depending on the type(s) of I&A mechanisms used. The supported card readers are:
    1) Omnikey 5121 SmartCard Reader,
    2) Omnikey 5321 SmartCard Reader,
    3) Omnikey 5125 SmartCard Reader,
    4) Omnikey 3121 SmartCard Reader,
    5) Any other Omnikey SmartCard Readers that share the same USB Vendor IDs and Product IDs with the above readers (example Omnikey 3021),
    6) SCM SCR 331.

The Target of Evaluation (TOE) is described using the standard Common Criteria terminology of Users, Objects, Operations, and Interfaces. Two additional terms are introduced:

1. "Channel" describes both data interfaces and hardcopy document input/output mechanisms, and
2. "TOE Owner" is a person or organizational entity responsible for protecting TOE assets and establishing related security policies.

Users are entities that are external to the TOE and which interact with the TOE. There may be two types of Users: Normal and Administrative.

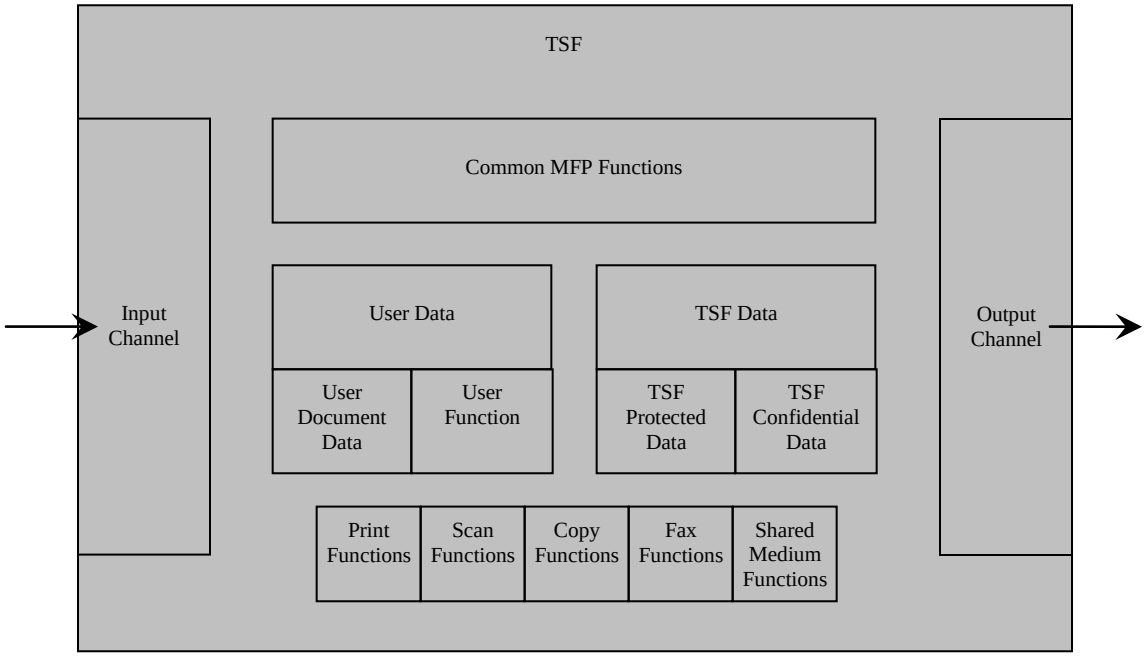
Objects are passive entities in the TOE, that contain or receive information, and upon which Subjects perform Operations. Objects are equivalent to TOE Assets. There are three categories of Objects: User Data, TSF Data, and Functions.

1. User Data are data created by and for Users and do not affect the operation of the TOE

Security Functionality (TSF). This type of data is composed of two types of objects: User Document Data, and User Function Data.

2. TSF Data are data created by and for the TOE and that might affect the operation of the TOE. This type of data is composed of two types of objects: TSF Protected Data and TSF Confidential Data.
3. Functions perform processing, storage, and transmission of data that may be present in the TOE. These functions are described below
    a. Printing: a function in which electronic document input is converted to physical document output
    b. Scanning: a function in which physical document input is converted to electronic document output
    c. Copying: a function in which physical document input is duplicated to physical document output
    d. Faxing: a function in which physical document input is converted to a telephone-based document facsimile (fax) transmission, and a function in which a telephone-based document facsimile (fax) reception is converted to physical document output
    e. Shared-medium interface: a function that transmits or receives User Data or TSF Data over a communications medium which is or can be shared by other users, such as wired or wireless network media and most radio-frequency wireless media

Figure 1: TOE Model



6 Documentation

The TOE is delivered as hardware with pre-installed software. Different part numbers are used to distinguish between Dell products, including instances of the TOE (in the CC evaluated form) and the corresponding printer model in its standard commercial form. The warehouse is not involved in any configuration or packaging of the TOE, and therefore treats it as a completely separate product with its own inventory.

Each shipment includes a documentation CD as well as a hard-copy version of the Common Criteria Installation Supplement and Administrator Guide. Masters for these items are supplied to the fulfillment centers after they have been approved for release. They are reproduced as needed by the fulfillment center to satisfy orders. All documentation provided with the product was evaluated as part of the evaluation.

The following documentation is delivered with the TOE:

5535dn MFP

1) Common Criteria Installation Supplement and Administrator Guide (Hard Copy)
2) Monochrome Laser MFP User's Guide (Soft Copy)
3) Quick Reference Guide (Soft Copy)
4) Networking Guide (Soft Copy)
5) Dell Printers Product Information Guide P/N 3055270 (Hardcopy)

Items #1 and #2 were evaluated as part of the Common Criteria evaluation.

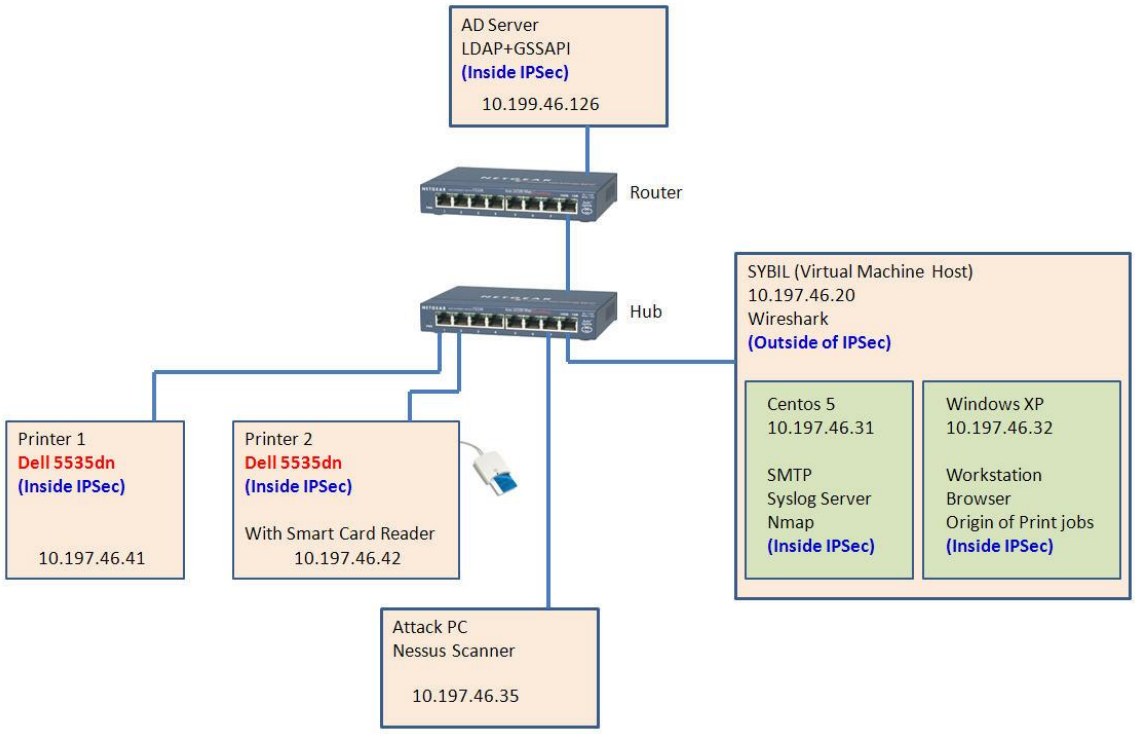
7 IT Product Testing

Testing was completed on December 14, 2011 at the COACT CCTL in Columbia, Maryland and at Lexmark International, Inc. in Lexington, KY. COACT employees performed the tests.

7.1 Evaluator Functional Test Environment

Testing was performed on a test configuration consisting of the following test bed configuration.

Figure 2: Test Configuration/Setup



An overview of the purpose of each of these systems is provided in the following table.

Table 5: Test Configuration Overview

System	Purpose
Workstation	This system is configured to send print jobs to Printer 1 and to exchange email with the Email Server. This system is Windows XP configured in a virtual environment. IP Address = 10.197.46.32
AD Server	This system acts as the Primary Domain Controller for the network, providing Active Directory, Kerberos, GSSAPI, DNS, NTP, and PKI services. IP Address = 10.199.46.126

System	Purpose
SMTP/Syslog Server	This system provides an SMTP server capable of receiving email from Printer 1 and forwarding it to a user on Workstation, and a Syslog server capable of receiving and diaplaying Syslog messages from Printer 1 and Printer 2. This is a virtual machine running Centos 5. IP Address = 10.197.46.31
Virtual Machine Host	The virtual machine host is using SYBIL to host the Syslog Server and the Workstation Browser. Wireshark is installed on this computer which will be used to monitor the test network. This virtual machine host is outside of the IPSec configuration. IP Address = 10.197.46.20
Attack PC	A network monitor able to analyze and display the traffic between Workstation and the MFPs and to launch other penetration tests. IP Address = 10,197.46.35
Printer 1	One instance of the Dell 5535dn without a Smart Card reader. IP Address = 10.197.46.41
Printer 2	Second instance of the Dell 5535dn with a Smart Card reader. IP Address = 10.197.46.42
Phone Network	Analog telephone network providing connectivity between Printer 1 and Fax Machine. This may be the Public Switched Telephone Network (PSTN) or Private Branch Exchange (PABX) or Telephone Line Emulator (TLE).

The following tables provide more information about the systems and configuration information specific to the test procedures. The configuration information consists of user accounts, user groups, and security templates to be used for the tests. All active systems connected to IP Network are configured to use IPSec.

Table 6: Workstation Requirements

Description	Test Configuration Specific Details
Authorized Users	“user1”

Table 7: Primary Domain Controller

Minimum Requirements	
AD Users/Groups	User “test” that is a member of group “Test_Group” User “test1” that is not a member of group “Test_Group”

Minimum Requirements	
	CAC user “cac1” that is a member of group “CAC_Group” CAC user “cac2” that is not a member of group “CAC_Group” CAC user “admin” that is a member of group “Administrators”
DNS Configuration	Entries for all active systems connected to IP Network
NTP Configuration	Acting as server No authentication required

Table 8: E-mail/Syslog Server

Minimum Requirements	
Syslog Configuration	Receive via UDP
Email Configuration	No credentials required to send Email

Table 9: Printer 1 Requirements

Minimum Requirements	
Internal Account Groups	“Administrators” “Users” “Restricted”
Internal Account Users	User “admin” as a member of “Administrators” User “user1” as a member of “Users” User “user2” as a member of “Users” User “user3” as a member of “Restricted”
LDAP+GSSAPI Configuration	LDAP+GSSAPI building block named “LDAPGSSAPI” with server Primary Domain Controller
Kerberos Configuration	KDC Address: Primary Domain Controller KDC Port: Kerberos port on Primary Domain Controller Realm: Realm configured on Primary Domain Controller

Minimum Requirements	
Security Templates	"Administrators_Only" with "Internal_Accounts_Building_Block" for authentication and authorization and group "Administrators" "Authorized_Users" with "Internal_Accounts_Building_Block" for authentication and authorization and group "Users" "LDAPGSSAPI_Users" with "LDAPGSSAPI" for authentication and authorization and group "Test_Group"
User Functions Enabled	Fax, Email
Function Access Controls	E-mail: LDAPGSSAPI_Users Fax: Authorized_Users Solution 1: Authorized_Users All FACs restricted to Administrators: Administrators_Only
Fax Configuration	Enable Fax Receive: On Fax Mode: Analog
Email Configuration	Primary SMTP Gateway: Email/Syslog Server Primary SMTP Gateway Port: Port used on Primary Domain Controller SMTP Server Authentication: No authentication required User-Initiated E-mail: None
Security Audit Logging Configuration	Remote Syslog Server: Email/Syslog Server Remote Syslog Method: Normal UDP
NTP Configuration	Enable NTP: On NTP Server: Primary Domain Controller

Located below are the configuration settings for the second printer in the testing lab's test configuration. Since the vendor did not test the functionality of the CAC Card Access Control, the lab has implemented an independent test to exercise the functionality of this feature.

Table 10: Printer 2 Requirements

Minimum Requirements	
CAC Configuration	Use MFP Kerberos Setup: Set DC Validation Mode: Device Certificate Validation

Minimum Requirements	
	A Certificate Authority certificate must be installed
Kerberos Configuration	KDC Address: Primary Domain Controller KDC Port: Kerberos port on Primary Domain Controller Realm: Realm configured on Primary Domain Controller
Security Templates	"Administrators_Only" with "PKI_Auth" for authentication and authorization and group "Administrators" "CAC_Users" with "PKI_Auth" for authentication and authorization and group "CAC_Group"
User Functions Enabled	Copy
Function Access Controls	Copy: CAC_Users All other required FACs: Administrators_Only
Security Audit Logging Configuration	Remote Syslog Server: Email/Syslog Server Remote Syslog Method: Normal UDP
NTP Configuration	Enable NTP: On NTP Server: Primary Domain Controller

Table 11: Attack PC

Description	Test Configuration Specific Details
Penetration and Attack Tools	Windows XP Professional SP3 Internet Explorer (Including all updates and patches) WinZip 10 ZENMAP GUI 5.21 Nmap 5.21 SnagIt 8 WireShark 1.6.2

7.1.1 Test Assumptions

The TOE and the TOE operating environment should be managed to satisfy the assumptions presented below:

A) The TOE is located in a restricted or monitored environment that provides protection from unmanaged access to the physical components and data interfaces of the TOE.

B) Administrators are aware of the security policies and procedures of their organization, are trained and competent to follow the manufacturer's guidance and documentation, and correctly configure and operate the TOE in accordance with those policies and procedures.

C) Administrators do not use their privileged access rights for malicious purposes.

D) TOE Users are aware of the security policies and procedures of their organization, and are trained and competent to follow those policies and procedures.

The following configuration options apply to the evaluated configuration of the TOE:

A) The TOE includes the single Ethernet interface that is part of the standard configuration of every MFP model. No optional network interfaces are installed.

B) No optional parallel or serial interfaces are installed. These are for legacy connections to specific IT systems only.

C) All USB ports on the MFPs that perform document processing functions are disabled. In the operational environments in which the Common Criteria evaluated configuration is of interest, the users typically require that all USB ports are disabled. If PKI authentication is used, the card reader is physically connected to a specific USB port during TOE installation; in the evaluated configuration this USB port is limited in functionality to acting as the interface to the card reader. If a card reader is installed, the PKI authentication functionality is the only I&A mechanism that can be used.

D) All management functions are performed via the touch screen panel and the HTTP(S) server (for remote management) is disabled. This is done to align the TOE with the P2600 protection profile. In addition, this mechanism is preferred over remote management capability because it requires physical access to the TOE, is more resistant to brute force password attacks, and precludes network-based attacks on the management functions.

E) Access controls are configured for all TSF data so that only authorized administrators are permitted to manage those parameters.

F) All network communication is required to use IPSec with ESP to protect the confidentiality and integrity of the information exchanged, including management sessions that exchange D.CONF and D.PROT as well as Syslog messages. Certificates presented by remote IT systems are validated.

G) Support for AppleTalk, NetWare (IPX) and LexLink are disabled since these protocols do not provide confidentiality and integrity protection.

H) I&A may use Internal Accounts and/or LDAP+GSSAPI on a per-user basis. The Backup Password mechanism may be enabled at the discretion of the administrators. If PKI authentication is used, all I&A must use the PKI authentication mechanism. No other I&A mechanisms are included in the evaluation because they provide significantly lower strength than the supported mechanisms.

I) LDAP+GSSAPI and PKI authentication require integration with an external LDAP server such as Active Directory. This communication uses default

certificates stored in NVRAM; the LDAP server must provide a valid certificate to the TOE. Binds to LDAP servers for LDAP+GSSAPI use device credentials (not anonymous bind) so that the information retrieved from Active Directory can be restricted to a specific MFP. Binds to LDAP servers for PKI authentication use user credentials from the card (not anonymous bind) so that the information retrieved from Active Directory can be restricted to a specific user.

J) Internal Accounts require User ID and password (rather than just User ID).

K) The Enable Audit parameter must be set to Yes.

L) Audit event records are transmitted to a remote IT system as they are generated using the syslog protocol.

M) User data sent by the MFP in email messages is sent as an attachment (not as a web link).

N) No Java applications are loaded into the MFP by Administrators. These applications are referred to as LES applications in end user documentation. The following LES applications are installed by the vendor before the TOE is shipped: "PKI Authentication", "PKI Held Jobs", and "CAC Smartcard Authentication Token".

O) No option card for downloadable emulators is installed in the TOE.

P) Incoming faxes are always held until released by an authorized administrator.

Q) Some form of credentials (device or user) is required to authenticate to the SMTP server.

R) Fax forwarding is disabled to limit the destinations for incoming faxes to the local printer only.

S) NPAP, PJL and Postscript have the ability to modify system settings. The capabilities specific to modifying system settings via these protocols are disabled.

T) All administrators must be authorized for all of the document processing functions (print, copy, scan, fax).

U) All network print jobs are held until released. Every network print job must include a PJL SET USERNAME statement to identify the userid of the owner of the print job. Held print jobs may only be released by an authenticated user with the same userid as specified in the print job.

V) Administrators are directed (through operational guidance) to specify passwords adhering to the following composition rules for Internal Accounts and the Backup Password:

1) A minimum of 8 characters

2) At least one lower case letter, one upper case letter, and one non-alphabetic character

3) No dictionary words or permutations of the user name

W) All unnecessary network ports are disabled.

All other assumptions associated with each test will be identified at the beginning of each set of test procedures.

7.2 Functional Test Results

The repeated developer test suite includes all of the developer functional tests. Additionally, each of the Security Functions and developer tested TSFI are included in the CCTL test suite. Results are found in the Dell 5535dn Multi-Function Printer Test Report, May 21, 2012, Document No. F2-0312-004.

7.3 Evaluator Independent Testing

The tests chosen for independent testing allow the evaluation team to exercise the TOE in a different manner than that of the developer's testing. The intent of the independent tests is to give the evaluation team confidence that the TOE operates correctly in a wider range of conditions than would be possible purely using the developer's own efforts, given a fixed level of resource. The selected independent tests allow for a finer level of granularity of testing compared to the developer's testing, or provide additional testing of functions that were not exhaustively tested by the developer. The tests allow specific functions and functionality to be tested. The tests reflect knowledge of the TOE gained from performing other work units in the evaluation. The test environment used for the evaluation team's independent tests was identical with the test configuration used to execute the vendor tests. The Independent Test Results are also found in the Dell 5535dn Test Report.

7.4 Evaluator Penetration Tests

The evaluator examined sources of information publicly available to identify potential vulnerabilities in the TOE.

The evaluator searched the Internet for potential vulnerabilities in the TOE using the web sites listed below. The sources of the publicly available information are provided below.

A) http://osvdb.org/

B) http://secunia.com/

C) http://web.nvd.nist.gov

D) http://www.securityfocus.com/

E) http://www.us-cert.gov

F) http://securitytracker.com/

The evaluator performed the public domain vulnerability searches using the following key words.

A) Dell

B) 5535dn

C) 5535

D) Multi-Function Printer

The evaluator selected the search key words based upon the following criteria. The searches that contained the keywords “Lexmark” were selected to further refine the search directly related to the TOE.

7.5 Test Results

The end result of the functional testing activities was that all tests gave expected (correct) results.

The end result of the evaluator penetration tests did not reveal any vulnerabilities.

8 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is the Dell 5535dn Multi-Function Printer.

9 Results of the Evaluation

The evaluator devised a test plan and a set of test procedures to test the TOE's mitigation of the identified vulnerabilities by testing the product for selected identified vulnerabilities.

The results of the testing activities were that all tests gave expected (correct) results. No vulnerabilities were found to be present in the evaluated TOE. The results of the penetration testing are documented in the vendor and CCTL proprietary report, Dell 5535dn Multi-Function Printer Test Report, May 21, 2012, Document No. F2-0312-004.

The evaluation determined that the product meets the requirements for EAL 2 augmented with ALC_FLR.2. The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by COACT Inc.

10 Validator Comments/Recommendations

The validation team's observations support the evaluation team's conclusion that the Dell 5535dn Multi-Function Printer meets the security claims stated in the Security Target. The validation team also wishes to add the following clarification about the use of the product. There are several configuration parameters contained in the ST and highlighted in Section 4.4 above that must be followed to ensure the product is operated in the secure manner required of the evaluated configuration. Failure to follow these guidelines will negate the assurances provided by the evaluation.

Audit records of TOE activity are exported to an external entity. Administrators of the product must ensure that there is sufficient storage for these records. In addition, the external audit storage must be protected from unauthorized access and modification or deletion of the audit records.

The encryption mechanisms provided by the TOE are not FIPS 140-2 validated. All encryption mechanisms are vendor affirmed to operate correctly.

It is important for users of the product to understand that the toner cartridges provided by the manufacturer have a chip included on which certain printer statistical data are stored and returned to the manufacturer with the empty cartridge. The maximum storage capacity of these chips is from 2 Kbytes to 16 Kbytes depending on model. If there is a concern for unauthorized usage for these statistics, the user should consider destruction of used cartridges or alternative sources of the toner.

11 Security Target

The Security Target is identified as the Dell 5535dn Multi-Function Printer Security Target Version 1.6, April 3, 2012. The document identifies the security functional requirements (SFRs) that are levied on the TOE, which are necessary to implement the TOE security policies. Additionally, the Security Target specifies the security assurance requirements necessary for EAL 2 augmented with ALC_FLR.2.

12 Glossary

The following abbreviations and definitions are used throughout this document:

AES	Advanced Encryption Standard
AIO	All In One
BSD	Berkeley Software Distribution
CAC	Common Access Card
CC	Common Criteria
CM	Configuration Management
EAL	Evaluation Assurance Level
ESP	Encapsulating Security Payload
FTP	File Transfer Protocol
GSSAPI	Generic Security Services Application Program Interface
HTTP	HyperText Transfer Protocol
I&A	Identification & Authentication
IPSec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISO	International Standards Organization
IT	Information Technology
KDC	Key Distribution Center
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MB	MegaByte
MFD	Multi-Finction Device
MFP	Multi-Function Printer
NTP	Network Time Protocol
OSP	Organizational Security Policy
PIV	Personal Identity Verification
PJL	Printer Job Language
PKI	Public Key Infrastructure
PP	Protection Profile
RFC	Request For Comments
SASL	Simple Authentication and Security Layer
SFP	Security Function Policy
SFR	Security Functional Requirement
SMTP	Simple Mail Transport Protocol
ST	Security Target
TFTP	Trivial File Transfer Protocol
TOE	Target of Evaluation
TSF	TOE Security Function
UI	User Interface
URL	Uniform Resource Locator
USB	Universal Serial Bus

13 Bibliography

The Validation Team used the following documents to produce this Validation Report:

- Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1 R2, September 2007.
- Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements, Version 3.1 R2, September 2007.
- Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements, Version 3.1 R2, September 2007.
- Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 1, Version 3.1 R2, September 2007.
- Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 3.1 R2, September 2007.
- Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.
- Dell 5535dn Multi-Function Printer Security Target, Version 1.6, April 3, 2012.
- Dell 5535dn Multi-Function Printer Test Report, May 21, 2012, Document No. F2-0312-004.
- Dell 5535dn Evaluation Technical Report, May 16, 2012, Document No. F2-0312-005.