

SHARP®

July 2010



Sharp Security Suite

TECHNICAL QUESTIONS & ANSWERS



Table of Contents

I. Executive Summary

II. Introduction

III. Technical Questions and Answers

| | |
|------------------------------------------------------------------------------------------|---|
| A. Common Criteria (CC) Validation | 1 |
| B. Protect Network against Malicious Files (.EXE, Viruses, Worms, etc.) | 3 |
| C. Protection against Unauthorized Access to Latent Document and Image Data | 4 |
| D. Protection against Unauthorized Access to Control Panel Functions | 5 |
| E. Protection against Unauthorized Retrieval of Hardcopy Output | 6 |
| F. Protection against Interception of Sensitive Data and Documents | 6 |
| G. Protection against Misuse / Abuse of “Scan-to” Functions | 7 |
| H. Protection against Fax Threats | 8 |

IV. Appendix

| | |
|------------------------------------------------------------------------------------------------------|----|
| 1. Sharp Network and Document Security Chart | 10 |
| 2. Common Criteria – EAL3 / EAL3+ versus EAL2 | 11 |
| 3. Common Criteria Validation – TOE-What actually was included in the validated product | 13 |
| 4. National Vulnerability Database | 16 |

For more information, please visit:

www.sharpusa.com/security

I. Executive Summary

This Technical Question & Answer highlights Sharp security offerings available to businesses and government agencies that seek to effectively mitigate the threat of information loss at the MFP level. The risk of data theft or misuse in today's competitive marketplace is real - whether due to a malicious network attack, disgruntled employee or electronic eavesdropping. In response, Sharp has developed a world-class suite of security offerings designed to help safeguard your most valuable asset – information.

The Industry Leader in MFD Security

As the office equipment industry transitioned from analog to digital imaging, Sharp recognized the urgent need to address inherent vulnerabilities posed by network-connected multifunctional devices (MFDs). In doing so, Sharp led the industry with the first Common Criteria-validated security solution (Optional), and is currently a leading manufacturer with a 128/256 bit encryption and data overwrite product validated at the highest commercial level for a full line of MFP products (23ppm-110ppm).

Sharp Corporation is ISO 9000 certified, assuring that rigorous manufacturing standards are met in order to consistently deliver safe, clean and efficient products.

Furthermore, first in the industry, Sharp MFPs, comply, meet and exceed the IEEE-2600™-2008 industry Security Standard Requirements. The IEEE-2600-2008 defines security requirements (all aspects of security including, but not limited to, authentication, authorization, privacy, integrity, device management, physical security, and information security) for manufacturers, users, and others on the selection, installation, configuration, and usage of hardcopy devices (HCDs) and systems, including printers, copiers, and multifunction devices (MFDs), and the computer systems that support these devices. For more information see

<http://www.sharppusa.com/ForBusiness/DocumentSystems/MFPsPrinters/ProductFeatures/Security.aspx>

The Sharp Approach

Sharp takes a comprehensive approach to security by protecting every step in the document lifecycle, from the initial scan to final output and distribution. Fully scalable, Sharp's Security Suite enables Information Technology (IT) personnel to confidently safeguard their infrastructure and MFD installed base, without impacting network traffic or workgroup productivity. Specifically, Sharp MFDs (Segment 2 and up, including color) can be customized to meet unique requirements, help optimizing data confidentiality and integrity. For example, Sharp MFDs support...

- User and device authentication
- Data encryption
- Memory clearing and sanitization
- Access control, user authorization and restrictions
- Architecture that virtually eliminates virus vulnerabilities and provides resistance to denial of service (DoS) attacks
- Activity monitoring (compliance auditing)
- Port management and filtering



National Vulnerability Database

As of 2010, Sharp enjoys an enviable position as an MFD manufacturer with no known IT product vulnerabilities listed on the U.S. Government Web site: <http://nvd.nist.gov>. A quick search of the National Vulnerability Database (NVD) confirms that Sharp MFD products pose no security risks. (For instructions on performing a search, please see *Appendix 4*.)

II. Introduction

Every day, billions of pages of confidential information - medical records, legal documents and financial data – are produced and distributed using sophisticated digital office systems - printers, copiers, facsimile and MFDs. Many businesses and government agencies are unaware that whenever these devices are connected to a network, the risk of unauthorized access and data loss exists. Even as a stand alone device, these “intelligent” systems retain latent document images, potentially exposing sensitive information.

This means that mission-critical data and documents are vulnerable to serious security breaches, yet organizations often focus attention and resources on securing their network, PCs and servers, not peripheral input/output equipment. This leaves the back door open to anyone intent on undermining your business interests – attackers, employees and competitors alike. Whether the threat is internal or external, effective security measures can be implemented on Sharp MFDs to help close potential entry points.

Sharp’s Security Strategy

As an industry leader in document security, Sharp Electronics recommends that businesses take a multi-layer approach to securing their documents and data. This has never been more important as the proliferation of e-mail and the Internet has made the need to monitor and safeguard document workflow a top priority.

Failure to take steps to protect information assets has serious consequences, perhaps exposing an organization to liability claims, financial loss, and criminal penalties. Whether its personal or financial information, health records, top-secret government information or sensitive corporate data, it’s critical to deploy solutions that minimize the risk of targeted or opportunistic threats.

What’s more, federal mandates now require compliance with stringent laws, specifically, the Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLB), and Sarbanes-Oxley Act (SOX), to protect medical, consumer and financial records, respectively. Additionally, government agencies must comply with security-relevant policies, such as DISA’s Security Technical Implementation Guide Requirements, NSTISSP #11¹ and DoD Directive 8500.2².

Sharp’s innovative suite of security offerings* help organizations to meet these rigorous compliance requirements by strengthening every link in the workflow chain - in relation to MFDs - by protecting...

- **...the network connection:** Can you prevent MFD-related attacks (viruses and attackers)?
- **...the latent documents and image data:** Can latent temporary data be encrypted/overwritten?
- **...the hardcopy output:** Can passersby be kept from viewing documents on an output tray?
- **...the MFD control panel:** Can access to device features be restricted?
- **...the stored sensitive documents:** Can an unauthorized user intercept sensitive documents?
- **...the “scan-to” function:** Can you effectively close any security hole posed by scanning?
- **...the fax connection:** Can an external attacker use the fax modem as a network entry point?

Unless the answer to each of these questions is a definitive “yes,” you’ll benefit by reading on. You’ll find answers to common questions regarding document security and the Sharp Security Suite that mitigates the risks of conducting business in today’s digital age.

* For a complete list of standard/optional security features offered on Sharp MFDs, please refer to Appendix 1: Sharp Network and Document Security Chart.

III. Technical Questions and Answers

A. Common Criteria (CC) Validation (Optional)

In 2001, sharp became the first office technology manufacturer to receive Common Criteria validation for MFD data and information security and currently holds the highest rating in the MFD industry – EAL4 – for the Sharp Data Security Kit (DSK).

Q1. What is Common Criteria (CC) Validation?

A1. Evaluations using Common Criteria, an internationally recognized and standardized methodology developed to certify Information Assurance claims, provide a high degree of confidence that security products perform as advertised. More than twenty countries recognize these standardized evaluations, and most of the associated government agencies require CC validation.

In the United States, the program is administered by the National Security Agency (NSA) and the National Institute of Standards (NIST), under the umbrella of the Department of Homeland Security. This National Information Assurance Partnership (NIAP) recognizes international and domestic evaluations conducted in accordance with Common Criteria.

Products validated under the Common Criteria program provide customers with a high degree of confidence that they address the security issues described in the posted evaluation documents. NIAP posts the claims and evaluation reports on their Web site. Listings can be accessed by going to the NIAP Common Criteria Portal: <http://www.commoncriteriaportal.org/>

Q2. What is meant by ISO 15408?

A2. ISO 15408 (International Standard Organization 15408) refers to a set of evaluation standards for security products and systems established by the Common Criteria Project, an international alliance started in 1993. The United States, Canada, Germany, France and the United Kingdom combined separate criteria into a single set of IT security criteria. After extensive public review and trial evaluations, Common Criteria Version 2.1 was produced in August 1999. This set of criteria is simply referred to as ISO 15408.

Q3. What is the highest validation level Sharp security offerings have achieved?

A3. Sharp's Data Security Kit (AR-FR1) was the first product of its kind to successfully complete testing and receive Common Criteria validation. Further Sharp has also attained the highest validation level of any office technology manufacturer – EAL4 (AR-FR4M20), multiple EAL3/EAL3+ validations have been achieved as well for example (AR-FR12M, AR-FR22, MX-FRX1, MX-FRX2, MX-FRX3, MX-FRX5, MX-FRX6, MX-FRX7, MX-FRX8, MX-FRX9, MX-FRX10, MX-FR11, MX-FR12, MX-FR13, MX-FR14, MX-FR15), in contrast to manufacturers who have achieved a lower EAL rating, Sharp subjects its products to more rigorous evaluation. With the most extensive involvement in the Common Criteria program, Sharp has demonstrated a continued commitment to providing the highest levels of Information Assurance.

Note: Evaluations at EAL1 and EAL2 are now typically considered inadequate for U.S. Government users.

Q4. What do Evaluation Assurance Levels mean?

A4. Evaluation Assurance Levels (EAL) provide an indication of the level of confidence users can place in the security claims of a manufacturer. There are seven assurance levels - EAL1 to EAL7. EAL1 to EAL4 certification is available for security technologies that fall into the commercial off-the-shelf (COTS) category, such as copiers, printers, facsimile and MFD systems. At higher levels of evaluation (EAL3 and EAL4), more information on the product is disclosed to the government-controlled labs and the integrity of the security offering is more thoroughly evaluated.

Note: For more information on EAL, please refer to Appendix 2.

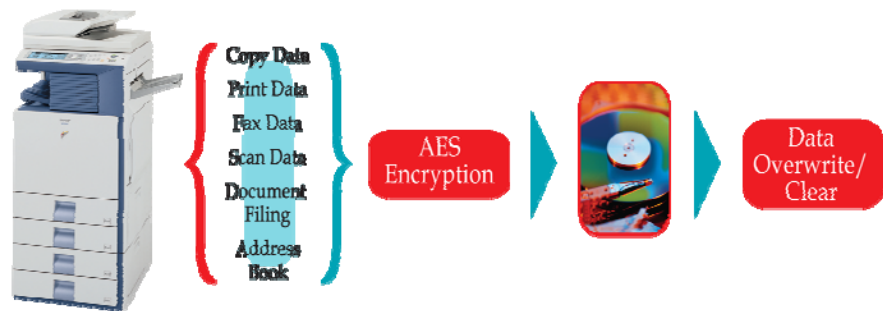
Q5. What is Sharp’s Target of Evaluation (TOE)?

A5. Sharp’s Target of Evaluation (TOE) is an MFD configured with the Data Security Kit (DSK) designed to protect document image data temporarily stored on the hard drive, or in other memory, and data processed by the MFD during copy, scan, print or fax operations. (from more information please refer to appendix 3)

Given the commercial name *Data Security Kit*, the DSK is an upgrade kit that not only adds security functions (e.g. encryption and overwrite) but also controls the major MFD systems and subsystems – print, copy, scan, fax jobs, network control, operating system, memory components (hard drive, RAM, ROM), local user interface, engine and job controller

Since Sharp has a tightly integrated firmware-based MFD architecture, the core software for the entire MFD was subject to the Common Criteria evaluation. Competitors have typically evaluated the software utilities managing their disk overwrite or a particular network, print, access, or fax feature.

Diagram 1:
One of Sharp TOE functions
“Encryption and Overwrite”



Note: For more information on Sharp’s TOE, please refer to Appendix 3. Note that TOE varies by product. For more information on Sharp’s DSK, please refer to section C: Protection against Unauthorized Access to Latent Document and Image Data.

Q6. How strong is the Sharp DSK versus competitive security offerings?

A6. Sharp has the highest EAL validation in the MFD industry - EAL4 – and potentially the broadest TOE. Some competitors are still certifying product at EAL2.

Q7. Why is Sharp’s DSK the strongest in the industry?

A7. Sharp more effectively addresses the need to secure document data left in memory. Not only does Sharp employ 256 bit encryption to scramble latent data, the DSK overwrites data stored/buffered in memory up to seven (7) times, with random sequences of 1s and 0s. This exceeds the three (3) overwrites supported by several competitors. Sharps newest validations now also include IP and MAC address filtering as well as SSL implementations, providing additional assurance for secure network connectivity.

Q8. How many Sharp DSKs are currently available?

A8. For details on Sharp security offerings, including compatible Sharp MFDs and EAL ratings, please refer to *Appendix 1: Sharp Network and Document Security Chart*.

Q9. Is there a Common Criteria Validation Web site where I can learn more?

A9. Yes. Visit <http://www.commoncriteriaportal.org/theccra.html> to obtain links to numerous sites that include products in evaluation, validated products, and much more.

B. Protect Network against Malicious Files (.EXE, Viruses, Worms, etc.)

Securing a company's computer network against virus attacks via the Internet is a significant issue in both the private and public sectors. If trouble strikes, crucial files could be lost or corrupted, productivity could be hurt and communication lines might be blocked and resources disabled (Denial of Service).

Q1. Can Sharp MFDs prevent PCs from connecting behind the firewall to transmit executable programs (malicious code) or initiate a Denial of Service attack?

A1. Sharp MFDs use unique embedded firmware* that is not based on the Windows®/Linux® operating system. Therefore, the Sharp MFD's internal systems are not subject to the same virus vulnerability as Microsoft and Linux operating systems. Sharp's unique architecture provides no user interface and cannot execute downloaded files or commands sent by an attacker to compromise the system.

**Note: This applies in most cases. The only exception is when the optional EFI™ print controller is installed.*

Q2. Are security patch downloads required on a regular basis?

A2. No. While competitors are struggling to provide security patches to protect their customers, Sharp customers are virtually immune to these threats, thus are freed from the onerous task of installing security patches.

Q3. Is it possible to use MFD credentials from one device to attack another device?

A3. Sharp MFDs support secure device authentication (see Q4) to block attackers from using MFD credentials to infiltrate other devices on the user's Intranet (corporate network). For instance, if device authentication is enabled, every e-mail address query (via an LDAP directory server) must first be authenticated, which verifies that the MFD used to send e-mail is an authorized device on the network. User authentication also requires that the user be identified, not just the MFD; the operator must log in with a valid username/password.

Q4. How does Sharp authenticate devices on the network?

A4. Sharp offers secure device authentication that utilizes Kerberos, 802.1x, Digest-MD5 (for LDAP-v3), IPSEC and SSL (Secure Socket Layer with Digital Certificate) protocols. Kerberos, Digest-MD5 and SSL are network authentication protocols that use private-/public-key cryptography to provide strong authentication for client (MFD)/server applications. Also see Q7.

Q5. What security features are supported by Sharp's Secure Network Interface?

A5. Sharp's Network Interface supports four key security features:

1. **IP address filtering:** Limits access to select IP addresses.
2. **MAC address filtering:** Limits access to specific computers, regardless of IP address.
3. **Protocol management:** Specific communication protocols can be disabled (e.g., TCP/IP (IPV4 and IPV6), NetBEUI, NetWare, EtherTalk).
4. **Port management:** Specific communication ports address can be changed individually as well as disabled (e.g., IPSEC, SSL, 802.1x, SMTP, LDAP, HTTP, FTP, LPD, IPP, Telnet, JCP, RARP, and POP3).

These security features greatly reduce vulnerability to both internal and external threats. When coupled with password protection, this means the administrator still has the convenience of remote setup while minimizing the risk of an outside attack. The combination of MAC and IP filtering controls who is able to connect to (or detect) a Sharp MFD on a network. A powerful access tool, filtering also controls which devices the MFD can communicate with, such as mail servers, file servers or computers.

Q6. Which secure network protocols do Sharp MFDs support?

A6. Sharp MFDs secure network traffic by encrypting data using IPSEC, SSL, SMB and/or SNMPv3 protocols.

Q7. Why are IPSEC and SSL protocols important?

A7. IPSEC and SSL (Secure Socket Layer) secure data communication over the network by authenticating the client (MFD) and server using private/public keys to encrypt/decrypt data. Data is rendered useless to anyone intent on intercepting communication to/from the Sharp MFD. Sharp units support importing of certificates from VeriSign®, RSA®, and others, assuring that the Sharp MFD will operate as a compatible, secure communication system on the user's network.

Q8. Why is SNMPv3 Protocol important?

A8. SNMPv3* is a secure protocol that is used to retrieve maintenance/accounting (click counts) information from the MFD. An interoperable protocol for network management, SNMPv3 provides secure access to devices using a combination of authentication and encryption. The security features provided in SNMPv3 are:

- **Message integrity:** Ensures that a packet has not been tampered with in transit.
- **Authentication:** Determines that the message is from a valid source.
- **Encryption:** Scrambles the contents of a packet to prevent it from being seen by an unauthorized source.

** Note: The previous version, SNMPv2, did not encrypt the administrator's password, and other sensitive information sent over the network, preventing many government agencies from using administrative software.*

C. Protection against Unauthorized Access to Latent Document and Image Data

Sharp raises the bar by offering multiple layers of volatile memory, as well as hard drive data security. This includes both encryption and overwrites.

Q1. What measures can be employed to protect against unauthorized access to latent data retained on the device's memory or hard drive?

A1. By installing the Sharp Data Security Kit (Optional) businesses and government agencies can significantly reduce the threat of someone gaining access to confidential documents stored on the device's hard drive or in any memory module.

Q2. What security functions are supported for the Document Filing feature?

A2. The secure document storage capability of Sharp MFDs, called Document Filing, employs various security measures to safeguard data, namely:

- **Access control:** Authentication is required before scanning.
- **Data backup:** Back up is supported using a secured Web page.
- **Confidential file:** Confidential files are password-protected.
- **Confidential folder:** Confidential folders are password-protected.
- **Encryption/Overwrite:** The Sharp Data Security Kit (Optional) automatically encrypts the stored files and encrypts and overwrites temporary data.
- **Property change:** The property of saved files can be switched between *Share*, *Protect* or *Confidential*.

Q3. How does the Sharp Data Security Kit (Optional) work?

A3. Sharp's Common Criteria validated Data Security Kit offers multiple layers of security. First, all latent image data within the MFD is encrypted (using an AES algorithm [see Q5]) before being written to the hard drive, RAM or Flash memory. When a document is printed, copied, scanned or faxed, the temporary data stored/buffered in memory is overwritten up to seven (7) times, rendering it unrecoverable. Sharp competitors typically overwrite just three (3) times. It's the combination of encryption and overwrites that sets Sharp apart.

Note: For information on specific Sharp MFDs that can be equipped with the Data Security Kit, please refer to Appendix 1.

Q4. Is data protected if the overwrite process is interrupted, for instance, a paper misfeed, power failure or operator-related issue arises?

A4. Sharp's Data Security Kit (Optional) is unique in that the latent image data is first encrypted. Therefore, the data is still protected even if the overwrite sequence is interrupted due to a service event. Most competitors do not provide encryption back up. Furthermore, when the MFD is turned on, the DSK automatically overwrites all temporary data.

Q5. How does the Sharp Data Security Kit (Optional) encrypt data and why?

A5. To secure spooled or stored data, Sharp uses Advanced Encryption Standard (AES) (128/256 bit), a widely used encryption algorithm. Encryption is a critical layer of security that is vital to protect latent image data and documents stored on the hard drive or in memory. Without encryption, network-connected MFDs (and other devices) would be still vulnerable to information loss or targeted theft. Not only are jobs in process at risk, documents stored in MFD mailboxes – for printing of frequently-used documents or secure private printing – also need to be protected.

D. Protection against Unauthorized Access to Control Panel and Scan to E-mail Functions

The prospect of an employee or others scanning a corporate client list or other sensitive information to a competitor is a threat every business faces. To mitigate this risk of information loss or unauthorized use, Sharp MFDs support a number of security features that enable businesses to restrict and monitor all device operation.

Q1. What measures can be employed on Sharp MFD systems to prevent unauthorized users from accessing control panel functions?

A1. Sharp takes a comprehensive approach to securing valuable MFD assets by providing both device access control and monitoring tools to help avoid the risk that resources are misused or abused.

Access Control:

- **User authentication:** Authentication using CAC – Common Access Card (Optional) or/and to the LDAP server or/and to Active Directory (or/and other authentication servers) identifies the sender and ensures that only authorized users (with a valid pin/username/password) can access setup, maintenance and/or MFD functions.
- **Account codes** (see Q2).
- **User/group profiles** (see Q3).
- **Password protection** (See Q4)

Device Monitoring:

- **MFD log file:** All MFD activity can be logged (To, From, When, What [file name]) to create an audit trail, ensuring compliance with privacy regulations set forth by the federal government.

Q2. What are Account Codes?

A2. Account Codes are a standard feature on all Sharp MFDs that track device usage from the control panel. The user must enter either a valid 5-digit code or user credentials, including a strong password. Each department can have their own code. A report can be generated that includes usage by Account Code.

Note: Depending on MFD model, 200 to 1000 Account Codes are available.

Q3. How do Profiles work?

A3. User and Group Profiles protect the Sharp MFD from unapproved usage and/or possible tampering by specifying functions that can be accessed. For instance, one user and/or group can be limited to copy and fax functions, locking out scan to e-mail and printing. Or to control supply costs, a profile can restrict access to color copying and/or printing.

Q4. Why is strong password protection important?

A4. Using up to 32 alphanumeric characters, including special symbols (e.g., #&*<>), Sharp's strong password protection makes the MFD highly secure. And to add another layer of protection, anyone that enters three invalid admin or document filing passwords can be locked out.

E. Protection against Unauthorized Retrieval of Hardcopy Output

Sensitive documents sitting on an MFD's output tray pose another challenge. It's not uncommon that those pages are accidentally or intentionally removed, perhaps falling into the wrong hands.

Q1. What measures can be taken on Sharp MFDs to prevent viewing or removal of document from the output tray?

A1. Confidential Print and Confidential Fax are standard Sharp features that help prevent users from accessing sensitive documents without appropriate identification. The user enters an 8-digit (MX Series) or 5-digit (AR Series) pin from the control panel before the print/fax file is released. Standard firmware also supports encrypted PDF files. Installation of the Sharp DSK encrypts all stored files.

Q2. How does the Anti-copy feature work?

A2. When this feature is enabled, the Sharp MFD will embed a nearly invisible watermark within a first-generation copy made on the MFD. If that hardcopy is subsequently copied on a Sharp MFD with DSK, the MFD will terminate the copy operation and display a warning message.

F. Protection against Interception of Sensitive Data and Documents

As mentioned previously, the Internet poses many security challenges. To reduce vulnerability to those with malicious intent, Sharp locks out the "bad guys" by securing electronic files communicated over the network. For example, tools to "sniff" passwords off the network are in common use today. Effective measures, however, can be taken to virtually eliminate this threat.

Q1. What measures can be employed on Sharp systems to protect sensitive documents en route to / from the MFD?

A1. Sharp also encrypts network traffic using IPSEC, SSL, SMB and/or SNMPv3 protocols, thus blocking any attackers trying to sniff the network traffic of companies that have implemented network encryption.

Q2. How does Sharp device authentication help protect documents on the network?

A2. Sharp offers secure device authentication protocols that assist in preventing an attacker (“man in the middle”) from tapping into data/document files, changing the content, and then redirecting the file – all while appearing to come from an “authorized” device. (Also see section B, Q4 and Q7.)

Q3. Can PDF files be encrypted?

A3. Yes. Sharp MFD users can send encrypted PDF files (scan and print) over the network. Only those recipients with the correct passcode can open the file. PDF encryption is important for healthcare companies, financial firms, education institutions and many other that must comply with stringent federal, state or local mandates.

Q4. How are print files secured when sent over the network?

A4. Print files can be encrypted using IPSEC or IPP over SSL technology, also known as IPPS. By using IPSEC and SSL technologies, the Sharp MFD establishes a secure session with the workstation, guaranteeing message privacy and integrity.

Q5. How does port management help protect documents on the network?

A5. Port management is the practice of selectively enabling/disabling ports and protocols, along with IP/MAC address filtering, it essentially provides an internal MFD firewall and insulates the MFD from TCP/IP and other port-based attacks, including internal attacks from malicious users. In short, port management, and IP/Mac filtering, assists in preventing unwanted device communication.

G. Protection against Misuse / Abuse of “Scan-to” Functions

Sharp MFDs support a variety of “scan-to” features. Users can easily scan hardcopy documents directly to e-mail addresses, a folder, a FTP site, and even a USB memory thumbdrive. Due to the potential for directing an e-mail or file to an unauthorized destination, Sharp has implemented a number of important scan-to safeguards.

Q1. How does Sharp protect against misuse/abuse of scan-to features?

A1. To effectively close any security holes posed by scan-to operations, Sharp takes the following measures:

- **Prevent anonymous “impersonated” e-mail:** Sharp prevents anonymous e-mail messaging; e-mails are sent with the sender’s information, without any way to bypass the system using “From” field spoofing techniques
- **E-mail log file:** The e-mail log files track To, From, When, What (file name), so scan-to activity can be monitored for any sign of compromise.
- **Scan to USB:** A restriction can be placed on scan-to-USB functions, preventing information leaks using this popular (and easily concealed) memory storage device.
- **Scan to FTP:** With Sharpdesk 3.21 or later version, a secure FTPS (SSL) connection can be obtained using a FTPS tunnel.
- **Scan encrypted PDF file:** Securely scan encrypted and password-protected files directly from the Sharp MFD without the need for other software/products.
- **Secure protocol support:** Select Sharp MFDs support SMB, IPSEC, LDAPS, FTPS, SMTPS, POP3S protocols for enhanced scanning security.
- **User authentication/encryption/digital signature with CAC card:** Sharp MFPs can enable the scanning function only to DoD CAC card holders that authenticate themselves. Furthermore users can select to digitally signed and/or encrypt (256 AES encryption) the scan files using DoD user certificates. (Requires CAC option)

Q2. How do you prevent “impersonated” e-mail transmission?

A2. User authentication prevents someone from entering a fictitious e-mail address. A user must enter a valid username/password (authenticate), before being granted access to scanning functions.

Q3. Can scan to e-mail/FTP/desktop/folder services be enabled/disabled?

A3. Yes. It is possible to enable/disable sending of scanned images to one or more destinations by selecting “Allowed” or “Prohibited” via the admin screen. By blocking a particular feature, you can help prevent users or groups from directing possibly sensitive files to unauthorized destinations.

Q4. Are there other ways to secure scan-to operations?

A4. Requiring that users enter login credentials (username/password) at the control panel is another way to help prevent unauthorized use of scanning functions, and provides an audit trail in the event of questionable MFD activity.

Q5. Why are log files so important?

A5. Log files track all job-related MFD activity, providing another tool that better enables businesses to comply with federal mandates regarding privacy.

H. Protection against Fax Threats

An MFD’s fax function works by converting scanned hardcopy into electronic image data, for transmission to a remote site over ordinary phone lines. With an external connection to the PSTN (Public Switched Telephone Network), IT personnel are rightfully concerned about attackers circumventing the firewall.

Q1. Is Sharp’s fax offering Common Criteria validated?

A1. Yes. Since the Sharp DSK includes firmware for fax functionality, fax security is addressed in the Common Criteria validation (at EAL3 and EAL3+).

Q2. Can the fax telephone line be used to gain access to internal systems of the Sharp MFD and, ultimately, the network?

A2. No. Sharp’s MFD architecture provides a logical separation between the fax telephone line and Local Area Network (LAN). It is, therefore, virtually impossible for attackers to gain access to the MFD’s internal systems and the network. Important points to remember include the following:

- The fax modem controller is separate from the MFD’s LAN network controller.
- The fax function is logically independent of the other MFD functions.
- The fax modem is fax-only (Class I, not data/fax, thus responds only to fax transmission protocols, prohibiting all others - including data communications).
- The fax modem controller has no mechanism to support any external code or executable file.

Sharp’s MFD architecture prevents network infiltration via a fax modem. This means common executable viruses, and other similar infectious software, cannot be used to compromise MFD security or disrupt network operations.

Q3. What is a Class I fax modem?

A3. A Class I fax modem is a modem with extensions to their command sets that allow the modem to communicate with Group 3 fax machines. A Class I modem only supports fax image communication, not data. This means that a Class I fax modem does not have the ability to pass executable files; an attacker cannot use the Sharp fax modem as a network entry point.

Q4. Can Sharp's fax modem protect against junk fax?

A4. Yes. Sharp's fax modem supports a feature called *Ignore Junk Fax* that enables the user to block junk fax from specified fax numbers, thereby eliminating the annoyance and loss of valuable resources, i.e., time and consumables.

Q5. How does the Sharp Data Security Kit help protect sensitive information received via fax?

A5. Sharp's DSK encrypts image data coming from the fax modem. After the received message is printed, the data is automatically erased. Without encryption, businesses run the risk that attackers can access sensitive documents residing in the internal memory.

Appendix

1. Sharp Network and Document Security Chart

| General | Black and White | | | | Color | | | |
|------------------------------------------------|------------------------------------|------------------------------------------------|-------------------------|---------------------------|------------------------------------------------------|-----------------------------|---------------------------------------------|---------------------------------------|
| | AR-M257/M317 Series | MX-M283/M363/M453/M503 Series | MX-M623/M753 | MX-M850/M950/M1100 Series | DCL310/DCL440/DL-C311/DL-C401/MX-C311/MX-C401 Series | MX-2600N/3100N Series | MX-4100N/4101N/MX-5001N Series ⁹ | MX-5500N/6200N/7000N/8201/7001 Series |
| Speed (PPM) | 25/31 ppm | 28/36/45/50ppm | 62/75ppm | 85/95/110ppm | 31/40 b/w / 31/40 color ppm | 26/31 b/w / 26/31 color ppm | 41/50 b/w / 41/50 color ppm | 55/62/70 b/w / 41 color ppm |
| Functions ¹ | Print/Copy/Scan/Fax | Print/Copy/Scan/Fax | Print/Copy/Scan/Fax | Print/Copy/Scan/Fax | Print/Copy/Scan/Fax | Print/Copy/Scan/Fax | Print/Copy/Scan/Fax | Print/Copy/Scan/Fax |
| Printer Controller | AR-P17/AR-P27 | Standard ² | Standard ² | MX-PB2, MX-PX4 | Standard | Standard | Standard | Standard |
| Network Interface Card | AR-P17, AR-NC5 ³ AR-P27 | Standard ² | Standard ² | Standard | Standard | Standard | Standard | Standard |
| Network Scanning Expansion Kit | MX-NSX1 | Standard ⁴ | Standard | MX-NSX1 | Standard | Standard | Standard | Standard |
| Facsimile Expansion Kit | AR-FX7 | MX-FX2 | AR-FX2 | MX-FX1 | MX-FX3 | MX-FX2 | MX-FX2 | MX-FX3 |
| Hard Disk Drive | — | Standard ⁴ | Standard | Standard | Standard | Standard | Standard | Standard |
| Security Features | | | | | | | | |
| Access Control Security | | | | | | | | |
| Account Codes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Comprehensive Embedded User Access Control | No | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| User Authentication | LDAP | LDAP | LDAP | LDAP | LDAP | LDAP | LDAP | LDAP |
| Confidential Print | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Follow You Printing™ | Optional ^{5,6} | Optional ^{5,6} | Optional ^{5,6} | Optional ^{5,6} | Optional ^{5,6} | Optional ^{5,6} | Optional ^{5,6} | Optional ^{5,6} |
| Card Access Control | Optional ⁷ | Optional ⁷ | Optional ⁷ | Optional ⁷ | Optional ⁷ | Optional ⁷ | Optional ⁷ | Optional ⁷ |
| CAC (Common Access Card) | Optional ¹³ | Optional ¹² | Optional ¹² | Optional ¹³ | Optional ¹² | Optional ¹² | Optional ¹² | Optional ¹³ |
| Fax Security | | | | | | | | |
| Confidential FAX | — | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Separation Between FAX and Network Connections | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Filter Junk Fax | — | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Data Security | | | | | | | | |
| Commercial Data Security Kit | AR-FR24U, AR-FR25U | MX-FR15U for U Series MX-FR23U for N Series | MX-FR22U | MX-FRX8U | MX-FR12U MX-FR13U MX-FR13U | MX-FR10U | MX-FR11U | MX-FRX3U MX-FRX9U |
| Common Criteria Data Security Kit | AR-FR24, AR-FR25 | MX-FR15 for U Series MX-FR14 for N Series | MX-FR22 ⁹ | MX-FRX8 | MX-FR13 MX-FR13 | MX-FR10 | MX-FR11 | MX-FRX3 MX-FRX9 |
| EAL Validation Level | EAL3+ | EAL3 | EAL3 | EAL3 | EAL3 | EAL3 | EAL3 | EAL3+ |
| Data Security Kit Features | | | | | | | | |
| Functions ¹ | Copy/Print/Scan/Fax | Copy/Print/Scan/Fax | Copy/Print/Scan/Fax | Copy/Print/Scan/Fax | Copy/Print/Scan/Fax | Copy/Print/Scan/Fax | Copy/Print/Scan/Fax | Copy/Print/Scan/Fax |
| Encrypts Image Data | Fax data only | Yes ⁸ | Yes ⁸ | Yes ⁸ | Yes ⁸ | Yes ⁸ | Yes ⁸ | Yes ⁸ |
| Hard Disk Overwrite | Not Applicable | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| RAM Overwrite | Yes | Yes ¹⁰ | — | — | — | — | — | — |
| FAX ROM Overwrite | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Resistance to (DoS) Denial of Services | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Resistance to Common Virus Attacks | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Document Control (Anti-Copy) | — | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Lock User after 3 Retries | — | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Hard Drive Overwrite Features | Not Applicable | — | — | — | — | — | — | — |
| Encryption (# of bit) | — | 256 | 256 | 128 | 256 | 256 | 256 | 128 |
| # Overwrites | — | Up to 7 | Up to 7 | Up to 7 | Up to 7 | Up to 7 | Up to 7 | Up to 7 |
| Overwrite Method | — | Random Data | Random Data | Random Data | Random Data | Random Data | Random Data | Random Data |
| Automatic Overwrite after each Job | — | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Automatic Overwrite at Start Up | — | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Manual Overwrite | — | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Document Filing | Not Applicable | — | — | — | — | — | — | — |
| Protection Method without DSK | — | Password protection | Password protection | Password protection | Password protection | Password protection | Password protection | Password protection |
| Protection Method with DSK | — | Adds encryption | Adds encryption | Adds encryption | Adds encryption | Adds encryption | Adds encryption | Adds encryption |
| Network Security | | | | | | | | |
| IP Filtering | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| MAC Address Filtering | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Port Management | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Password Protected Setup | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| IPSec, IPv6, SSL, TLS | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes ¹³ |
| 802.1x, IEEE 802.2008 ¹¹ | No | Yes | Yes | No | Yes | Yes | Yes | No |
| SHIMFY3 | No | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| SMB | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Audit Trail Security | | | | | | | | |
| Embedded Log File | No | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Equitrac Copy Audit Trail | Optional ^{5,8} | Optional ^{5,8} | Optional ^{5,8} | Optional ^{5,8} | Optional ^{5,8} | Optional ^{5,8} | Optional ^{5,8} | Optional ^{5,8} |
| Equitrac Print Audit Trail | Optional ⁵ | Optional ⁵ | Optional ⁵ | Optional ⁵ | Optional ⁵ | Optional ⁵ | Optional ⁵ | Optional ⁵ |
| Scan Audit Trail | | | | | | | | |
| Scan to E-mail | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Document Security | | | | | | | | |
| Scan Encrypted PDF file | No | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Print Encrypted PDF file | No | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

1 Some Functions Require Optional Equipment

2 Standard on N Series. MX-M283/M363/M457/M503

Requires MX-PB10, MX-M753 Requires MX-PB13

3 RJ45 Network Interface Included with the Printer Controller,

Certain Operating Systems and Protocols May Require (AR-NC5J) Option

4 Standard on N versions

5 Requires Equitrac Office® or Equitrac Express®

6 Requires Equitrac Embedded for Sharp's MFPs

(for 35ppm and up) or PageControl

7 3rd Party Applications with Sharp OSA Technology

(for MFPs 35 ppm and up)

8 RPS 197 AES Encryption

9 Available late 2010

10 For MFP without Hard Disk

11 Meets standard requirements

12 Common Access Card with MX-EC50 for N series

13 Common Access Card with DCL310S

Appendix

2. Common Criteria – EAL3+ / EAL3 versus EAL2

In 2001, sharp was the first vendor in the industry to offer common criteria EAL2 validated product (Sharp Data Security Kit AR-FR1). Nearly a half-decade ago, EAL2 appeared to be adequate for less sophisticated MFDs. Today that has changed.

EAL is an Evaluation Assurance Level, not certification. It is a measure of how confident a user can be with the vendor's advertised performance of their specific certified Target of Evaluation (TOE). Vendors are validated against the security claims they make in a Common Criteria document named the Security Target (ST). This document is posted online for all certified products, along with the Validator's Report, which provides a clear overview of exactly what a vendor has certified.

Higher security validation EAL3+/EAL3 provides higher assurance that the security solutions were implemented properly. This means that the Common Criteria validation agency will not only check the product against the vendor's claims but also check the schematics and the firmware code to ensure that the proper implementation and proper security protection methods were used. EAL2 is one of the lowest validation processes, requiring minimum checks against the vendor's claim of security.

EAL3+/EAL3 provide assurance by an analysis of the security functions, using a functional and interface specification, guidance documentation, and the high-level design of the TOE to understand the security behavior. Therefore, EAL3+/EAL3 represent a meaningful increase in assurance from EAL2 by requiring more complete testing coverage of the security functions and mechanisms and/or procedures that provide some confidence that the TOE will not be tampered with during development.³

The following are the main validation areas that are not included in EAL2 validation:

- **Configuration Management (CM).** Configuration Management (CM) is one method or means for establishing that the functional requirements and specifications are realized in the implementation of the TOE. In EAL3+/EAL3, applying Configuration Management to these additional items provides added assurance that the integrity of TOE is maintained, e.g., access control assurance requirements are added to the CM system.

At EAL2 access control is not tested, which means that unauthorized users can possibly gain access to MFD assets. In contrast, Sharp products were examined to make sure that only authorized users can access MFD assets.

Note: ISO 9000 certification has nothing directly to do with security, as suggested by some vendors. ISO 9000 is related to Quality Assurance, confirming that the company has very structured and controlled manufacturing and management practices. This is critical if secure products are to be delivered with integrity. Sharp Corporation is ISO 9000 certified.

- **Development** – In this stage, the design document was examined. At EAL3+/EAL3, the relationships between the various internal and external components are examined in more detail for relevance to security. Sharp has included all the security components for validation. The internal interaction is important to examine as a complete product. In EAL2, components are examined separately, instead of as an integrated product. As a result, some vulnerabilities may be overlooked.

- **Guidance Documents** - The guidance documents class provides the requirements for user and administrator guidance documentation. For the secure administration and use of the TOE, it is necessary to describe all relevant aspects for the secure application of the TOE. Guidance documentation includes user and administrator guidance³. In this area there is no difference between EAL2 and EAL3.
- **Life Cycle Support** – Life Cycle Support is an aspect of establishing discipline and control in the processes of refinement of the TOE during its development and maintenance. Confidence in the correspondence between the TOE security requirements and the TOE is greater if security analysis and the production of the evidence are done on a regular basis, as an integral part of the development and maintenance activities³.

Life Cycle Support is not required at EAL2. At EAL3+/EAL3, the physical security procedures of the development location and any procedures used to select development staff is being evaluated. It is important to control the development environments to make sure quality development control was in place when the TOE was developed. This is an example of where ISO 9000-certified vendors, like Sharp, have some advantage.

- **Testing** – Testing helps to establish that the TOE security functional requirements are met. Testing provides assurance that the TOE satisfies at least the TOE security functional requirements, although it cannot establish that the TOE does no more than what was specified. Testing may also be directed toward the internal structure of the TSF, such as the testing of subsystems and modules against their specifications³.

At EAL3+/EAL3, the developer is required to demonstrate that the tests that have been identified, include testing of all of the security functions, are described in the functional specification. The analysis should not only show the correspondence between tests and security functions, but should also provide sufficient information for the evaluator to determine how the functions have been exercised³.

The extra step that Sharp took with EAL3+/EAL3, and the extra validation to all the MFD components, including network and scanning, provide assurance for secure operation between subsystems. Unauthorized users cannot access assets.

- **Vulnerability Assessment** – This class addresses the existence of exploitable covert channels, the possibility of misuse or incorrect configuration of the TOE, the possibility to defeat probabilistic or permutational mechanisms, and the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE³.

At EAL3+/EAL3, the objective is to ensure that misleading, unreasonable and conflicting guidance is absent from the guidance documentation, and that secure procedures for all modes of operation have been addressed. Insecure states should be easy to detect.

Sharp's DSK has a strong admin and user security control that was examined and tested along with the other security functions. Leaving the validation at EAL2 can mean that a possibly vulnerable interface may not be tested and therefore mistakenly validated as securely implemented. Sharp security products are tested for vulnerabilities in networked environments as illustrated in *Diagram 4*. It is recommended that users check competitive vendors' products and compare the test environment.

Appendix

3. Common Criteria Validation (What actually was included in the validated product)

CC program defines the Target of Evaluation (TOE) as a set of software, firmware and/or hardware that may be an IT product, a part of an IT product, a set of IT products, a unique technology that may never be made into a product, or a combination of these.

Each vendor selects/defines this TOE in their Security Target when they apply for CC validation.

Given the commercial name *Data Security Kit*, Sharp validates the DSK as the specified TOE. The DSK included the firmware that controls the major MFD systems and subsystems - fax card, network control, operating system, memory components (hard drive, RAM, ROM), local user interface, engine and job controller.

Competitors have typically evaluated the software utilities managing their disk overwrite or a particular network, print, access, or fax feature.

In other words, the Sharp DSK consists of MFD firmware, with enhanced security features, that protects the main assets of the MFD, while also protecting user data and user credentials stored in the MFD (temporarily or permanently). No matter which access port the attacker attempts to use (fax port, network port or walk up UI), Sharp has an offering designed to help block potential attackers from penetrating and accessing MFD assets.

Typical Sharp Data Security Kit implementations are shown in *Diagram 3*. For illustration purposes, the MX-FRX2 Data Security Kit is installed within a mid-range MFD (e.g., 40-/50-ppm). The certified Data Security Kit is actually the core control software for the entire MFD dealing with all operational functions and addressing RAM, flash and hard drive memory, when hard drives are used.

Important: Many Sharp copiers are available in multifunctional configurations (print/copy/scan), both with and without a hard drive. Many government agencies prefer models without hard drive for classified document processing applications. In these models all latent data is erased when the device is turned off. Adding the optional DSK will provide encryption and overwrite for better protection

Diagram 3 shows that the Data Security Kit, in this case the MX-FRX2, is on the unit's main controller board and deals with all input/output activity associated with memory. This includes the user interface, network and local interfaces to the imaging engine and paper handling systems.

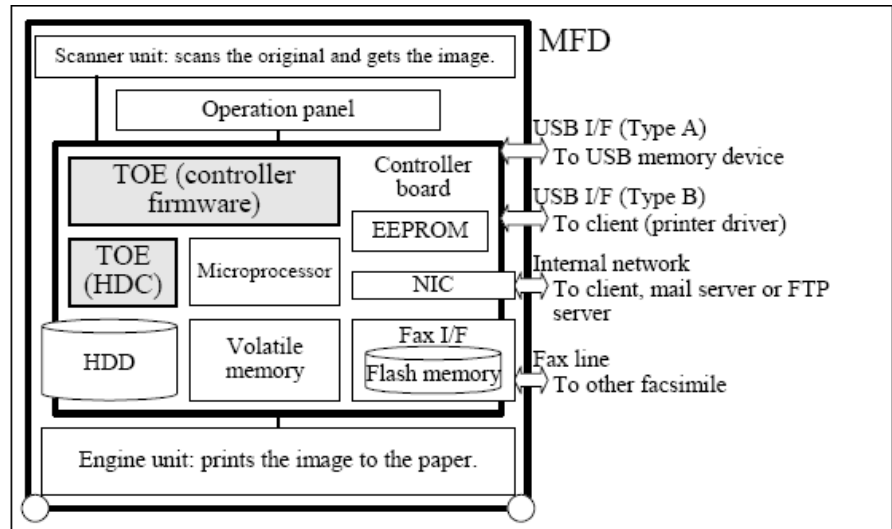


Diagram 3:
Sharp DSK
Implementation
within Mid-range
MFD.

Diagram 4 shows a usage environment for the TOE. It includes the external network, fax lines, clients and servers. This confirms the Sharp products are validated for use in real world networked environments where all MFD capabilities are deployed.

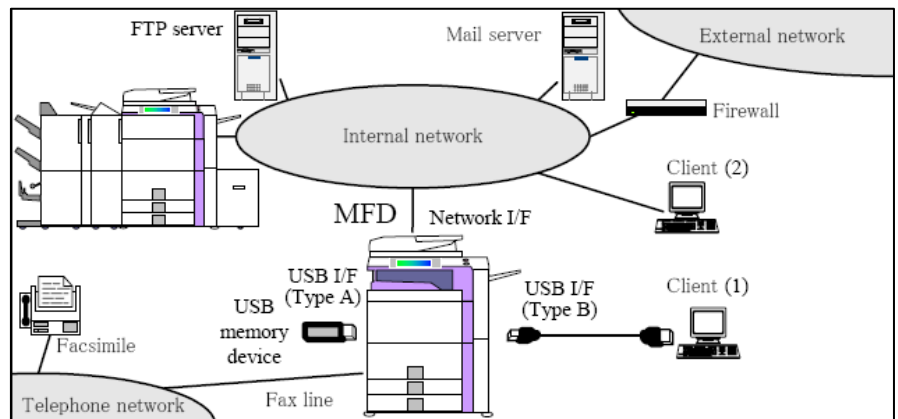


Diagram 4:
Usage Environ-ment
of the TOE

Diagram 5 provides the configuration layout of the Evaluator Independent Testing (EIT). This also confirms that Sharp’s MFD network interfaces are tested by the validation lab.

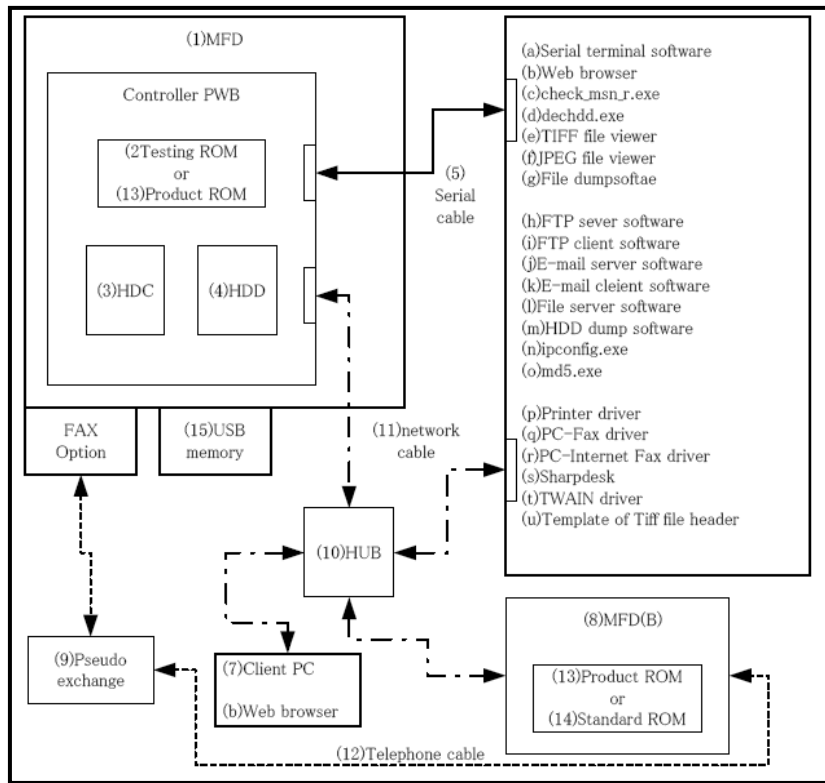


Diagram 5:
Configuration of EIT

Appendix

4. National Vulnerability Database

The National Vulnerability Database (NVD) is a comprehensive cyber-security vulnerability database that integrates all publicly available U.S. Government vulnerability resources and provides references to industry resources. No Sharp MFD products are currently listed on this site, unlike key competitors' MFDs.

To search for vulnerable products on the NVD Web site, proceed as follows:

1. Open your Web browser.
2. Enter: **http://nvd.nist.gov**.
3. Select CVE and CCE Vulnerability Database Advanced Search
4. Select Vendor, e.g., Sharp or MFD competitor name.
5. Press **Enter** (or click **Search All**). See sample screen below.
6. Perform another search or close your browser.

The screenshot shows the NVD website interface. At the top, it is sponsored by DHS National Cyber Security Division/US-CERT and NIST. The main header reads "National Vulnerability Database" with the tagline "automating vulnerability management, security measurement, and compliance checking". Below the header is a navigation menu with categories like Vulnerabilities, Checklists, Product Dictionary, Impact Metrics, Data Feeds, and Statistics. The main content area displays search results for "Search Results (Refine Search)", indicating 9 matching records. Three results are visible:

- CVE-2009-1656**: Summary: Xerox WorkCentre and WorkCentre Pro 232, 238, 245, 255, 265, 275; and WorkCentre 5632, 5638, 5645, 5655, 5665, 5675, 5687, 7655, 7656, and 7675 allows remote attackers to execute arbitrary commands via unknown attack vectors, aka "command injection vulnerability." Published: 05/16/2009. CVSS Severity: 10.0 (HIGH).
- CVE-2008-6436**: Summary: Cross-site scripting (XSS) vulnerability in the Web Server in Xerox WorkCentre 7132, 7228, 7235, and 7245 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. Published: 03/06/2009. CVSS Severity: 4.3 (MEDIUM).
- CVE-2008-5225**: Summary: Multiple cross-site scripting (XSS) vulnerabilities in Xerox DocuShare 6 and earlier allow remote attackers to inject arbitrary web script or HTML via the PATH_INFO to the default URI under (1) SearchResults/ and (2) Services/ in dsdn/dsweb/, and (3) the default URI under unspecified docushare/dsweb/ServicesLib/Group-#/ directories. Published: 11/25/2008. CVSS Severity: 4.3 (MEDIUM).

On the left side of the screenshot, there is a sidebar with "Mission and Overview" and "Resource Status" sections. The "Resource Status" section lists various data types available in the NVD, such as CVE Vulnerabilities (38615), Checklists (128), US-CERT Alerts (182), US-CERT Vuln Notes (2345), OVAL Queries (2517), and CPE Names (17819). It also notes the last update date as Tue Sep 08 11:25:23 EDT 2009 and a CVE publication rate of 17.87.

End Notes:

- ¹ *The National Information Assurance Acquisition Policy #11 is a national security policy governing the acquisition of IT products that might be used to process national security sensitive information.*
- ² *Department of Defense (DoD) Directive 8500.2 establishes policies and assigns responsibility under Section 2224 of title 10, United States Code to achieve DoD information assurance (IA) through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network centric warfare.*
- ³ *Source: Common Criteria Assurance Level Part III*

© 2010 by Sharp Electronics Corporation. All rights reserved.

Sharp is a registered trademark of Sharp Corporation. All other trademarks and registered trademarks are property of their respective owners. Sharp does not warrant or grant that any of the information contained herein pertaining to any third parties is accurate or complete. Sharp is not responsible for or does not endorse the contents of any third party linked sites.

Specifications are subject to change without notice.



SHARP ELECTRONICS CORPORATION Sharp Plaza, Mahwah, NJ 07495-1163 1-800-BE-SHARP www.sharpusa.com