TOSHIBA

Security Guide Vol.6.1

October, 2020

R13121304207-TTEC

OME150116F0

TOGETHER INFORMATION™

TABLE OF CONTENTS

Trademarks

The trademarks described in this manual are as shown below.

- Windows, and the brand names and product names of other Microsoft products are trademarks of Microsoft Corporation in the US and other countries.
- MIFARE is a trademark of NXP Semiconductors.

Other company names and precuts names in this document are the trademarks of their respective companies.

1. PREFACE

Toshiba Tec Corporation (hereafter called "Toshiba Tec") guarantees the security of your data and documents for enabling your business to meet the increased security demands of today's world. All our e-BRIDGE Next models conform with the highest security standards, preventing your data and documents from any unauthorized access without sacrificing the efficiency and performance of the systems.

Model and series names in this manual

In this manual, each model name in the sentences is replaced with the series name as shown below.

Model name	Series name
e-STUDIO550/650/810	e-STUDIO810 Series
e-STUDIO3511/4511	e-STUDIO4511 Series
e-STUDIO600/720/850	e-STUDIO850 Series
e-STUDIO281C/351C/451C	e-STUDIO451C Series
e-STUDIO232/282	e-STUDIO282 Series
e-STUDIO352/452	e-STUDIO452 Series
e-STUDIO2500C/3500C/3510C	e-STUDIO3510C Series
e-STUDIO163/165/205	e-STUDIO205 Series
e-STUDIO166/167/207	e-STUDIO207 Series
e-STUDIO2330C/2820C/2830C/3520C/4520C	e-STUDIO4520C Series
e-STUDIO5520C/6520C/6530C	e-STUDIO6530C Series
e-STUDIO255/355/455	e-STUDIO455 Series
e-STUDIO655/755/855	e-STUDIO855 Series
e-STUDIO2040C/2540C/3040C/3540C/4540C	e-STUDIO4540C Series
e-STUDIO5540C/6540C/6550C	e-STUDIO6550C Series
e-STUDIO206L/256/306/356/456/506	e-STUDIO506 Series
e-STUDIO556/656/756/856	e-STUDIO856 Series
e-STUDIO2050C/2550C	e-STUDIO5055C Series
e-STUDIO2555C/3055C/3555C/4555C/5055C	
e-STUDIO306LP	e-STUDIO306LP Series
e-STUDIO5560C/6560C/6570C	e-STUDIO6570C Series
e-STUDIO207L/257/307/357/457/507	e-STUDIO507 Series
e-STUDIO557/657/757/857	e-STUDIO857 Series
e-STUDIO2000AC/2500AC	e-STUDIO5005AC Series
e-STUDIO2505AC/3005AC/3505AC/4505AC/5005AC	
e-STUDIO2008A/2508A/3008A/3508A/4508A/5008A	e-STUDIO5008A Series
e-STUDIO5506AC/6506AC/7506AC	e-STUDIO7506AC Series
e-STUDIO5508A/6508A/7508A/8508A	e-STUDIO8508A Series
e-STUDIO3508LP/4508LP/5008LP	e-STUDIO5008LP Series

Model name	Series name
e-STUDIO2010AC/2510AC	e-STUDIO5015AC Series
e-STUDIO2515AC/3015AC/3515AC/4515AC/5015AC	
e-STUDIO2018A/2518A/3018A/3518A/4518A/5018A	e-STUDIO5018A Series
e-STUDIO5516AC/6516AC/7516AC	e-STUDIO7516AC Series
e-STUDIO5518A/6518A/7518A/8518A	e-STUDIO8518A Series
e-STUDIO330AC/400AC	e-STUDIO400AC Series

2. SECURITY FUNCTION LIST

Possible dangers	Functions	e-STUDIO5055C Series e-STUDIO6570C Series e-STUDIO507 Series e-STUDIO857 Series	e-STUDIO5005AC Series e-STUDIO5008A Series e-STUDIO7506AC Series e-STUDIO8508A Series	e-STUDIO5008LP Series	e-STUDIO5015AC Series e-STUDIO5018A Series e-STUDIO7516AC Series e-STUDIO8518A Series e-STUDIO400AC Series
Security standard	Conformance to IEEE 2600.1	Yes	Yes		
	Conformance to IEEE 2600.2			Yes	
	Conformance to HCD PP				Yes
	FIPS 140-2 compliant HDD, JCMVP compliant HDD	Option * Standard for the North America	Option * Standard for the North America	Option * Standard for the North America	Option
	Encryption algorithm				JCMVP obtained CAVP obtained[*1]
Leakage of information due to a theft of the HDD	Delete all data in the HDD when destroying	Yes	Yes	Yes	Yes
	Erase automatically after copying/printing/scanning is completed (Data Overwrite Kit)	Option	Option	Option	Option
	Encryption HDD with the Wipe function	Yes	Yes	Yes	Yes
Unauthorized access from the network	Close unnecessary port	Yes	Yes	Yes	Yes
	IP Address filtering, MAC Address filtering	Yes	Yes	Yes	Yes
Unauthorized E-mail	E-mail authentication function (POP before SMTP)	Yes	Yes	Yes	Yes
	E-mail authentication function (SMTP authentication)	Yes	Yes	Yes	Yes

Possible dangers	Functions	e-STUDIO5055C Series e-STUDIO6570C Series e-STUDIO507 Series e-STUDIO857 Series	e-STUDIO5005AC Series e-STUDIO5008A Series e-STUDIO7506AC Series e-STUDIO8508A Series	e-STUDIO5008LP Series	e-STUDIO5015AC Series e-STUDIO5018A Series e-STUDIO7516AC Series e-STUDIO8518A Series e-STUDIO400AC Series
	E-mail authentication function (LDAP authentication)	Yes	Yes	Yes	Yes
Data wiretapped over the network	SSL/TLS (SMTP, POP3, LDAP, IPP, DPWS, FTP, HTTP, SOAP, Syslog)	Yes	Yes	Yes	Yes
	IPsec	Option	Option	Option	Option
	Digital certificate (PKI/SCEP)	Yes	Yes	Yes	Yes
	SNMPv3	Yes	Yes	Yes	Yes
	SNTP Authentication	Yes	Yes	Yes	Yes
	Secure DDNS	Yes	Yes	Yes	Yes
	IEEE802.1X with the wired LAN	Yes	Yes	Yes	Yes
Data wiretapped over the wireless LAN	WPA/WPA2 compliant	Yes	Yes	Yes	Yes
	IEEE802.1X	Yes	Yes	Yes	Yes
Leakage of electronic file	PDF encryption	Yes	Yes	Yes	Yes
Unauthorized access from the telephone line	Communication cut other than the fax protocol	Yes	Yes	Yes	Yes
Fax and IP-Fax mis-sending to other destination	Prevention from fax mis-sending to other destination	Yes	Yes	Yes	Yes
Taking away prevention	Private printing	Yes	Yes	Yes	Yes
	Hold printing (Print, Fax, IP-Fax, E-mail)	Yes	Yes	Yes	Yes
Unauthorized copy	Hardcopy Security Printing (control copying)	Yes	Yes	Yes	Yes

Possible dangers	Functions	e-STUDIO5055C Series e-STUDIO6570C Series e-STUDIO507 Series e-STUDIO857 Series	e-STUDIO5005AC Series e-STUDIO5008A Series e-STUDIO7506AC Series e-STUDIO8508A Series	e-STUDIO5008LP Series	e-STUDIO5015AC Series e-STUDIO5018A Series e-STUDIO7516AC Series e-STUDIO8518A Series e-STUDIO400AC Series
	Hardcopy security printing (prohibit copying, information tracking)	Option	Option	Option	Option
Unauthorized access	User authentication function (Windows authentication)	Yes	Yes	Yes	Yes
	User authentication function (LDAP authentication)	Yes	Yes	Yes	Yes
	Role-Based Access Control	Yes	Yes	Yes	Yes
	User authentication function (IC card authentication: MIFARE, HID, etc.)	Yes	Yes	Yes	Yes
	User authentication function (PIN authentication)	Yes	Yes	Yes	Yes
	User authentication function (Two-factor authentication)	Yes	Yes	Yes	Yes
	User authentication function (NFC authentication)			Yes	Yes
	Administrator privilege password authentication	Yes	Yes	Yes	Yes
	Restrict service technician to access	Yes	Yes	Yes	Yes
	Password authentication (BOX password)	Yes	Yes	Yes	Yes
	Record various security logs	Yes	Yes	Yes	Yes

Possible dangers	Functions	e-STUDIO5055C Series e-STUDIO6570C Series e-STUDIO507 Series e-STUDIO857 Series	e-STUDIO5005AC Series e-STUDIO5008A Series e-STUDIO7506AC Series e-STUDIO8508A Series	e-STUDIO5008LP Series	e-STUDIO5015AC Series e-STUDIO5018A Series e-STUDIO7516AC Series e-STUDIO8518A Series e-STUDIO400AC Series
	Log records whether copying/printing/scanning by user succeeded or failed	Yes	Yes	Yes	Yes
	Restriction of editing Address Book	Yes	Yes	Yes	Yes
	Access restriction to logs	Yes	Yes	Yes	Yes
	Syslog	Yes	Yes	Yes	Yes

Note 1: There is no plan to obtain the CAVP authentication for the e-STUDIO400AC Series.

3. DEVICE SECURITY

At every layer of the technology stack, Toshiba Tec protects our MFPs from any undesirable occurrences such as an unauthorized access, to ensure complete security through the entire lifecycle of the device from installation and operation to the end of its life.

3.1 Protection of HDD Data

An HDD (hard disk device) is equipped in TOSHIBA MFPs. Scanned original document data in copying are stored temporarily in the HDD. When copying is completed, although the management information (FAT: File Allocation Table) is erased, the temporarily stored data still remain in the HDD. In addition, a confidential document can be stored and controlled with a password in an e-Filing box of the HDD.

Some customers may be concerned that if a person with bad intent steals the HDD, the person can recreate a document from residual data or data in an e-Filing box and may be able to access confidential and private information. However, by utilizing the following encryption function and data overwriting function, the HDD data can be protected.

3.2 Data Encryption Function

3.2.1 Security HDD with the Wipe function

A security HDD with the Wipe function is installed and all data on the HDD are encrypted by an AES 256-bit algorithm. Therefore, by means of the Wipe function, even if the HDD is stolen, data invalidation works to prevent information leakage as soon as the HDD is installed in another device in an attempt to read data illegally out of the HDD. After completion of the use of the MFP or at the end of the lease period, all data on the HDD are instantly invalidated and data retrieval is completely disabled, once the service technician has performed this operation on the MFP according to the customer's instructions. For details about the security HDD with the Wipe function, refer to “Security HDD WP(English) for Subs.pdf”.

For the models in which no security HDD with the Wipe function is installed, an HDD encryption function using the software is embedded as the default and therefore this can be applied. An AES (Advanced Encryption Standard) 128-bit algorithm is adopted as the encryption method.

3.2.2 FIPS/JCMVP authentication HDD

A security HDD with the Wipe function compliant to FIPS 140-2/JCMVP is provided as an option.

3.2.3 Overwrite feature

Installation of an optional data overwrite kit (GP-1060/1070) allows data temporarily stored on the HDD from a copying, printing, scanning, faxing or IP-faxing operation to be automatically overwritten and erased by a DOD standard compliant method after the operation is completed.

This data overwrite kit also has the function of completely erasing the data in all HDD areas. After completion of the use of the MFP or at the end of the lease period, a service technician will perform this function according to the customer's instructions. Therefore, the retrieval of residual data on the HDD is completely disabled.

3.3 Network Security

An MFP has a TCP/UPD port opened in order to provide a network service. A client PC is connected to the MFP port that could respond to the service via the network. For example, in order to provide the LPD printing service, 515 ports of the MFP are opened. Some customers may be concerned that if an unnecessary port is opened, it could become a security hole.

3.3.1 Network access control

Ports, which do not provide a service, are not opened. Moreover, any port unnecessary for operation can be closed by using the administrator setting.

3.3.2 IP address filtering and MAC address filtering

IP address filtering and MAC address filtering are supported. Only an access request from a network node, such as a client PC, with an address registered in the MFP is accepted or access from a registered address can even be refused. Due to this, access from a malicious network node can be restricted. Moreover, a function which accepts an access request only from a client PC with a specific IP address or MAC address registered in the MFP, and one which does not accept an access request from a client PC with a specific IP address or MAC address registered in the MFP, are both supported.

From the e-STUDIO5005AC Series, the filter can be set to each port. It also can be set for a rejection of the response to ICMP.

3.3.3 Communication path protection (wired LAN)

Encrypted communication that flows over the network can protect communications. Although communication data can easily be wiretapped when the Network Trace Tool is used, through encryption, it will not be stolen even when wiretapped.

3.3.4 SSL (Secure Socket Layer) / TLS (Transport Layer Security)

Since TOSHIBA MFPs support up to TLS1.2, SSL3.0 whose vulnerability has been discovered is not used.

SSL/TLS communication is supported in HTTP Server/Client, IPP, LDAP, SMTP Client, POP3, FTP Server, Web Service Print, FTP Client, Web Services Scan, Syslog and SOAP.

In the HTTP Client function, SSL/TLS encryption is also carried out for access to TopAccess. HTTP is also used to access Address Book Viewer by utilizing encryption communication by means of SSL/TLS.

In IPPS, SSL/TLS encryption prevents print data from being wiretapped.

In POP3/SMTP, SSL/TLS communication prevents e-mail data from being wiretapped.

The FTP server function is used for backing up or restoring FTP print data and e-Filing Box data. SSL/TLS encryption can prevent these data from being wiretapped.

In Web Service Print, SSL/TLS encryption can prevent print data from being wiretapped.

In Web Service Scan and TWAIN Scan, SSL/TLS encryption can prevent data via Remote Scan from being wiretapped.

In FTPS, communications in Scan to Remote can be encrypted.

This MFP supports POODLE and FREAK. Therefore, lower security encryption and transmission systems such as SSL2.0/3.0 or SHA-1 are not used

3.3.5 IPsec (IP Security Architecture)

IPsec (IP Security Protocol) protects communication in the IP layer. It is said that the person who sends/receives data is authenticated, and non-repudiation is protected in order to secure confidentiality and entirety.

Both AH (Authentication Header) and ESP (Encapsulating Security Payload) security protocols are supported. AH secures the entirety of IP Packet, and ESP secures the confidentiality and entirety of IP Packet. For Key management protocol together with IPsec used, both IKEv1 and IKEv2 are supported. In the installation of the certificate, Import or SCEP can be utilized. IPv6 Ready logo for IPsec is also supported, and IPsec Ready Logo Phase-II is correspondent.

3.3.5.1 Wired IEEE802.1X

IEEE802.1X is a standard for authentication utilized in LAN connecting. As IEEE802.1X is well known for user authentication specification in wireless LAN such as IEEE802.11b, the specification itself is correspondent to wired LAN. It consists of supplicant, 802.1X switch, and authentication server. IEEE802.1X does not accept any communication from clients who are not certified, but it does accept communication from users to be certified. EAP (Extensible Authentication Protocol) is used to transmit an authentication message. EAP authentication has EAP-MD5 and EAP-TLS methods.

There are some EAPs to be utilized in 802.1X, and both the supplicant and the authentication server need to be correspondent to EAPs. Currently EAP-MD5, MSCHAPv2, EAP-TLS, EAP-TTLS and PEAP are supported. In installation of the certificate with EAP-TLS, EAP-TTLS and PEAP used, Import or SCEP can be utilized.

3.3.5.2 Network authentication

LDAP authentication supports CRAM-MD5, Digest-MD5 and Kerberos to protect the user name and password required for access to an LDAP server.

SMTP authentication supports CRAM-MD5, Digest-MD5, Kerberos and NTLM (IWA: Integrated Windows Authentication) to protect the user name and password required for access to an SMTP server.

POP3 authentication supports Kerberos, NTLM (SPA: Secure Password Authentication) and APOP to protect the user name and password required for access to a POP3 server.

SMB authentication supports NTLMv2 and Kerberos.

Dynamic DNS supports Secure Dynamic DNS (Domain Name System). When Secure Dynamic DNS is used, only the MFP in which the resource record has been registered or device with management authority for a DNS server can update zone information.

SNTP supports SNTP authentication, enabling authentication of an SNTP session between the MFP and an SNTP server

3.3.5.3 SNMPv3

Network Protocol SNMPv3, which has both a data encryption and a user authentication function, enhances security features.

3.3.5.4 Communication path protection (wireless LAN)

This function encrypts wireless communication to prevent decryption and access by a third party. It can also allow communications only with a pre-permitted party when a connected party is authenticated. Since wireless communication is performed by radio waves, communication could be intercepted in radio wave service areas. To prevent unauthorized usage by a third party, such as a falsification of data and spoofing, a wireless LAN option supports WPA/WPA2 Mixed Mode and WPA2, which encrypts communication data and allows user authentication for a communication party.

WPA and WPA2 are security standards established by Wi-Fi Alliance. WPA was created as a subset of IEEE802.11i, especially for improving user authentication and encryption. Later on, WPA2 that completely complies with IEEE802.11i was released. Compared with WPA, WPA2 provides more enhanced encryption and connectivity. Two connection methods are supported, as follows. WPAPSK allows user authentication and encrypts data when a "passphrase" shared between an access point and a client PC is preset. "Passphrase" is an optional character string set with from 8 to 63 characters. In addition to WPAPSK, a stronger security system (802.1X authentication) through a RADIUS server (authentication server) is supported. This is a connection mechanism, which verifies if the connected access point and the client PC are mutually appropriate parties.

As 802.1X authentication systems, EAP-TLS with a digital certificate and PEAPv0/EAP-MSCHAP v2 with a password are supported.

To make 802.1X authentication faster, WPA2 optionally supports Pairwise Master Key (PMK) caching. PMK caching stores authentication results including an encryption key to connect to a wireless LAN access point smoothly even if the location is changed. Moreover, a countermeasure to KRACKs which is the vulnerability of the wireless LAN has also been adopted.

3.4 Telephone Line and IP-Fax Access Control

A fax function is equipped in some MFPs as an option.

3.4.1 Telephone line access control

Regarding telephone line access, the MFPs do not accept another protocol, only the fax. The current fax board supports only a standard G3 fax and the unique procedural protocol of Toshiba Tec. When a connection is made to machines other than a regular one or a TOSHIBA one, the protocol cannot be established. As a result, it becomes a communication error and the line is disconnected. Therefore, you will not be able to access the network through the fax board from a telephone line. Furthermore, there is no chance of improper data becoming mixed. Remote-Maintenance from the fax line is not supported.

3.4.2 IP-Fax access control

For the IP-Fax function, a transmission/reception via a SIP (Session Initiation Protocol) server, via Gateway and direct transmission/reception are available. In addition, it can be set to receive only a SIP message from a SIP server which has not been registered in consideration of the security.

3.4.3 Prevention of Fax and IP-Fax mis-sending to other destinations

There is a possibility of a leakage of confidential information to an unintended address due to misdialing or misoperation when a fax or IP-fax is being sent. Various functions are provided to prevent this.

If this is required, ask your service technician to change the setting. Then the following options to prevent fax mis-sending operation will become available.

- A confirmation screen is displayed before the [START] button is pressed after the fax number is entered.
- A confirmation screen is displayed before the [START] button is pressed after the abbreviated dial or one-touch entry. After confirming, press the [START] button to send the fax.
- In case of sending a group broadcast transmission, a screen to confirm the selected group is displayed. Press the [START] button again to send the fax.
- One is not allowed to operate the [START] button while being on-hook or holding up an external telephone receiver. Moreover, there is a refusal sound and the operation is prevented even when the [START] button is pressed. (IP-Fax is not supported.)

4. ACCESS SECURITY

The access security accepts the access for specified users who have an access privilege to designated data or devices. The access to the device is controlled in the following three levels.

- The access to our MFPs is limited to only authorized persons or sites where it is physically or digitally available.
- Security policies are centrally managed and thereby ensure the highest level of access security.
- By monitoring the access to the MFPs, our security system proactively sends alerts to any unauthorized access.

4.1 Limitation of Use

4.1.1 Role-Based Access Control

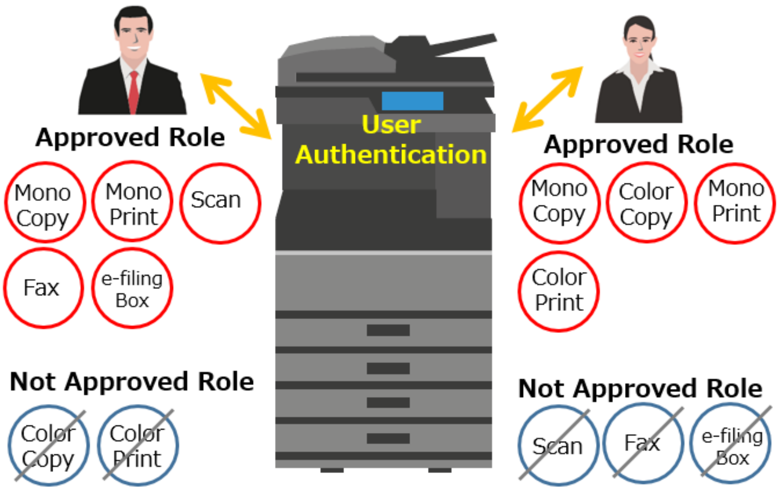
Unauthorized usage of the MFP may cause information leakage from a copying, printing, scanning or e-Filing box operation. To prevent the leakage, the available operations by a user can be restricted.

After user authentication is completed through the control panel or TopAccess, the only operations (objects) that are only permitted are copying, printing and faxing. For example, copying, printing, fax and IP-Fax transmitting and receiving and black output are available, while scanning and color output are prohibited for User B.

Setting of the role for users (which means the role of users, and which is able to be set for the administrator or the general user or pertinent section) is available in the centralized managed directory database LDAP (including the Active Directory LDAP function). Moreover, an attribute which an LDAP server has already had beforehand can also be utilized as a role.

When logging in the MFP with the user authentication function, the MFP acquires the role information already allocated to a user in an LDAP server, and checks the access rights allocated to its role from ACL (Access Control List) and gives usage permission for each function to the user. The 20 settings are available access rights to be allocated in the role: e.g.: Device setting, Copy, E-mailSend, FileSave, iFaxSend, Print, e-Filing, FaxSend, Color output (Copy, Print), Remote Scan, USB Print/Save, Editing Address Book, Log management. As the setting of the role information can be allocated to the access rights to all users' attributes set in the existing LDAP server, configuration of a new LDAP server is not required and you can set it securely. In addition, the roles will be set in local authentication or created by the administrator.

Role-Based Access Control



4.2 Log Information Access

Operations on the control panel and in TopAccess can be recorded as logs in order to prevent unauthorized usage of the MFP and ensure traceability.

By enabling user authentication, the history of the operations (copying, printing, scanning, fax and IP-Fax transmitting and receiving) by the user and failure logs can be recorded. Thus, unauthorized access or fraud can be detected. On the control panel or in TopAccess, obtained logs can be observed. When user authentication is enabled, users can only browse their own job logs.

When user authentication is disabled, job logs can be switched between visible and hidden, allowing administrators and auditors to browse all logs.

Various security logs are added.

From the e-STUDIO5005AC Series, the Syslog has also been supported.

4.3 Identification Authentication

4.3.1 User authentication function

A user authentication function is equipped in the MFP in order to prevent unauthorized access to the MFP. The user authentication function provides the following user management tasks:

- Restricting operations on the touch panel
- Restricting access to MFP configuration or log information
- Restricting available operations (copying/printing/scanning/faxing) by users (Role-Based Access Control)
- Logging operations by users
- Managing the counter by users
- Necessity or lack thereof for setting of user authentication at each function
- Personal authentication by means of an NFC function from an Android mobile terminal is available, instead of entry of the password.

4.3.2 Authentication methods

The following authentication methods have been supported.

- Department code authentication
- User ID/password authentication
  - Local authentication (authentication is performed by the MFP itself)
  - Windows domain authentication (a Windows server is used as an authentication server)
  - LDAP server authentication (an LDAP server is used as an authentication server)
- PIN authentication
- IC card authentication
- Two-factor authentication using an IC card and PIN
- Authentication using an NFC function with an Android terminal

4.3.3 Restriction on operations by user authentication

Operations on the touch panel can be restricted by first having an authentication screen displayed. It is possible to set whether the authentication screen is to be displayed or not when each function button (COPY, SCAN, PRINT and FAX) is pressed by setting the user authentication for each function of the MFP.

4.3.4 Registration and management of user information

There are two methods to register/manage user information utilized in user authentication:

1) Regarding department management, up to 1,000 departments can be registered and used. Also, up to 10,000 users can be registered in the MFP.

2) It can be coordinated with the user authentication system established in the corporation. Available user authentication systems are the Windows authentication system (Active Directory) that is generally widely used for directory services and LDAP.

As for the authentication method, in addition to entering an ID and password on the keyboard, a non-contact IC card MIFARE/HID etc., which provides both convenience and security, can be used as an optional authentication device.

This authenticates users and allows them to use the MFP just by holding an IC card MIFARE/HID onto the card reader connected to the MFP, eliminating a cumbersome password entry on the control panel. Also, as the existing corporate ID card (MIFARE/HID, etc.) used to enter/leave a room can be used for operating the MFP without making any changes and this method can be introduced at low cost.

4.3.5 Password policy setting

The following password policy can be set when local authentication is performed. Due to this, a more difficult password can be set in local authentication.

- Minimum password length
- Password validity period
- Character strings whose use in the password is prohibited
- Number of the lockout times and the lockout period caused by a login failure

4.4 Tracking

4.4.1 Tracking by image logs

To ensure the traceability of the MFP's copying, scanning, faxing and IP-Faxing data, they can be stored as image thumbnail data along with the job information.

When copying or scanning is performed or a fax or IP-Fax is transmitted or received in the MFP, the data can be transmitted to a designated external server as the image thumbnail data along with the job information (date and time, user name, file name, serial number of the MFP). This function enables the tracking of data if an information leakage does occur subsequent to copying, scanning, faxing and IP-Faxing with the MFP.

In order to prevent information leakage resulting from the improper use of this function, it is disabled by default. Ask your service technician to enable this function if you want to use it.

4.4.2 Tracking by forced printing

To enable the tracing of the MFP's copying and printing documents, information such as the date and time, user name, etc. can be forcibly added onto them.

Forced printing of the date and time, user name and card ID enables the tracking of the data related to who has performed output copying, printing, fax and IP-Fax transmission as well as when.

4.4.3 Security function during E-mail transmission

Unauthorized usage of the Scan to E-mail function may cause an information leakage through E-mails or wiretapping. To prevent this problem, the Scan to E-mail function provides a security function for E-mail transmission.

The following security functions are supported for e-mail transmission in the Scan to E-mail function of the MFP.

4.4.4 E-mail authentication

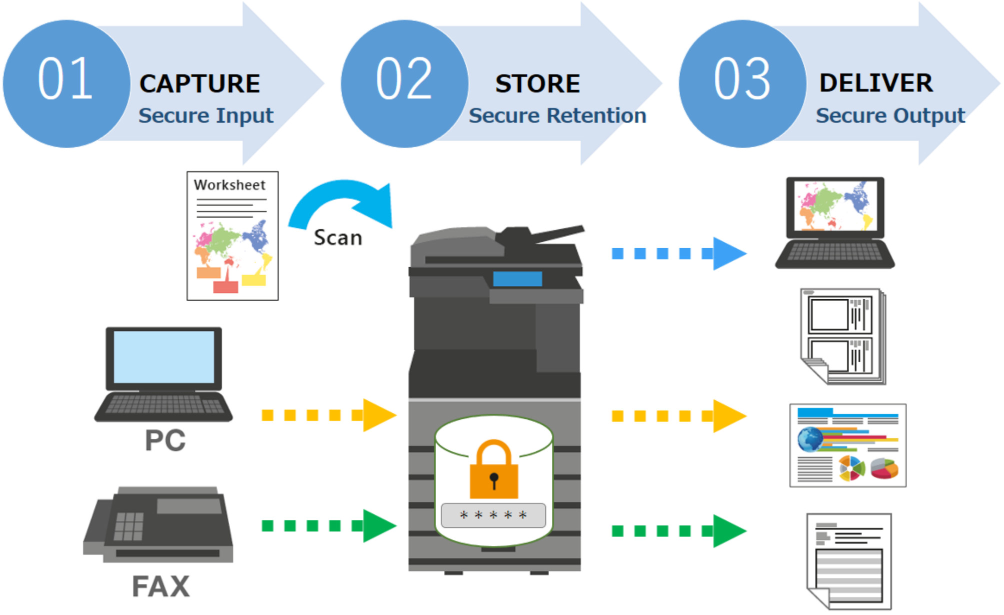
As the authentication systems, standard protocols (POP before SMTP, SMTP Authentication (LOGIN/PLAIN/CRAM-MD5/Digest-MD5/Kerberos) and LDAP Authentication (LOGIN/PLAIN/CRAM-MD5/Digest-MD5/Kerberos)) are equipped in the MFP, thus the protocols can be selected in accordance with the corporate policy.

4.4.5 BCC transmission function

The BCC (Blind Carbon Copy) function is also available for transmitting internet faxes as well as the E-mail transmission.

5. DOCUMENT SECURITY

Not only the security of the MFPs themselves, but also the security of your documents is also ensured during the entire lifecycle. Your sensitive documents are consistently protected when they are entered in, stored on, and leave the MFPs in any physical or digital means such as printing, fax, scanning, copying and so on.



5.1 Security in Printing

5.1.1 Secure printing function

When user authentication is disabled, private printing is used to transmit print data with a password up to 64 alphanumeric characters from a client PC to the MFP, the transmitted data are stored temporarily in the HDD of the MFP. Unless the password is entered from the control panel, printing will not start.

When user authentication is enabled, hold printing, private printing or multi station printing (optional) is used to allow users to command only print jobs sent on their own without entering a password for private printing, after logging into the MFP. By setting the MFP to require a user name and a password when a job is sent to the MFP from a printer driver, user authentication is available for a shared client PC used by multiple users.

In addition, users can command their own print jobs by simply holding an IC card over the control panel instead of performing user authentication, through the use of an optional authentication non-contact IC card device, MIFARE/HID, etc. Once logged in, users are also allowed to automatically to output their print data without sending a print job. Secure printing can be switched to forced private printing or forced hold printing.

The e-Filing box with a password, private printing, hold printing or multi station printing function is used to store or print confidential documents.

The administrator configuration allows all jobs to be temporarily stored in private, hold or multi station queues, and then released as desired, instead of being immediately released.

Document or user names can be hidden on the status screen to ensure security.

5.1.2 Hardcopy security printing

The Hardcopy Security Printing function embeds a particular fine dot pattern on documents during printing. When they are copied, hidden characters emerge. Due to this, this function can effectively restrict unauthorized copying and prevents the leakage of information printed on the document.

In addition to this, GA-1190A (optional) can also prohibit unauthorized copying and perform information tracking. An embedded fine dot pattern is added to a document during printing by specifying Hardcopy Security Printing in a printer driver. When this printed document is copied, the pre-embedded character string “COPY” will conspicuously appear to restrict information leakage caused by unauthorized copying. Moreover, when attempt is made to copy, fax, IP-Fax or scan a printed document on a TOSHIBA MFP equipped with a copy prohibiting function, the operation stops if this pattern is detected. As a result, the security of confidential documents can be strictly maintained. If this printed document is left unattended, and the scanned image data on it are analyzed using an optional software item, such as "when", "who", "what", "which client PC to create" and "which MFP to print", they are retrieved and displayed on the client PC screen.

5.1.3 Confidential document access control

With regard to images stored in the HDD, access restriction must be password authenticated. Image data that need to be handled as confidential documents will be protected from leakage and falsification by a third party.

5.1.4 e-Filing box with a password

Setting a 64-digit password into the HDD of the MFP can create an e-Filing box. The file stored in the e-Filing box can be printed from the control panel. Thumbnail display from a client PC Web browser and editing can be access restricted by the password. The password policy can be applied to a password of the e-Filing box.

5.1.5 PDF encryption

This function is available to encrypt PDF documents and restrict the operation by setting a password during scanning. By entering the password (user password), the encrypted PDF file can be displayed. The encryption level is 128bit RC4, 40bit RC4 and 128bit/256bit AES. Operation restrictions can be set for Print, Documents Change, Contents Extraction and Accessibility, respectively. The restriction setting information is protected by the password (master password). If an encrypted PDF file is sent to a wrong destination or sniffed, this function prevents users who do not know the password from viewing it. This function also protects distributed PDF documents from unauthorized printing or tampering.

5.1.6 Confidential setting of document name and user name

This function allows one to indicate a document name, a user name and a destination by “*” when a job state or log is displayed on the touch panel or TopAccess.

5.2 Protection of Fax and IP-Fax Received Data

Some customers may be concerned about the leakage of confidential information when receiving faxes and IP-Faxes that are printed during holidays or at night. Making the setting of the following functions will prevent the leakage of confidential information.

5.2.1 Fax and IP-Fax secure receiving function

The start time (SECURE RECEIVE ON STATE) and end time (SECURE RECEIVE OFF STATE) can be set for days of the week in the administrator mode.

- When this function is enabled, received data are stored in the MFP instead of being automatically printed.
- When this function is disabled, received data are immediately printed.

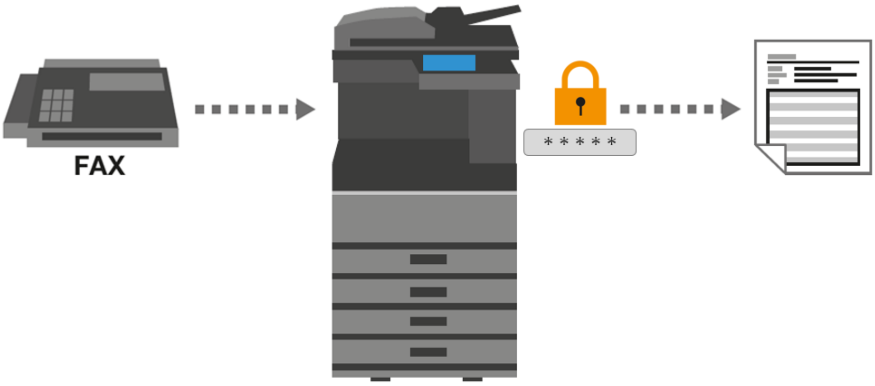
While this function is enabled, received fax and IP-Fax data are printed in the following cases.

- By entering a password while this function is enabled
- Printed automatically when this function is disabled

The function is automatically disabled when the fax hold function is enabled. Such data are stored in the fax hold queue when the fax hold function is enabled even if the fax secure receiving function is enabled and a schedule is set.

When data are received while the secure receiving function is enabled, a message indicating the presence of received data appears at the bottom of the touch panel of the MFP.

The message remains until all data are printed. When data are received while the secure receiving function is enabled, the PRINT DATA lamp is also turned on. This lamp remains on until all data are printed. The lamp remains on when the MFP goes into sleep mode even if received data are present. The lamp is turned off; however, when the MFP goes into super sleep mode while received data are present.



5.2.2 Fax hold function

The fax hold function is used to prevent the leakage of confidential information received by fax and IP-Fax. The fax hold function can only be enabled by a service technician. Therefore, if you need to use this function, contact your service technician.

When the fax hold function is enabled, fax and IP-Fax received data are always stored in the fax hold queue.

Users initially registered as “Faxope” users, or users assigned as “Fax Operator” can print out the data stored in the fax hold queue. To print out the data, click [Print] and select [Hold print (Fax)]. The “Fax Operator” role can be assigned to any user using the administrator mode.

When the fax hold function is enabled and fax and IP-Fax received data are present, a message indicating the presence of received data appears at the bottom of the touch panel of the MFP and the PRINT DATA lamp is turned on.

6. MEASURES TO VULNERABILITY

6.1 Provision of the Security Patch

If a vulnerability has been disclosed in the firmware, a security patch against it will be timely provided.

6.2 Malware Targeted at Windows

Some customers may be concerned about infection of network viruses (worms) such as WannaCry or infection from websites (TopAccess) targeting Windows. They may also be concerned about countermeasures against viruses that invades MFPs via a USB storage device.

MFPs are not affected by network malware (viruses, etc.) targeted at Windows. For example, they are not affected by WannaCry.

6.3 Vulnerability to OSS

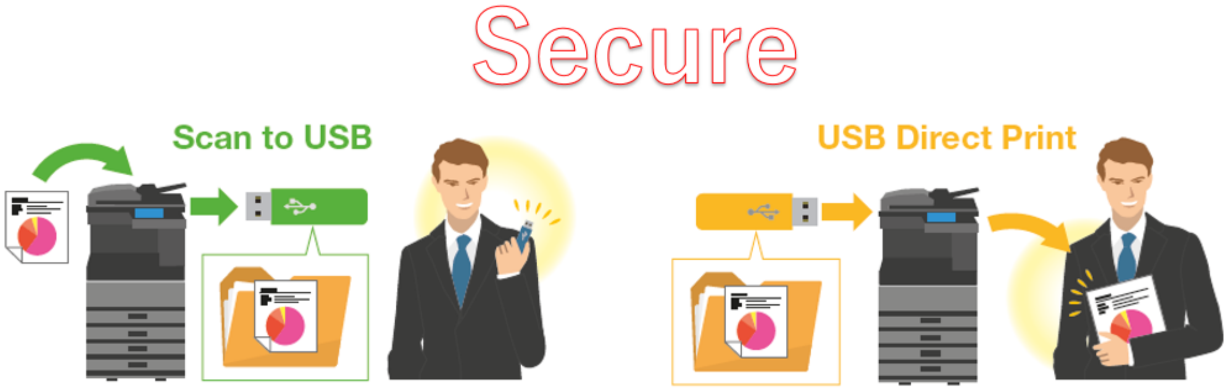
MFPs use some open sources (OSS). Countermeasures to vulnerabilities to these disclosed OSS have been taken one by one. Cross-Site Request Forgery, Cross Site Scripting, SQL Injection and OS Command Injection are well-known vulnerabilities. Countermeasures to them have been taken in MFPs. In addition, countermeasures to the following vulnerabilities reported by the press have also been taken. POODLE, FREAK, GHOST, Heartbleed, Shellshock, KRACK, Faxploit, KNOB

6.4 Invading of Viruses from a USB Port

Countermeasures against viruses that make their invading to MFPs via a USB storage device have also been taken. In USB Direct printing, a file is handled as print data. Therefore, even if Malware or scripts are included in the file, only an image drawing error will occur. Malware or scripts are not executed.

When Scan to USB is performed, the file is just loaded from the MFP to a USB storage device. Malware in the USB storage device is not operated.

Due to this, Malware or scripts in the USB storage device are not executed.



6.5 E-mail

Since the MFP has functions such as receiving e-mails, printing attached files and storing into an e-Filing box, some customers may be concerned about virus infections occurring when they receive e-mails.

In the e-mail receiving function, an attached file is handled as print data. Therefore, even if malware or scripts are included in the file, only an image drawing error will occur. Malware or scripts are not executed.

7. SOLUTION PLATFORM SECURITY

7.1 e-BRIDGE Open Platform Security

In e-BRIDGE Open Platform, Meta Scan function (GS-1010, optional) and Embedded Web Browser function (GS-1020, optional) which provides Embedded Web Browser and Web Service interface are supported. By using the user authentication function which can be limited to operate the control panel of the MFP, the security of these functions can be maintained. After a scanning operation, confidential data to be stored are protected from falsification and leakage by a third party.

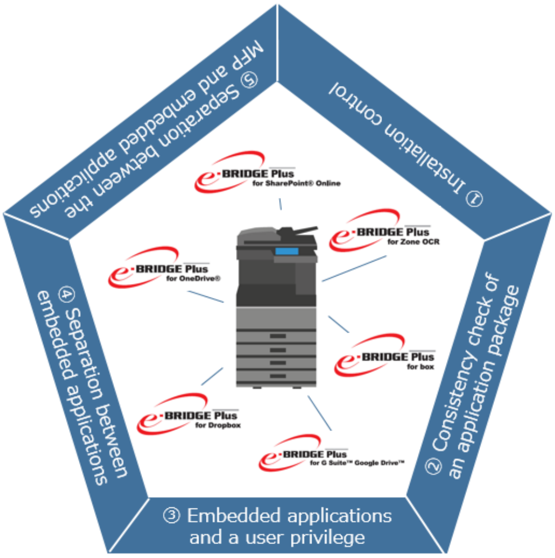
In department management or user authentication, neither Embedded Web Browser nor Meta Scan function can be used without authentication.

7.2 Embedded Application Platform

The Embedded Application function allows one to install additional applications in the MFP and utilize them. This function equips the following features to protect the customers' MFPs.

7.2.1 Installation Control

Installation and uninstallation of the embedded applications can be performed only by an administrator or service technician such as a user with an MFP management privilege. Installation and uninstallation is controlled so that a user with no MFP management privilege cannot make to do so. Therefore, it will be possible to prevent the operation of unintended applications by an administrator on the MFP.


① Installation control
② Consistency check of an application package
③ Embedded applications and a user privilege
④ Separation between embedded applications
⑤ Separation between the MFP and embedded applications
e-BRIDGE Plus for SharePoint® Online
e-BRIDGE Plus for Zone OCR
e-BRIDGE Plus for OneDrive®
e-BRIDGE Plus for box
e-BRIDGE Plus for Dropbox
e-BRIDGE Plus for G Suite™ Google Drive™

7.2.2 Consistency check of an application package

An application installer of the embedded applications allows to install only a package certificated by Toshiba Tec in the MFP. Therefore, this will prevent the installation of invalid applications such as falsified package and a one created by unknown creator in the MFP.

7.2.3 Embedded applications and a user privilege

The operation by general users is controlled. Therefore, even when they operate embedded applications which are performed on the touch panel of the MFP, they cannot perform the operations beyond the privilege given by role base user authentication of the MFP. Due to this, no operations which are not permitted to general users by an administrator can be performed through embedded applications.

7.2.4 Separation between embedded applications

File storages of which embedded applications can be operated are separated from each other. Even when multiple embedded applications are installed, accessing to each data item is not possible. Due to this, confidential data can be stored securely in file storages of the embedded applications.

7.2.5 Separation between the MFP and embedded applications

File storages of embedded applications and the MFP are separated in each other. Due to this, confidential data stored in the MFP cannot be viewed from the embedded applications directly.

Therefore, protection against the leakage of confidential data such as a user password from the embedded applications will be given. In addition, operation of the MFP from embedded applications is controlled by the above role base user authentication. Due to this, general users cannot perform viewing or operating of data beyond their given privilege.

8. REMOTE MAINTENANCE

8.1 e-BRIDGE CloudConnect Security

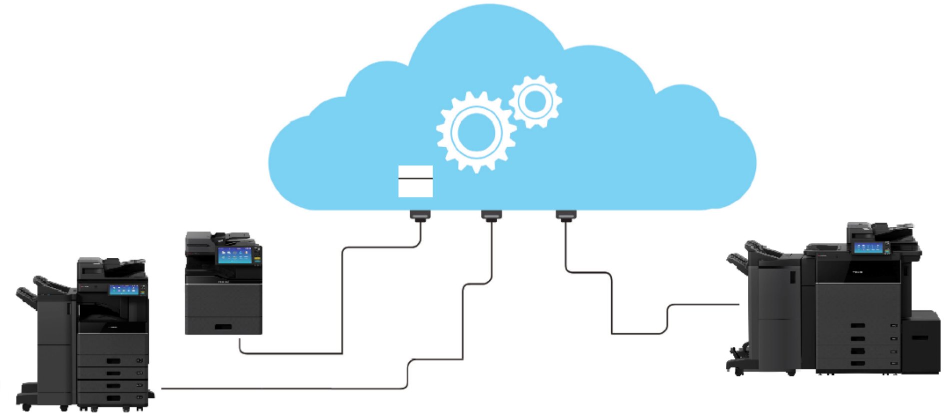
e-BRIDGE CloudConnect securely and reliably collects operation data transmitted from your MFPs.

e-BRIDGE CloudConnect uses the same principles used by client PCs accessing secure data over a browser with HTTPS (server authentication and encryption). Data can only be sent from MFPs and access is limited to e-BRIDGE CloudConnect servers with valid authentication certificates. This will provide very high-level security.

To prevent server spoofing and to make sure data are transmitted to the correct server, e-BRIDGE CloudConnect features server authentication functionality that confirms whether the server to be accessed (e-BRIDGE CloudConnect) is the actual server that has been specified. All transmitted and received data are encrypted to preserve confidentiality and safety, and to protect against stealing, leaking and tampering.

e-BRIDGE CloudConnect only handles the MFP operation status information. This includes data concerning charging and maintenance such as information on counter data (the number of sheets used, etc.), MFP failures, consumables' replacements, MFP settings and adjustments. Since e-BRIDGE CloudConnect does not handle actual document data, copy, fax, print and scan data will not be leaked to a third party. On request, a service technician can set e-BRIDGE CloudConnect to permit or deny transmission. The MFP is operated and managed based on the system's security policy, in accordance with ISO 27001 international standard for information security management.

If a security issue has occurred, security patches can be distributed by using e-BRIDGE CloudConnect.



9. REGULATORY REQUIREMENTS

9.1 MFP

9.1.1 ISO/IEC15408

ISO/IEC15408 (Information Technology Security Evaluation Criteria) is called as CC certification and is an international standard for evaluating and certifying the functionality and quality of IT products. The security functions and quality of certified IT products have been accepted in many countries participating in the Common Criteria Recognition Arrangement (CCRA).

EAL stands for Evaluation Assurance Level, which indicates the levels of assuring the evaluations. Target IT products are evaluated in accordance with the requirements defined by EAL. The higher EALs include the evaluations for the lower ones. However, EALs represent evaluation strictness, not security strength. Therefore, the level of the EALs is not always matched the security level of the evaluated products.

The products later than the e-STUDIO4540C Series and e-STUDIO6550C Series have obtained EAL3+ALC_FLR2 certification which conformed with IEEE2600.1.

The e-STUDIO5008LP Series have obtained EAL2+ALC_FLR2 certification which conformed with IEEE2600.2.

The e-STUDIO5015AC Series, e-STUDIO5018A Series, e-STUDIO7516AC and e-STUDIO8518A Series have obtained a CC certification which conformed with HCD PP v1.0 (Protection Profile for Hardcopy Devices 1.0).

HCD PP v1.0 is a document collectively drawn up by the IT security agencies IPA (Information-technology Promotion Agency, Japan) and NIAP (National Information Assurance Partnership, U.S.A.), and companies of the digital multifunctional devices in Japan and U.S.A. and describes security requirements for government procurement of those devices. Various security functions and encryption requirements necessary for digital multifunctional devices are regulated.

CC certificate acquisition status

Model Name	Acquisition	URL
e-STUDIO550/650/810	Certified in March, 2004	—
e-STUDIO3511/4511	Certified in March, 2005	—
e-STUDIO600/720/850	Certified in March, 2006	—
e-STUDIO281C/351C/451C	Certified in March, 2006	—
e-STUDIO232/282	Certified in March, 2006	—
e-STUDIO352/452	Certified in March, 2006	—
e-STUDIO2500C/3500C/3510C	Certified in June, 2006	—
e-STUDIO163/165/205	Not certified	—
e-STUDIO166/167/207	Not certified	—
e-STUDIO232/282	Certified in August, 2008	—
e-STUDIO352/452	Certified in August, 2008	—
e-STUDIO600/720/850	Certified in August, 2008	—
e-STUDIO2330C/2820C/2830C/3520C/4520C	Certified in December, 2008	—
e-STUDIO5520C/6520C/6530C	Certified in December, 2008	—

Model Name	Acquisition	URL
e-STUDIO255/355/455	Certified in June, 2009	—
e-STUDIO655/755/855	Certified in June, 2009	—
e-STUDIO2040C/2540C/3040C/3540C/4540C	Certified in October, 2011	https://www.ipa.go.jp/security/jisec/jisec_e/certified_products/c0328/c0328_it0296.html
e-STUDIO5540C/6540C/6550C	Certified in October, 2011	https://www.ipa.go.jp/security/jisec/jisec_e/certified_products/c0327/c0327_it0297.html
e-STUDIO206L/256/306/356/456/506	Certified in May, 2012	https://www.ipa.go.jp/security/jisec/jisec_e/certified_products/c0348/c0348_it1388.html
e-STUDIO556/656/756/856	Certified in May, 2012	https://www.ipa.go.jp/security/jisec/jisec_e/certified_products/c0349/c0349_it1389.html
e-STUDIO2050C/2550C	Certified in October, 2012	https://www.ipa.go.jp/security/jisec/jisec_e/certified_products/c0376/c0376_it2409.html
e-STUDIO2555C/3055C/3555C/4555C/5055C	Certified in April, 2013	https://www.ipa.go.jp/security/jisec/jisec_e/certified_products/c0388/c0388_it2432.html
e-STUDIO306LP	Certified in November, 2013	https://www.ipa.go.jp/security/jisec/jisec_e/certified_products/c0412/c0412_it3465.html
e-STUDIO5560C/6560C/6570C	Certified in November, 2015	https://www.ipa.go.jp/security/jisec/jisec_e/certified_products/c0491/c0491_it4484.html
e-STUDIO207L/257/307/357/457/507	Certified in November, 2015	https://www.ipa.go.jp/security/jisec/jisec_e/certified_products/c0489/c0489_it4482.html
e-STUDIO557/657/757/857	Certified in November, 2015	https://www.ipa.go.jp/security/jisec/jisec_e/certified_products/c0490/c0490_it4483.html
e-STUDIO2000AC/2500AC	Certified in September, 2016	https://www.ipa.go.jp/security/jisec/jisec_e/certified_products/c0522/c0522_it5581.html
e-STUDIO2505AC/3005AC/3505AC/4505AC/5005AC	Certified in September, 2016	https://www.ipa.go.jp/security/jisec/jisec_e/certified_products/c0523/c0523_it5582.html

Model Name	Acquisition	URL
e-STUDIO2008A/2508A/3008A/3508A/4508A/5008A	Certified in September, 2016	https://www.ipa.go.jp/security/jisec/jisec_e/certified_products/c0524/c0524_it5583.html
e-STUDIO5506AC/6506AC/7506AC	Certified in November, 2016	https://www.ipa.go.jp/security/jisec/jisec_e/certified_products/c0528/c0528_it5584.html
e-STUDIO5508A/6508A/7508A/8508A	Certified in November, 2016	https://www.ipa.go.jp/security/jisec/jisec_e/certified_products/c0529/c0529_it5585.html
e-STUDIO3508LP/4508LP/5008LP	Certified in July, 2017 (IEEE2600.2)	https://www.ipa.go.jp/security/jisec/jisec_e/certified_products/c0566/c0566_it6624.html
e-STUDIO2010AC/2510AC	Certified in March, 2019 (Protection Profile for Hardcopy Devices 1.0)	https://www.ipa.go.jp/security/jisec/jisec_e/certified_products/c0629/c0629_it8689.html
e-STUDIO2515AC/3015AC/3515AC/4515AC/5015AC	Certified in March, 2019 (Protection Profile for Hardcopy Devices 1.0)	https://www.ipa.go.jp/security/jisec/jisec_e/certified_products/c0633/c0633_it8690.html
e-STUDIO2018A/2518A/3018A/3518A/4518A/5018A	Certified in March, 2019 (Protection Profile for Hardcopy Devices 1.0)	https://www.ipa.go.jp/security/jisec/jisec_e/certified_products/c0631/c0631_it8692.html
e-STUDIO5516AC/6516AC/7516AC	Certified in March, 2019 (Protection Profile for Hardcopy Devices 1.0)	https://www.ipa.go.jp/security/jisec/jisec_e/certified_products/c0632/c0632_it8693.html
e-STUDIO5518A/6518A/7518A/8518A	Certified in March, 2019 (Protection Profile for Hardcopy Devices 1.0)	https://www.ipa.go.jp/security/jisec/jisec_e/certified_products/c0630/c0630_it8691.html
e-STUDIO330AC/400AC	Applying (Protection Profile for Hardcopy Devices 1.0)	https://www.ipa.go.jp/security/jisec/jisec_e/certified_products/c0684/c0684_it9734.html

9.1.1.1 JCMVP authentication

The JCMVP is a certification system operated by IPA (Information-technology Promotion Agency, Japan). This system certifies that the encryption module conforms with JIS X 19790 (ISO/IEC 19790).

It has been verified that each encryption algorithm has been implemented in the MFPs properly and the result has been registered in the following implementations of IPA.

AES Verified Implementations

Model Name	Cert. #	URL
e-STUDIO2010AC/2510AC e-STUDIO2515AC/3015AC/3515AC/4515AC/5015AC e-STUDIO2018A/2518A/3018A/3518A/4518A/5018A e-STUDIO5516AC/6516AC/7516AC e-STUDIO5518A/6518A/7518A/8518A	47	https://www.ipa.go.jp/security/jcmvp/jcmvp_e/algval/aesval.html#47
	48	https://www.ipa.go.jp/security/jcmvp/jcmvp_e/algval/aesval.html#48
	49	https://www.ipa.go.jp/security/jcmvp/jcmvp_e/algval/aesval.html#49
e-STUDIO330AC/400AC	61	https://www.ipa.go.jp/security/jcmvp/jcmvp_e/algval/aesval.html#61
	62	https://www.ipa.go.jp/security/jcmvp/jcmvp_e/algval/aesval.html#62

RSA Verified Implementations

Model Name	Cert. #	URL
e-STUDIO2010AC/2510AC e-STUDIO2515AC/3015AC/3515AC/4515AC/5015AC e-STUDIO2018A/2518A/3018A/3518A/4518A/5018A e-STUDIO5516AC/6516AC/7516AC e-STUDIO5518A/6518A/7518A/8518A	20	https://www.ipa.go.jp/security/jcmvp/jcmvp_e/algval/rsaval.html#20
	21	https://www.ipa.go.jp/security/jcmvp/jcmvp_e/algval/rsaval.html#21
e-STUDIO330AC/400AC	31	https://www.ipa.go.jp/security/jcmvp/jcmvp_e/algval/rsaval.html#31

SHS Verified Implementations

Model Name	Cert. #	URL
e-STUDIO2010AC/2510AC e-STUDIO2515AC/3015AC/3515AC/4515AC/5015AC e-STUDIO2018A/2518A/3018A/3518A/4518A/5018A e-STUDIO5516AC/6516AC/7516AC e-STUDIO5518A/6518A/7518A/8518A	31	https://www.ipa.go.jp/security/jcmvp/jcmvp_e/algval/shaval.html#31
	32	https://www.ipa.go.jp/security/jcmvp/jcmvp_e/algval/shaval.html#32
e-STUDIO330AC/400AC	44	https://www.ipa.go.jp/security/jcmvp/jcmvp_e/algval/shaval.html#44
	45	https://www.ipa.go.jp/security/jcmvp/jcmvp_e/algval/shaval.html#45

HMAC Verified Implementations

Model Name	Cert. #	URL
e-STUDIO2010AC/2510AC e-STUDIO2515AC/3015AC/3515AC/4515AC/5015AC e-STUDIO2018A/2518A/3018A/3518A/4518A/5018A e-STUDIO5516AC/6516AC/7516AC e-STUDIO5518A/6518A/7518A/8518A	22	https://www.ipa.go.jp/security/jcmvp/jcmvp_e/algval/hmacval.html#22
	23	https://www.ipa.go.jp/security/jcmvp/jcmvp_e/algval/hmacval.html#24
e-STUDIO330AC/400AC	29	https://www.ipa.go.jp/security/jcmvp/jcmvp_e/algval/hmacval.html#29

DRBG Verified Implementations

Model Name	Cert. #	URL
e-STUDIO2010AC/2510AC e-STUDIO2515AC/3015AC/3515AC/4515AC/5015AC e-STUDIO2018A/2518A/3018A/3518A/4518A/5018A e-STUDIO5516AC/6516AC/7516AC e-STUDIO5518A/6518A/7518A/8518A	8	https://www.ipa.go.jp/security/jcmvp/jcmvp_e/algval/drbgval.html#8
	9	https://www.ipa.go.jp/security/jcmvp/jcmvp_e/algval/drbgval.html#9
e-STUDIO330AC/400AC	14	https://www.ipa.go.jp/security/jcmvp/jcmvp_e/algval/drbgval.html#14
	15	https://www.ipa.go.jp/security/jcmvp/jcmvp_e/algval/drbgval.html#15

KDF Verified Implementations

Model Name	Cert. #	URL
e-STUDIO2010AC/2510AC e-STUDIO2515AC/3015AC/3515AC/4515AC/5015AC e-STUDIO2018A/2518A/3018A/3518A/4518A/5018A e-STUDIO5516AC/6516AC/7516AC e-STUDIO5518A/6518A/7518A/8518A	1	https://www.ipa.go.jp/security/jcmvp/jcmvp_e/algval/kdfval.html#1
e-STUDIO330AC/400AC	2	https://www.ipa.go.jp/security/jcmvp/jcmvp_e/algval/kdfval.html#2

KDF: Key Derivation Function

9.1.1.2 CAVP authentication (FIPS140-2)

The CAVP (Cryptographic Algorithm Validation Program) is a certification system collectively operated by NIST (National Institute of Standards and Technology, U.S.A.) and CSEC (Communications Security Establishment Canada). The certified encryption algorithm has been disclosed in the following URL of NIST.

Model Name	Validations Number	URL
e-STUDIO2010AC/2510AC e-STUDIO2515AC/3015AC/3515AC/4515AC/5015AC e-STUDIO2018A/2518A/3018A/3518A/4518A/5018A e-STUDIO5516AC/6516AC/7516AC e-STUDIO5518A/6518A/7518A/8518A	C374	https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=10734
	C375	https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=10735
	C376	https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=10736

9.2 Security HDD with the Wipe Function

The security HDD with the Wipe function used for GE-1230 (option) has been given JCMVP authentication by IPA (Japan) and CMVP (FIPS140-2) authentication by NIST (U.S.A.), as a certification system of encryption products.

9.2.1 JCMVP authentication

JCMVP authentication is an encryption module certificate system based on JIS X 19790 (ISO/IEC 19790) carried out by IPA. It has been certified that AES, SHS, HMAC and DRBG have been properly implemented as encryption modules and the result has been registered in the following Cryptographic Module Validation List of IPA.

Model Name	Cert. #	URL
GE-1230 Toshiba Secure TCG Opal SSC and Wipe technology Self-Encrypting Drive (MQ01ABU050BW, MQ01ABU032BW and MQ01ABU025BW)	F0022	https://www.ipa.go.jp/security/jcmvp/jcmvp_e/val.html#F0022

9.2.2 CMVP authentication (FIPS140-2)

The CMVP (Cryptographic Module Validation Program) is a certification system collectively operated by NIST (National Institute of Standards and Technology, U.S.A.) and CSEC (Communications Security Establishment Canada). The certified encryption module has been disclosed in the following URL of NIST.

Model Name	Cert. #	URL
GE-1230 Toshiba Secure TCG Opal SSC and Wipe technology Self-Encrypting Drive (MQ01ABU050BW, MQ01ABU032BW and MQ01ABU025BW)	2082	https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/2082

9.3 HIPAA

The Health Insurance Portability and Accountability Act designed to ensure that patient information is treated with the highest level of confidentiality both within the healthcare organization and outside of the organization. Toshiba security solutions offer various features that address the privacy and security of protected patient information. Secure device access, private printing capabilities, and an audit trail prevent improper device usage and only allow authorized users to receive the confidential data or documents.

9.4 GLB Act

The Gramm-Leach-Bliley Act directly relates to financial institutions, ensuring that consumers' are aware of how their personal financial information is being used and shared. The Financial Privacy Rule and Safeguards Rule govern the disclosure of private financial information and require all financial institutions to design and maintain systems to support the protection of customer information.

9.5 FERPA

The Family Education Rights and Privacy Act is a federal law that protects the privacy of student education records. This requires a heightened level of the security for educational institutions complying with the U.S. Department of Education. Password printing, controlled device access, data encryption and/or deletion ensure that sensitive information is not accessible on the multifunction devices.

9.6 The Sarbanes-Oxley Act (SOX)

Recently, stringent rules with the objective of changing financial practices and corporate governance regulations have been introduced. In response to high-profile corporate scandals, this has been passed to protect investors by improving the accuracy of corporate financial disclosures made in relation to the securities laws. Data security safeguards focus on restricting access to information, the tracking of data, and protection of data integrity.

9.7 DoD

The Department of Defense, directly under the President of the United States of America, formulates national security and defense policies. The Department of Defense Manual outlines rigid policies and standards in the interest of protecting the security of the United States. Toshiba's Disk Overwrite solution complies with the DoD standard of clearing and sanitizing a hard disk drive containing classified information.

9.8 California SB-327

Beginning January 1, 2020, this California legislative act requires a manufacturer of a connected device to equip the device with a reasonable security feature or features that are appropriate to the nature and function of the device, appropriate to the information it may collect, contain, or transmit, and designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure, as specified.

9.9 Security in the Organization

As the information society advances, personal information is becoming an increasingly important asset. In the meantime, cases where personal information is illegally collected and used for unexpected purposes without notifying relevant individuals are increasing and the society is becoming more concerned about the handling of personal information.

Once a large amount of personal information leaks, the company will not only lose credibility but also fall into a dangerous situation that may cause serious damage endangering company's existence. It is a social responsibility for companies to establish a good relationship of trust with customers, make an effective use of personal information, and protect it as well.

Toshiba Tec provides products equipped with a wide variety of the aforementioned security features, to allow its customers to avoid information leak. Toshiba Tec will enhance the partnership with customers and move forward with implementing safer security measures.

Toshiba Tec recognized the importance of personal data protection at an early stage and established the Privacy Policy and the Personal Data Protection Guidelines as in-house regulations, in February, 2001.

The personal data protection system has been improved. The Privacy Policy was amended and published on the web site in August, 2004. The Personal Data Protection Guidelines were significantly revised in accordance with regulatory requirements in November, 2004 and re-established as the Personal Data Protection Program (PDPP).

For details about Privacy Policy in Toshiba Tec, refer to the following URL.

http://www.toshibatec.com/privacy/