



SHARP

Data Security
for Sharp MFP

Security Overview

Introduction

This document briefly outlines the scope and depth of Security offered by Sharp on the range of Digital Multiple Function Peripherals (from now referred to as MFP), which combine functionality such as copier, printer, scanner, fax, I-fax and image server.

The security measures to protect data under any or all of these functions are described in more detail through various specifications and test documentation. Many of these supporting documents are public domain since claims have been verified through the Common Criteria evaluations carried out by NIAP, and will appear as Target of evaluation documents.

However some other information's are highly confidential and not disclosed since they describe methods of achieving security that would in essence be a breach of security to disclose.

MFP Benefits and associated risks

An MFP plays an integral part of document output in the office these days, since it combines all of the essential document communications functionality commonly used – copy, print, scan, FAX, and emerging functions such as I-fax and Image server.

These functions can be provided at greatly reduced operational cost against individual function products, with higher quality and offer common scanning and finishing benefits to all of the features.

The advent of Digital copiers and printers 8-9 years ago introduced the concept of producing documents rather than copying pages (Mopier concept). In other words, a whole document could be scanned or spooled before any output is made. The benefits are to be able to make multiple copy sets from a single scan, or multiple printouts of the same document without repeated spooling, or provide advanced finishing such as collated document sets or even paginated booklets.

Unlike a traditional copier, an MFP can be shared on a network and manages vast quantities of digital data. However achieving these advanced features has a downside that image data from any of the functions – scanning, printing, copying, faxing gets stored on memory devices such as RAM, flash ROM, and often a hard disk drive.

Non Volatile memory such as flash ROM or Hard disk drive (HDD) is always at risk in that these component parts could be stolen and yet retain any residual data from earlier operation.

In addition, the very act of connecting the MFP to a network, poses risks of hacker penetration to steal data from any memory, or mount a denial of service attacks.

Objective of Sharp Data Security

The objective of Data Security is to guard against any form of non-authorized penetration of data on the MFP either during regular operation, or outside of this operation such as non-working hours or periodical service. Many of these guards come as standard, and require little training to be able to invoke.

Sharp's highest security measure known as the Data Security kit (DSK) is a low cost upgrade to the firmware, that gives a significant enhancement to the base security, with NIAP awarded Common Criteria assurance that the security measures are sound.

Sharp recognised many risks to data security and set about a program to provide secure devices for not just operation, but also for security in non-operational times such as overnight or during periodical service. This was the first generation that was applied to the AR287, AR337, AR407, AR507 devices.

However subsequent discussions with customers needing higher levels of data security assurance led to a second generation of security that is now available for the Sharp product range with many enhancements including protocol filtering and MAC address filtering on the network interface and encryption of stored data.

(Currently Sharp are developing further enhancements for the next generation products.)

Function of DSK

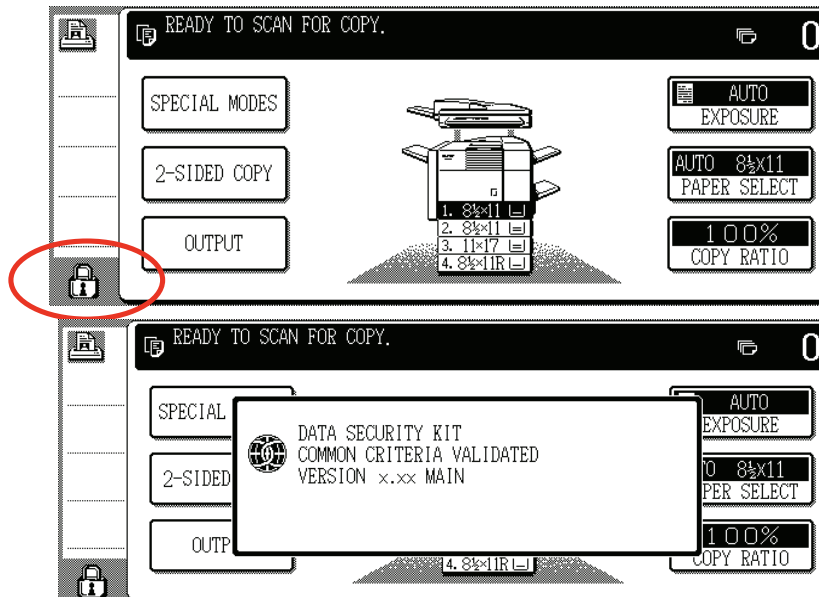
Sharp DSK has the following functions that apply to any or all data from Scan, print, copy, fax:

- Encryption of any data on HDD / RAM Memory / Flash memory
- Overwriting of data on HDD / RAM Memory / Flash memory after the operation is completed.
- Overwriting of entire HDD / RAM Memory / Flash memory on power up or when demanded.
- Setting of number of times for overwriting up to 7 times (1 time is default)
- Clear identification on LCD control panel when DSK is installed and when it operates.

Configuration of DSK

In installing DSK, you replace the standard firmware ROM embedded onto the MFP main board with DSK ROM. After replacing the ROM, the DSK function is activated by entering a product key at the LCD control panel (provided by Sharp).

When installed and activated, a security symbol is permanently displayed on the LCD operation panel. If this symbol is not displayed, the MFP is NOT secure.



The DSK includes ROM, certification sticker, user manual, and installation check sheet. The Certification sticker placed onto the MFP with the DSK installed.

Note well, the original ROM set must be sent away with the installation technician, since an MFP can be reverted to as it was before DSK installation if the DSK ROM is replaced with the initial ROM set. Be assured however that in the unlikely event that DSK is uninstalled, no data will have been left in the memories prior to the ROM switch. NIAP have confirmed this point, and provided that all operators ensure the security logo is displayed on the LCD panel prior to usage, they can be assured of secure operation.

Detailed configuration will not be made public for the following reasons:

- To prevent such operation by unauthorised persons.
- An approved Service technician always handles installation, to ensure correct operation.
- It is not necessary for Users to look at the actual configuration.

Encryption and Data erasing are operated automatically when DSK installed. It is not necessary to worry about forgetting to activate the function or intentionally de-activating the setting (Even the administrator is not able to switch off. Thus there is always an assured security level.

Encryption of data

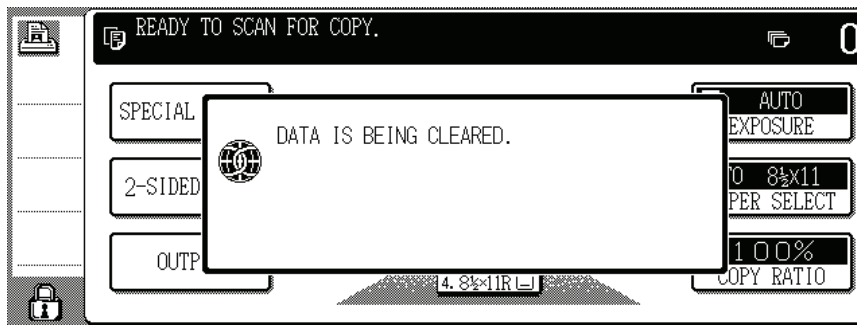
Sharp MFP stores copy / scan / print data on firstly on RAM memory, overflowing to HDD as the data volume increases (on just RAM if the HDD is not embedded), FAX data on Flash memory. The DSK encrypts data as it is being stored on these memory devices.

An Encryption key is needed for encryption. The method of encryption, and the generation and destruction of encryption Keys are closely guarded secrets of Sharp Corporation. This in itself is an additional security method.

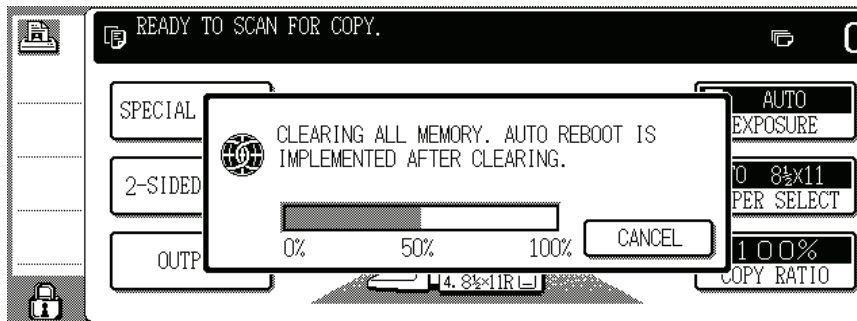
Since the DSK handles these encryption issues automatically, it is not necessary for users to worry about any configuration or necessity to prime the copier before and after usage. NIAP have confirmed the security of this operation during Common Criteria testing.

Erasing of data

The DSK erases data after job completion from all memory devices and renders it unrecoverable.

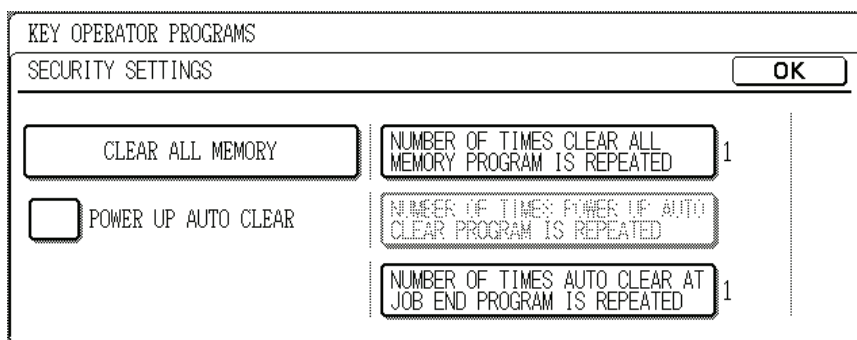


In addition to erasing after job completion (erasing the data area used for the job), the user can set; manually erasing all data area, and automatically erasing entire memory (and entire HDD) when MFP is powered on.



In reality, randomly generated data is written over HDD and RAM, and 0 is written over Flash memory. Again for security purposes the algorithm used for random data generation will not be made public.

Regarding the number of overwrites in one erase operation, 7 times can be set as a maximum for HDD, RAM (depending on models). Data 0 can be overwritten only once on Flash memory. Default setting for numbers of times overwrite is 1 time. Many organisations recommend 3 times overwrite to be sure, some organisations have suggested that 7 times is their minimum.



Print Server Card AR-NC5J security compatibility

IP address/MAC address filtering

Access filtering is controlled on a secure area of the configuration web page of the MFP device.

Access to and from MFP can be limited to designated IP addresses or address ranges. This means that in a small peer to peer network environment access is restricted to an identified workgroup.

FTP protocol is blocked by denying access by IP address.

MAC address filtering is a much tougher filter, since a MAC address is unique to a network card. MAC address filtering is recommended when a device is connected to a greater enterprise network, where IP addresses can be reconfigured to steal identity. Typically a Print server MAC address will be permitted, with a backup address for administrator. All other users will only have access through the print server. For desktop scanner usage, additional MAC addresses may be necessary.

Up to 4 IP addresses ranges can be defined, and up to 10 MAC addresses can be designated. IP address filtering can allow or deny transmission to designated IP addresses (MAC address filtering can only allow transmission).



IP Address Filter Config

Name	Value	Comment
Filter Mode	DENY <input type="button" value="v"/>	Select one
Filter #0 Start Address	<input type="text" value="0.0.0.0"/>	IP address
Filter #0 End Address	<input type="text" value="0.0.0.0"/>	IP address
Filter #1 Start Address	<input type="text" value="0.0.0.0"/>	IP address
Filter #1 End Address	<input type="text" value="0.0.0.0"/>	IP address
Filter #2 Start Address	<input type="text" value="0.0.0.0"/>	IP address
Filter #2 End Address	<input type="text" value="0.0.0.0"/>	IP address
Filter #3 Start Address	<input type="text" value="0.0.0.0"/>	IP address
Filter #3 End Address	<input type="text" value="0.0.0.0"/>	IP address

MAC Address Filter Config

Name	Value	Comment
Filter #0 Address	<input type="text" value="000000000000"/>	MAC address
Filter #1 Address	<input type="text" value="000000000000"/>	MAC address
Filter #2 Address	<input type="text" value="000000000000"/>	MAC address
Filter #3 Address	<input type="text" value="000000000000"/>	MAC address
Filter #4 Address	<input type="text" value="000000000000"/>	MAC address
Filter #5 Address	<input type="text" value="000000000000"/>	MAC address
Filter #6 Address	<input type="text" value="000000000000"/>	MAC address
Filter #7 Address	<input type="text" value="000000000000"/>	MAC address
Filter #8 Address	<input type="text" value="000000000000"/>	MAC address
Filter #9 Address	<input type="text" value="000000000000"/>	MAC address

Protocol filtering

Network connection and conformity to standards such as TCP/IP introduces many “back door” methods of communication that are not well publicised, but understood by programmers and network specialists.

The AR-NC5J network card, and compatible embedded network options of other Sharp MFPs offer the ability to block these protocols, and change default port settings for Internet access.

Reasons for filtering ports and access:

- Blocking of Telnet: Prevents administrator password from being seen as plain text.
- Blocking of RARP: Prevents malicious RARP server from assigning IP address without permission.
- Blocking of JCP: Prevents administrator password from being seen as plain text.

Name	Value
Filter	ENABLE http://172.20.3.50:129/security.htm
Telnet Remove	ENABLE
JCP Remove	ENABLE
RARP Remove	ENABLE

Submit

More recently, additional control and filtering has been added to block SNMP protocol, and to change the HTTP port access number (commonly known default is 80).

Service Control

HTTP
Port Number

SNMP
SNMP

Submit (S)

Protocol filtering is controlled on secure areas of the configuration web page of the MFP device.

*Glossary

- **FTP:** File transfer protocol – direct delivery peer to peer of data files.
- **Telnet:** Protocol used to remotely operate node in TCP/IP network such as Internet or Intranet.
- **RARP:** Protocol used to find out which IP address corresponds to a given physical address (MAC address) in TCP/IP network.
- **ARP** to find out which MAC address corresponds to a given IP address.
- **JCP:** a uniquely developed Silex protocol to locate Silex node based on MAC address and assign IP address accordingly in TCP/IP network.
- **SNMP:** Simple Network Management protocol - access protocol to the Device MIB, Tools to interrogate MIB data using SNMP are freely available on the Web.
- **MIB:** Management Information Block – Tabular data constructed during real time in a network device operational system. Information containing full network access details, device operational status, configuration location etc.

Secure Printing

All Sharp MFP devices with printing capability have a built in secure printing mode. This is more commonly referred to as Confidential print or PIN printing.

This is a very important feature, since the biggest breach of security is that sensitive documents might be left on the MFP output tray and forgotten to be collected.

To operate, the user enters a 5 digit code in the printer driver before a print job is sent (This can be defaulted to ensure that the user must always enter a code!).

The data is spooled to the MFP and held unprinted on a Hard disk drive. When the user enters the same 5 digit code on the MFP, the print job is released. The user collects the document while present at the MFP.

Of course, this re-introduces the risk that data is deliberately being kept on the Hard disk drive. But however, by installing the DSK option, any stored data is encrypted, guarding against unauthorised data recovery, then securely erased after usage.

For enhanced versions of Secure printing, 3rd party hardware products are available through Sharp to integrate Magnetic or proximity card identification with pin code entry to enable Printer and copier usage.

User Authentication

Today's MFPs incorporate highly featured scanning functions that when fully configured and enabled will permit sending of scanned data to virtually any destination worldwide through internet connection. Naturally this introduces an enormous potential for data theft.

Sharp has introduced Authentication methods on all Scan enabled MFPs ensuring that only authorised operators with validated network accounts are permitted to scan documents.

For added convenience and traceability, the operators email address is added to the "from" field of the sent document, and a blind copy can be sent to the administrator, or to an archive to keep a record of all scanned documents.

Finally a log is kept for an audit trail of document scans.

Sharp MFPs offer up to 5 different levels of Authentication method from Anonymous up to Kerberos level.

For more controlled destination management, Sharp MFPs interface directly to LDAP, so that all send destinations can be setup and maintained on a central server, denying unknown destinations from being configured on the local device.

Summary by model

Product Feature		AR-M160	AR-M236	ARM350	AR-P350	AR-M550	ARC-170M	ARC-260P
		AR-M205	AR-M276	AR-M450	AR-P450	AR-M620 AR-M700	ARC-260M	
Confidential PIN printing		-	•	•	•	•	•	•
Paper left on scanner warning		-	•	•	N/A	•	•	N/A
User Access control		•	•	•	•	•	•	•
Configuration Access control		•	•	•	•	•	•	•
Network Firewall	IP Address Firewall	•	•	•	•	•	•	•
	Mac Address Firewall	•	•	•	•	•	•	•
	Protocol and port service access control	•	•	•	•	•	•	•
LDAP address book access control		•	•	•	N/A	•	-	N/A
Sender email authentication		-	•	•	N/A	•	-	N/A
Sender email audit trail		-	•	•	N/A	•	-	N/A
internal auditor	Print	-	•	•	•	•	•	•
	Copy	•	•	•	N/A	•	•	N/A
	Fax	-	•	•	N/A	•	•	N/A
	Scan	•	•	•	N/A	•	•	N/A
Data Security Kit	Hard Disk Erase by overwrite	-	N/A	•	•	•	•	•
	All Memory erase by overwrite	-	•	•	•	•	•	•
	Number of times of overwrite	-	1	1 to 7	1	1 to 7	1	1
	AES Data Encryption on HDD	-	N/A	•	•	•	-	-
	AES Data Encryption on RAM memory	-	•	•	•	•	-	-
	AES Data Encryption on Fax Memory	-	•	•	N/A	•	-	-
External Secure print Release option	Equitrac etc.	•	•	•	•	•	•	•