TA Triumph-Adler
The Document Business
CONSULTING REALISATION EFFICIENCY

Security White Paper

for TA Triumph-Adler MFPs & Printers

Version 052019

May 08, 2019

Date	Version	Page	Details
September 30, 2013	1.0		First Release
June 19, 2017	062017		Chapter 3: changed the title and added some description in 3.1 Chapter 3: added some explanations about “LDAP over TLS”, “Bonjour” and “Privet” in the table, 3.1.2 Chapter 3: added 3.1.3 Secure Hash Algorithm Settings Chapter 3: added some description in 3.3.3 Chapter 3: added some description in 3.3.4 Chapter 4: added some description in 4.1.3
October 12, 2018	102018		Chapter 1: made some changes in the description about certification. Chapter 2: added a sentence in 2.2.2 User Authorization Management Chapter 3: added descriptions about “VNC”, “VNC over TLS” and “Enhanced VNC over TLS” in the table, 3.1.2 Chapter 4: deleted “Option” from 4.1.1 and 4.1.2 Chapter 4: added “Trusted Platform Module (TPM)” Chapter 8: some adjustment in 8.4 Chapter 8: added “Secure Boot” and “Run Time Integrity Check (RTIC)”
May 8, 2019	052019		Chapter 4: changed the names of the security functions and added some descriptions in 4.1.2 HDD Overwrite-Erase Chapter 4: changed the name of the security function and added the new security functions such as “7-time Overwrite (A)”_DoD 5220.22-M ECE and “7-time Overwrite (B)”_BSI/VSITR method in 4.1.4 Security Data Sanitization

This document describes all the security features provided for TA Triumph-Adler printers and MFPs. However, not all the security features will be supported by all systems. For further information please refer to the instruction handbook.

1. Introduction

TA TRIUMPH-ADLER MFPs/Printers are embedded with an OS as standard. Like a PC, installing a HDD or SSD are also available into the MFP/Printer. The MFPs/Printers for the office use handle various types of sensitive information. Whereas, the MFPs/Printers are exposed to recent advanced and diversified threats, such as unauthorized access to the devices via a network, tapping or alteration of information in transit over a network, and leakage of information from HDD. KYOCERA Document Solutions Inc. (referred to as TA TRIUMPH-ADLER, hereafter) provides customers with a variety of security functions installed on its MFPs/Printers. We are always proactively taking security countermeasures against these threats so that our customers may rest assured to securely use TA TRIUMPH-ADLER MFPs/Printers. In addition, TA TRIUMPH-ADLER has obtained Common Criteria certification (known as ISO15408) that objectively verifies if security functions are correctly performed at customers' hand by the third party. This verification also applies to rigorous process that includes appropriate product design, manufacturing and delivery. TA TRIUMPH-ADLER products have been designed to have the necessary security functions and capabilities and so have been certified as they conform to an IEEE 2600.1/ IEEE 2600.2, which is an international security standard for hard copy devices enacted in 2009. Additionally, Federal Information Processing Standard, FIPS 140-2 certified cryptographic module, which complies with the security standard created by the U.S. National Institute of Standards and Technology, NIST, is installed on TA TRIUMPH-ADLER devices. TA TRIUMPH-ADLER will continuously drive further security enhancement as standards develop or new technologies evolve to protect the TA TRIUMPH-ADLER devices.

The target audience for this document is intended for staff members at the sales companies of TA TRIUMPH-ADLER, local dealers and customers to explain how security functions installed on our MFPs/Printers perform against the threats and enable us to maintain security management. We are sincerely hoping that this document will be fully utilized for TA TRIUMPH-ADLER sales and services activities or customer use.

2. Identification, Authentication and Authorization

2.1. Identification and Authentication

Identification and Authentication is an important process of verifying that a user has permission to access or use a device. A user is required to enter access credentials, such as a login user name and password, the user ID in order to identify the user, and password that only the user can know. *(Figure 1)*

To use the identification and authentication function, users are required to register a login user name and a login password on the MFPs/Printers in advance. That is, only users who have been registered are allowed to access the MFP/Printer. TA TRIUMPH-ADLER MFPs/Printers can help an administrator manage authorization that he/she can appropriately give a different level of authorization to each person such as “general user” or “administrator”. Specific MFP/Printer functions can also be restricted on a per user basis. Before gaining access the MFPs/Printers, a user must successfully authenticate by entering a valid login user name and a valid login password, thereby protecting the MFPs/Printers against unauthorized use. Who, when and how often accessed to the MFPs/Printers, can be tracked later based on user access logs.

2.1.1. User Authentication

This function protects information by controlling access to the information after identifying authorized user of MFP/Printer.

This enables to realize access control of asset and protection of asset.

When a login user name and a login password a user enters agreed with the ones that have been registered in advance, the user would be authenticated and then granted access to the MFP/Printer.

Password Policy

Password policy that encourages users to employ strong passwords including minimum length, complexity and a period of validity can be set. The function also rejects passwords, which is not applicable to the password policy. This helps prevent weak passwords set by general users and unauthorized access.

Account Lockout Policy

Account lockout is a function that temporarily lockouts the account when exceeding a predetermined number of login attempts within a predetermined period of time. Retry count (1-10 times) before lockout and a lockout period (1-60 minutes) can be set. When failed login with wrong passwords repeatedly occur more than the preset number of time, the user account will be disabled. The account lockout policy setting highly minimizes successful password cracking attacks on MFP/Printer.

2.1.2. Authentication Mode

TA TRIUMPH-ADLER MFPs/Printers have the following authentication modes.

Local Authentication

The local authentication mode authenticates users based on the user data registered on the local user list on the MFPs/Printers. Only the registered users can access to the MFPs/Printers.

Network Authentication

Network authentication mode authenticates users via an authentication server. Users can login with the user data registered on the authentication server. The servers such as NTLM and Kerberos are provided. The third party server linkage is also available.

Kerberos Authentication

Kerberos authenticates users between a client and an authentication server on a network. This unifies a plurality of servers and user authentication information, and allows users Single Sign On. Communication channels can be encrypted here.

NTLM Authentication

NTLM is used for network login when connecting between MFPs/Printers and the network. The NTLM authentication performs between MFP/Printer and a server using challenge-response mode to refrain from transmitting a non-encrypted password on the network. The challenge data from the server has been encrypted and NTLM hash is used as an encryption key for encryption.

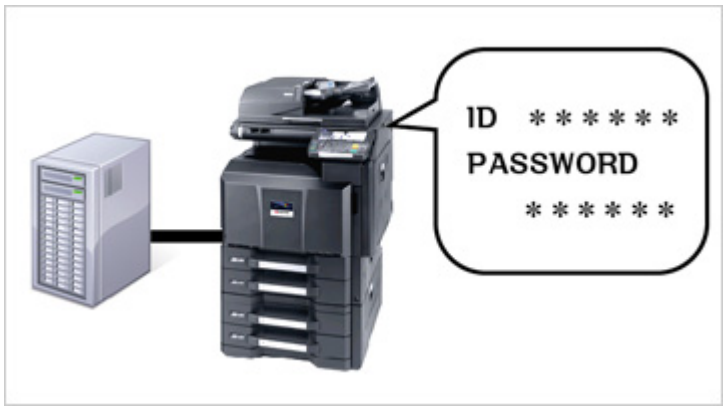

Figure 1

2.1.3. MFP/Printer Login

The following login modes can also be used other than entering a login user name and a login password from an operation panel.

ID Card Authentication (Option)

There are two ways for ID card authentication. One is to login with an ID card only and the other is to hold the ID card near or over a card reader and then enter a password. ID card authentication can be used in Local authentication. *(Figure 2)*

When the ID card information has been registered on the user list of the MFPs/ Printers, an external authentication server, or the third party authentication server in advance, the authenticated user can be granted access to the devices with her/his ID card.

Authentication with an ID card, such as an employee card currently used, enables Department Management and User Management features. Specific functions can be restricted based on the user information associated with the ID cards. *(Figure 3)*

Figure 2

Figure 3

2.2. Authorization

The use of specific functions such as color print, full color copy, send, fax transmission, box storage, external memory storage etc. can be restricted on an authorized user basis. It helps significantly lower the possibility of information leakage from MFPs. According to the various user level authorization, “user”, ”administrator” or “device administrator”, access to settings on the MFP/Printer can also be limited. Some MFPs/Printers have a combined, a two-sided and an EcoPrint restriction features. This may be useful, for example, a user without having an authorization to set “not combine”, has to set “2in1” or more to make copies, otherwise user cannot make copies.

2.2.1. Authorization Mode

MFPs/Printers have the following authorization modes.

Local Authorization

Local Authorization is an authorization function that can be used with a local user list registered on the MFP when performing a local authentication. The usage can be limited by user.

Network Authorization (Group Authorization)

Network Authorization is a process through determination using the group information obtained upon network authentication and the group authorization information stored on the MFPs in advance. Restrictions can be applied based on the respective groups registered in the authentication server. The usage of the MFPs can be limited by the group registered in the server, making the MFPs more secure to be used by the particular group.

Login by Function

Login is restricted by functions; Print restriction, (Color) Print restriction, Copy restriction, (Color) Copy restriction, (Full-Color) Copy restriction or EcoPrint restriction when guest authorization is set. Users who wish to use the functions with login restrictions are required for login authentication. Therefore only limited users registered on the list earlier can use the particular functions. The security can strongly prevent the leakage of information from the TA TRIUMPH-ADLER devices to outside whereas maintaining the user-friendliness.

2.2.2. User Authorization Management

As for the user authorization management, usages of functions are permitted by an only authorized user based on the various authorization levels given to the respective users. User authorization includes Machine Administrator, Administrator, and General User. In addition, some “Administrator”

authorizations can also be given to General Users. Therefore the users who have no authorization cannot illegally use the particular function, which the unauthorized users are not allowed.

2.3. Session Management

Session management is a function that manages a period of time as a session between the time when user login to the MFPs and the time when user logout from the MFPs, after users are authenticated.

The following management functions are available.

Auto Panel Reset

Auto panel reset is a function that automatically logs out, resets the settings and then returns to the default settings when no operation has done after a certain period of time. Users can specify when to perform reset after the last operation. The auto panel reset helps prevent unauthorized access to the MFPs from malicious attacks when the last user failed to logoff the system.

3. Network Security

3.1. Settings for Secure Communication

TA TRIUMPH-ADLER MFPs/Printers can limit communications on a network only from a set range of IP addresses and Port numbers. The powerful Secure Hash Algorithm is also scheduled to be available for TLS server certificates. This algorithm prevents alteration of data, tapping data, and masquerading over a network.

3.1.1. IP Filter Settings

IP filter is a function that restricts network access to the MFPs/Printers by setting ranges of IP addresses or types of protocols. This function specifies the ranges of IP addresses to be permitted to access (and subnet mask combination) and allows only accesses from the clients with IP address set in the specified range. Some permitted communication protocols can be chosen and then set to be active. As for IPv4 and IPv6 support, communications from single PC or communications from multiple PCs, as well as IPP (network protocol for remotely managing print jobs) and HTTP (protocol for transmitting data between web server and web browser) can be set. Thus the specified settings help deny unauthorized access to the MFPs/Printers.

3.1.2. Port Settings

Only the required port numbers are set to be enabled to communicate using protocols such as IPP or SMTP, thereby disabling port numbers which are not set to be enabled.

Protocol	Port No.	Setting	Note
FTP Server	TCP 21	Enable/Disable	FTP server is a protocol for receiving a document.
HTTP	TCP 80	Enable/Disable	HTTP is a protocol that is used when receiving/sending data from a web page between www server and browser.
NetBEUI	TCP 139	Enable/Disable	NetBEUI is a protocol for a small network that is used for file sharing and print services, as well as for receiving a document.
HTTPS	TCP 443	Enable/Disable	HTTPS is a protocol that performs encryption using TLS.
IPP over TLS	TCP 443	Enable/Disable	IPP over TLS is a protocol that combines TLS which encrypts a channel, and IPP which is used for internet printing. In addition, the IPP over TLS can have a valid certificate.
LPD	TCP 515	Enable/Disable	LPD is a printing protocol that is used for printing text files or Postscripts.
IPP	TCP 631	Enable/Disable	IPP is a protocol that controls to send/receive print data via TCP/IP including internet, or print devices.
ThinPrint	TCP 4000	Enable/Disable	ThinPrint is a print technology available in Thin client environment, and also supports TLS.
WSD Scan	TCP 5358	Enable/Disable	Windows Vista WSD is a protocol that enables a MFPs/Printers for a network connection. This also enables users to detect (install) MFPs/Printers device or send/receive data easier. Original documentation image scanned through MFP/Printer can be stored in WSD PC as a file.

WSD Print	TCP 5358	Enable/Disable	Windows Vista WSD is a protocol that enables MFPs/Printers for a network connection. This also enables users to detect (install) MFPs/Printers device or send/receive data easier.
Enhanced WSD	TCP 9090	Enable/Disable	Enhanced WSD takes a procedure for easily connecting the various devices connected to a network, and using. The status of MFP/Printer can be monitored by the status monitor through this port 9090.
Enhanced WSD over TLS	TCP 9091	Enable/Disable	Enhanced WSD (TLS) is a security protocol as well as an enhanced WSD with using TLS. This provides encryption, authentication and safety (Protect against alteration).
RAW	TCP 9100-9103	Enable/Disable	RAW protocol takes different steps, compared to LPR for printing. In general, MFP/Printer uses port number 9100, and also uses SNMP or MIB to configure and monitor printer status.
SNMPv1/v2	UDP161	Enable/Disable	SNMP protocol is used in network management system. Normal communication will be performed using read and write community names.
SNMPv3	UDP161	Enable/Disable	SNMP protocol is used in network management system. Normal communication will be performed using user name and password. Authentication option or encryption option can be used.
DSM Scan		Enable/Disable	DSM (Distributed Scan Management) uses Windows Server 2008 R2 which is used for handling a large amount of user data in a large organization.
FTP Client		Enable/Disable	FTP client is a communication protocol for forwarding a file via a network.
LDAP		Enable/Disable	Address Book on LDAP server is referred as an external address book. FAX number and mail address can be designated as destination.
LDAP over TLS		Enable/Disable	LDAP over TLS is a protocol that uses TLS for encrypting a channel to secure LDAP communication.
POP3		Enable/Disable	POP3 is a standard protocol for receiving e-mails.
POP3 over TLS		Enable/Disable	POP3 over TLS is a protocol that combines POP3 which is used for receiving an email, and TLS which is used for encrypting a channel.
SMTP		Enable/Disable	SMTP is a protocol for sending emails.
SMTP over TLS		Enable/Disable	SMTP over TLS is a protocol that combines SMTP which is used for sending an email, and TLS which is used for encrypting a channel.
SMB Client		Enable/Disable	SMB is a protocol that performs file or printer sharing through a network. SMB Client supports V3.0.
eSCL		Enable/Disable	eSCL is a protocol that is used for remote scan from Ma OS X.
eSCL over TLS		Enable/Disable	eSCL over TLS is eSCL communication protocol using TLS certificate. All eSCL over TLS communications are encrypted.
LLTD		Enable/Disable	LLTD is a protocol for network topology discovery and quality of service diagnostics.

Privet		Enable/Disable	Privet is a protocol that allows discovery of cloud connected devices on the local network, and provides interfaces to get information about the device and perform some actions, such as sending a print job locally.
REST		Enable/Disable	REST is the software architecture of the web application that supports multiple software in a distributed hypermedia system.
REST over TLS		Enable/Disable	REST over TLS is REST communication using TLS certificate. All REST over TLS communications are encrypted.
Bonjour		Enable/Disable	Bonjour is a networking technology that allows users to automatically discover devices.
VNC		Enable/Disable	Virtual Network Computing (VNC) is a remote-control software that uses RFB protocol to control a GUI of a device remotely over a network connection.
VNC over TLS		Enable/Disable	VNC over TLS is a remote-control software that uses RFB protocol to control a GUI of a device remotely over a network connection between a client PC and the device through TLS.
Enhanced VNC over TLS		Enable/Disable	Enhanced VNC over TLS is TA TRIUMPH-ADLER's own remote-control software that uses RFB protocol to access a device by One Time Password (OTP) and control a GUI of the device remotely, which only an authorized administrator is allowed. The OTP-based secure access to the device increase the security strength of access control.

3.1.3. Secure Hash Algorithm Settings

The powerful Secure Hash Algorithm used in the TLS encryption technology is scheduled to be supported for self-issued certificates and the CSR certificate. This function can also be used for user environments that will adopt secure measures.

3.2. Authentication Protocol

Authentication protocol is a communication protocol that aims to achieve authentication for secure communication. TA TRIUMPH-ADLER MFPs/Printers support IEEE802.1x network authentication, SMTP authentication and POP before SMTP authentication protocol with email sending capability. This prevents masquerading.

3.2.1. IEEE802.1x

IEEE802.1x is a standard regarding port-based authentications defined by IEEE (Institute of Electrical and Electronics Engineers). This protocol allows communications only to authorized users (authenticated devices) when connecting to the network, and thus prevents unauthorized devices from connecting to network. As you can see from the above, TA TRIUMPH-ADLER devices support the IEEE802.1x which would not allow unauthorized access by unauthenticated clients to the network, thereby preventing unauthorized disclosure of information. The TA TRIUMPH-ADLER MFPs/Printers employ four types of authentication modes as described below.

PEAP-TLS/PEAP (Protected Extensible Authentication Protocol-Transport Layer Security)

The client is authenticated based on the ID and certificate and the certificate of authentication server is checked at the same time.

EAP-PEAP (Extensible Authentication Protocol-Protocol Extensible Authentication Protocol)

The client is authenticated based on the ID/password and only the common name of the authentication server certificate is checked.

EAP-FAST (Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling)

EAP-FAST is an IEEE802.1.x/EAP authentication method developed by Cisco System, Inc. Mutual authentication is performed for the client and authentication server based on the user ID and password and PAC (Protected Access Credential) establishes a tunnel for the user based on the unique shared secret key.

EAP-TTLS (Extensible Authentication Protocol-Tunneled Transport Layer Security)

The client is authenticated based on the user ID and password, and also authentication server is authenticated based on the electric certificate.

As for EAP-TLS, Client and server electric certificates are required for authentication, whereas for EAP-TTLS, the user ID and password are used instead of a client certificate. This makes EAP-TTLS easier to introduce compared to EAP-TLS. Electric certificates are used to prove the validity of authentication server. Therefore, it helps improve more secure and trusted communications.

3.2.2. SMTP Authentication

SMTP authentication is a function that permits to send an e-mail only when the ID and password are successfully authenticated on SMTP server. The function prevents unauthorized users to send e-mails through the SMTP server by limiting access to the SMTP server.

3.2.3. POP before SMTP

POP before SMTP performs POP authentication before sending e-mails from the SMTP server. The e-mails can be sent within the specified period after completion of POP authentication. POP authentication before sending an e-mail prevents masquerading.

3.3. Communication Channel Protection

Communication channel protection is to ensure secure protection of Network communication channel. Depending on purposes or encryption schemes, the variety of protocols is available. TA TRIUMPH-ADLER MFPs/Printers support the following protocols as described, thereby effectively protecting data against alterations or leakage via the Network.

3.3.1. SNMP v3

SNMP is a standard protocol that monitors and controls devices connecting to the network. Moreover, SNMPv3 provides ability to protect data confidentiality through authentication and encryption.

3.3.2. IPv6

IPv6 is a new IP protocol compared to IPv4. TA TRIUMPH-ADLER has obtained the IPv6 Ready Logo up to the Phase2. IPv6 support, which is available in the TA TRIUMPH-ADLER MFPs/Printers, can connect to the router, and use basic control protocol like ping. In addition to the above-mentioned basic connections, a more secure connection is ensured by implementing rigorous security measures.

3.3.3. IPSec

IPSec is a protocol with a functionality that protects data in transit from tapping or alteration by encrypting respective IP packets. To send/receive data using IPSec, IPSec-enabled PC, is connected to the network, and also IPSec-enabled MFPs/Printers are connected to the network, and then both of them are set to be IPSec capabilities-enabled. Encryption using IPSec is applied to print data sent from a PC to a MFP/Printer, and scanned data to be sent from a MFP to a PC. Thus IPSec supports more secure exchange of data. In addition, the strong Secure Hash Algorithm can be used for communication between a pair of hosts (host-to-host).

3.3.4. TLS

TLS is a system to encrypt data for transmissions such as Web access or others, and also has a functionality to mutually check if communication destination parties are reliable for mutual communications. TA TRIUMPH-ADLER MFPs/Printers support TLS encryption protocols including TLS1.0, TLS1.1 and TLS1.2, and thereby preventing alteration of data or tapping data on network. In addition, the strong Secure Hash Algorithm can be used for communication between a server and a client. The following are TLS encryption protocols.

IPP over TLS

IPP over TLS is an internet printing protocol that acts as a combination of IPP, which is for exchanging print data on the internet or TCP/IP network, and TLS, which is for encryption of a communication channel. This allows users to safely send print command to the MFPs/Printers through the network.

HTTP over TLS

HTTP over TLS is a protocol that acts as a combination of HTTP, which is for sending/receiving data to and from web browser or others on the TCP/IP network, and TLS, which is for encryption of a communication channel. In transmitting data between a PC and a MFP/Printer, this mitigates risks of alteration and leakage of data by unauthorized users.

FTP over TLS

FTP over TLS is a protocol that acts as a combination of FTP, which is used for forwarding a file on the TCP/IP network, and TLS, which is for encryption of a communication channel. When sending scanned data from a MFP/Printer using the FTP protocol, TLS encryption is applied to the channel. FTP over TLS enables more secure transmissions.

ThinPrint over TLS (Option)

ThinPrint over TLS is a protocol that acts as a combination of ThinPrint, which is for bandwidth control and print job compression, and TLS, which is for encryption of a communication channel. Thus this provides secure and fast printing environment.

SMTP over TLS

SMTP over TLS is a protocol that acts as a combination of e-mail transmission, and TLS, which is for encryption of a communication channel between a server and a MFP/Printer. This prevents masquerading, tapping or modifying data in transit.

POP3 over TLS

POP3 over TLS is a protocol that acts as a combination of POP3, which is an email reception protocol, and TLS, which is for encryption of a communication channel between a server and a MFP/Printer. This prevents masquerading, tapping or modifying data in transmit.

3.4. Wi-Fi Direct (Option/Standard for KDA only)

Wi-Fi Direct devices can connect to each other without having to go through an access point. That is, you don't need to use your router. This is because Wi-Fi Direct devices establish their own ad-hoc networks as and when required. The networks operate in a security domain that is independent from any infrastructure network. Wi-Fi Direct uses Wi-Fi Protected Setup that enables users to easily set the connection and WPA2-PSK (Personal). This prevents unauthenticated device connections to the independent network provided by MFP/Printer thus protecting MFP/Printer against unauthorized use.

3.5. E-mail Send/Receive Restriction Function

When sending/receiving emails, TA TRIUMPH-ADLER system provides the email send/receive restriction as described below, thereby preventing sending wrong emails or malicious attacks by unauthorized users.

3.5.1. E-mail Send Destination Restriction Function (Permission/Rejection)

Email send destinations can be restricted using the email send restriction function for permission or rejection. Permitted send destination domains are registered in advance so that emails can only be sent to the permitted destination domains registered earlier. Rejected send destination domains are also registered in advance so that emails to the rejected destination domains registered earlier would be rejected. This prevents sending wrong emails.

3.5.2. E-mail Sender Restriction Function (Permission/Rejection)

TA TRIUMPH-ADLER MFPs/Printers have a function to print files attached to e-mails. E-mail reception can be restricted through the email sender restriction function based on presetting. Permitted sender domains are registered in advance so that emails can only be received from the permitted sender domains registered earlier. Rejected sender domains are also registered in advance so that incoming emails from the rejected sender domains registered earlier would be rejected. Thus, security measures are implemented against malicious attacks such as spam emails.

4. Stored Data Protection

4.1. Data Protection

The sensitive or confidential information stored in HDD or SSD must not be leaked from MFPs/Printers. TA TRIUMPH-ADLER implements security protection measures against the stored information through functions as described below, and so ensures that our customers can securely use TA TRIUMPH-ADLER MFPs/Printers.

4.1.1. HDD/SSD Encryption

HDD/SSD encryption function is a security function that encrypts documents, user settings and device information to be stored on HDD or SSD inside MFP. Encryption is applied to the data with using the 128-bit and 256-bit AES (Advanced Encryption Standard: FIPS PUB 197) algorithm. FIPS 140-2-certified HDD can be included in the MFPs/Printers. Even though the HDD or SSD is removed from the MFP by a malicious person, the sensitive or confidential information stored in the HDD or SSD would not be disclosure.

4.1.2. HDD Overwrite-Erase

HDD overwrite-erase function is another security function that disables the third persons to read various data such as user settings, device information and image data and others stored on the HDD.

Scanned data is temporarily stored in the HDD and then outputted at the MFP. Users also can register various settings. Actual data still remain in the HDD until the data is overwritten with other data, even after output or deletion of the data by users. So there is a possibility that the remaining actual data can be restored using special tools and others, and this could cause leakage of information. The HDD overwrite-erase function is configured to overwrite the actual data of the outputted or deleted data with meaningless data so that the actual data cannot be restored.

HDD overwrite-erase process is performed automatically. So no manual operation is necessary. HDD data is immediately overwritten even when respective jobs are canceled during operation or right after entire job has finished.

The following two overwrite methods are available for the HDD overwrite-erase function and are available depending on the MFP/Printer model.

◆ Once Overwrite

The once overwrite method overwrites unnecessary data once with a fixed value which makes it difficult to restore or recover the data.

◆ 3-time Overwrite (A)

The 3-time overwrite (A) conforms to the U.S. Department of Defense DoD 5220.22-M method and overwrites the unwanted data of the HDD. The unwanted data is 1) overwritten with a fixed value, 2) overwritten with the value's complement, 3) overwritten with random data. Finally, the last pass is verified. It would be difficult to restore the completely erased data. *(Figure 4)*

When overwriting-erasing bulk data, the 3-time overwrite (A) method may take longer compared to the once overwrite method.

Figure 4

4.1.3. Trusted Platform Module (TPM)

Trusted Platform Module (TPM) is included in TA TRIUMPH-ADLER MFPs that can protect sensitive information such as image data and certificates. An encryption key used for encrypting the HDD is encrypted by a root encryption key contained in the TPM. The certificates are encrypted by the same root encryption key. The root encryption key is rigorously protected within the TPM so that it cannot be disclosed outside of the security chip. The HDD encryption key and the root encryption key are saved separately. Even if the HDD is removed from the MFP, data stored on the HDD cannot be leaked and is securely protected.

4.1.4. Security Data Sanitization

At the MFPs/Printers' lease end or device end of life, in case that private, sensitive or confidential data still remain inside the MFPs/Printers, it could cause the residual data leakage to outside. To refrain from leaking the data, the "security data sanitization" is a security function that completely sanitizes the data retained inside the devices or the residual data, using the 3-time overwrite (A)_ DoD 5220.22-M, the 7-time overwrite (A)_DoD 5220.22-M ECE, or the 7-time overwrite (B)_BSI/VSITR method as described below. (depending on the MFP/Printer model).

◆ 3-time Overwrite (A)

The 3-time overwrite (A) conforms to the U.S. Department of Defense DoD 5220.22-M method and overwrites all data areas of the HDD. All data areas are overwritten with a fixed value, then overwritten with the complement of the fixed value, then overwritten with random data, and lastly, the data is verified. So even with a sophisticated restoration process, it would be difficult to restore the completely erased data. The data is overwritten three times, and then the data is verified once.

◆ **7-time Overwrite (A)**

The 7-time overwrite (A) conforms to the U.S. Department of Defense DoD 5220.22-M ECE method and overwrites all data areas of the HDD. DoD 5220.22-M ECE is an extended variant of DoD 5220.22-M. All data areas are overwritten twice by the DoD 5220.22-M method and once with random data. So even with a sophisticated restoration process, it would be extremely difficult to restore the completely erased data. The data is overwritten seven times.

◆ **7-time Overwrite (B)**

The 7-time overwrite (B) conforms to the VSITR method defined by the German Federal Office for Information Security (BSI) and overwrites all data areas of the HDD. All data areas are overwritten with zero (0x00) and then with the fixed value (0xff). This will be performed three times repeatedly. Then the data areas will be overwritten with the fixed value (0xAA). So even with a sophisticated restoration process, it would be extremely difficult to restore the completely erased data. The data is overwritten seven times.

When overwriting-erasing bulk data, the 7-time overwrite (A) and (B) methods may take longer compared to the 3-time overwrite (A) method.

The security data sanitization function has the following features: a sanitization schedule timer that can be set to be sure to conduct sanitization at the scheduled time; notification prior to sanitization that notifies an administrator and a service person prior to the sanitization; a sanitization completion report (including the sanitized contents and the date of sanitization) that automatically prints upon completion of the data sanitization; a system lock after sanitization that disables users to use the MFPs/Printers after performing the sanitization. An administrator can set and execute the features. So device settings can revert back to factory default settings.

4.2. Access Restriction

"User Box", "Job Box" and "FAX Box" that can store data can be created inside MFPs. Access to the data saved in the boxes can be restricted.

4.2.1. User Box

Users can create the "User Box" to store data in MFPs. Box usage restriction, data retention period and password can be set for the respective boxes. *(Figure 5)*

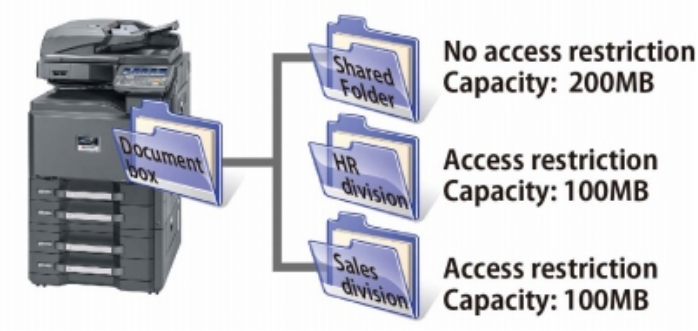

Figure 5

Box Password

User who can gain access to a box can be restricted with a password. User is required to enter an appropriate password which is allowed to be set up to 16 characters (using the variety of characters including upper case letters, lower case letters, digits and special characters) in advance.

Box Usage Restriction

Box capacity usage can be restricted to manage HDD capacity.

Owner Setting

User box can only be accessed by a user who has registered as an owner for his/her own user box, and so cannot be accessed by unauthorized user. "Shared box" that is whether the box is shared or not can be set. If shared, even user who is not set as an owner can access to the box. Considering ease of use, the box can be efficiently protected against unauthorized access. Thus security is appropriately maintained.

Document Retention Period

After a certain period of time, document data stored can be automatically erased so that it does not have to be kept for long period of time. Therefore there would be only fewer chances for data leakage.

Timing of Deletion

Once print job is finished, document data stored in a box will be automatically deleted. So, the data deletion will not be forgotten. This prevents the data from being viewed by unauthorized third person.

4.2.2. Job Box

Data for "Private Print", "Quick Copy", "Proof and Hold" and "Stored Job" can be stored in a Job Box, however the box can be neither deleted nor created by users. The box can be PIN code-protected. Thus access to the box is restricted. *(Figure 6)*

Figure 6

Automatic Deletion of Temporary Document Data Storage

Data temporarily saved in a box for “Private Print”, ”Quick Copy” and “Proof and Hold” can be automatically deleted after the data has been stored for a specified time period. The data is kept only for a required period of time. So, the risk of data disclosure is highly reduced.

4.2.3. FAX Box

A box that stores fax received data, located inside MFP, is called “FAX Box”. The fax received data can be stored in the fax box using a memory forward function. Also, the fax received data will be assigned to the respective boxes based on sender sub addresses or fax numbers so that prompt confirmation on important document can be easily made. The fax received data can be confirmed on a panel of MFP. Wanted fax can be printed out right away, whereas unwanted fax can be deleted. *(Figure 7)*

Figure 7

BOX Password

User who can gain access to a box can be restricted with a password. The user is required to enter an appropriate password which is allowed to be set up to 16 characters (using a variety of characters including upper case letters, lower case letters, digits and special characters) in advance.

Owner Setting

A box can only be accessed by a user who has registered as an owner for his/her own box, and so cannot be accessed by unauthorized user. “Shared box” that is whether the box is shared or not can be set. If shared, even user who is not set as an owner can access to the box. Considering maintaining conveniences, the box can be efficiently protected against unauthorized access. Thus security is appropriately maintained.

Timing of Deletion

Once the print job is finished, received data saved in a box can be automatically deleted. Otherwise, keeping data longer than necessary could create risks. Timely deletion would help maintain efficient security condition.

5. Print Security

5.1. Secure Print

Secure print is a print function for MFPs/Printers. The secure print function can be used for printing company confidential documents or personal documents to refrain from leaving unattended printed documents with others or viewing them by other third people at the device.

5.1.1. Private Print

Private print is a function that once holds a print job in MFPs/Printers sent from a PC until user enters his/her appropriate password through an operation panel of the MFPs/Printers. Application software requires the user to set an access code in the printer driver when sending a print job from the PC, and then the user is required to enter the appropriate access code from the panel of the device when printing a document. After printing is finished, the data will be erased. Even if main power switch is turned off before printing, the data will still be erased. This helps maintain relatively high security on the device.

5.2. Unauthorized Copy Prevention

When coping, the following functions can prevent unauthorized copy by enhancing document security capabilities.

5.2.1. Text Stamp/Bates Stamp

Since text stamp function that shows importance of documentations at first sight is available, users can choose a few stamps such as “Confidential”, “Do not duplicate” “Privacy”, depending on a variety of stamps availability. Users even can edit the text stamp as they like. The bates stamp function “Serial Number” will print the serial number of the machine used for the print-out and the function “Numbering which will print page numbers in sequence onto the printed documents. In addition, the function “Date” and “User Name” is also available.

5.2.2. Security Watermark

Document material can be embedded with a security watermark pattern or text. When printed material embedded with the pattern is copied, the security watermark pattern will be visible. This clearly indicates that the unauthorized copy was made. *(Figure 8)*

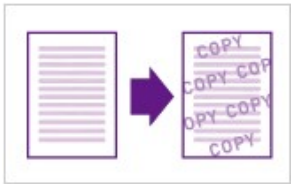

Figure 8

6. FAX Security

6.1. FASEC (For Japan Only)

FASEC is a security guideline for facsimile communication enacted by Communication and Information network Association of JAPAN (CIAJ). The FASEC logo is applied to facsimile on MFPs, which has fax functions to meet the functional requirements that are to prevent; wrong transmission, wrong connection by dial tone detection, leaving unattended received fax sheets as well as to confirm if data is properly transmitted. TA TRIUMPH-ADLER fax security functions are complied with the functional requirements, and thus TA TRIUMPH-ADLER has obtained the logo for its MFPs.

6.2. FAX Encrypted Communication

This is a communication method that original (data) is encrypted prior to sending at a sending side. So, image data in transit cannot be tapped by third persons. Thus, there is no way for the third persons to view and learn about the contents. The incoming data is first decrypted and then printed at a receiving side. This is relatively effective communication method when transmitting sensitive and confidential documents that must not be disclosed to them.

This is only available between TA TRIUMPH-ADLER devices which support the same encrypted communication function.

The same encryption key is used for encrypting/decrypting the original communication data at the sending and receiving side (device). When the keys are not identical at the sending and receiving side (device), encrypted communication cannot be performed. Therefore, the two parties (i.e. sending and receiving side) have to mutually determine and register the same encryption key, respectively in advance prior to encrypted communication.

6.3. Send/Receive Restriction

This is a function that enables the device to send/receive fax only if the predetermined communication condition (i.e. permitted fax number and permitted ID number) are met. The function enables to restrict fax destination for communication. When reception restriction is applied to a rejection list, inbound fax sent from a sender registered on a rejection fax number list as well as who do not register their local fax number will be rejected. As for fax transmissions, faxes can only be transmitted to destinations registered on a permitted telephone list and an address book.

6.4. Wrong Transmission Prevention

To prevent important documents from being transmitted to the wrong destinations, users will be prompted to enter recipient's fax numbers twice prior to fax transmissions. The wrong transmission prevention function can be set for an address book, ten-keys and speed dial. In addition, the function prohibits recalling address destinations. The previous destination is not maintained and thus prevents transmitting another document to the previous send destination. This is also effective in preventing information leakage because the destinations cannot be viewed by other people. Furthermore, the destination information will be deleted right after logout when user authentication is on.

6.4.1. Confirmation Entry

Users will be prompted to enter the same fax number twice for confirmation when they wish to send a fax by specifying the fax number to directly enter with numeric keys. The send destination will be enabled only when the same fax number entries twice are confirmed. This prevents wrong transmissions by pressing wrong keys. The function can be set by users.

6.4.2. Prohibition of FAX Number Direct Entry with Numeric Keys

Direct entry with numeric keys through the operational panel for fax transmission can be restricted. This function allows users to transmit faxes only to the send destinations registered on a destination list. So users will not be able to send faxes except the recipients listed on the address book and one-touch keys. This helps prevent wrong transmissions caused by entering wrong fax numbers and unauthorized usage.

6.4.3. Destination Confirmation Prior to Transmission

Upon pressing [Start] key, the send destinations will be displayed on the screen for users to check when the destination confirmation prior to transmission function is set. The completion confirmation key would not be enabled unless all the destinations had been displayed on the screen. Since users can re-confirm the destinations before sending faxes, the function will be able to help prevent wrong transmissions.

6.5. Use Prohibition Time

This is a security function with the capability to set a time period which prohibits printing received faxes. When the use prohibition time is set, all operations including printing, copy, print, received mail or USB, transmission and network fax transmission as well as printing fax in the specified period will be prohibited. This is PIN code-protected and can also be temporarily canceled. This prevents unauthorized use of MFPs like printing data during night time with less people.

6.6. Sub Address Communication

Sub Address Communication is a communication function that sends/receives data with a sub address and a password, which are complied with the recommendation from ITU-T (International Telecommunication Union Telecommunication Standardization Sector). Sub address communication function enables communications with other company's machines as well, such as confidential communication (i.e. communication to send to the certain box of the receiving machine) or polling communication (i.e. communication to receive the original on the sending machine through operation from the receiving machine) which used to be available only for TA TRIUMPH-ADLER machines. When the sub address communication function is used, for example the incoming data will be saved in the sub address box. So, the function will be able to help perform relatively secure communications.

6.6.1. Sub Address Confidential Transmission (Send/Receive)

After sub address confidential box is created in the recipient machine, an important document, which must not be disclosed to other people, can be sent to the box with keeping confidentiality by identifying a sub-address and a password. The received document is saved in the box registered in advance without printing immediately upon reception. Thus the received data can be printed without being viewed by anyone.

6.6.2. Sub-Address Bulletin Board Transmission (Send/Receive)

When recipient machines support the sub address bulletin board transmission function, user's documentation will be securely transmitted without information leakage.

6.7. Memory Forward

With this function, the received images can be forwarded to other fax machines or computers, or printed as well, upon fax reception. When the forward setting is on, all incoming images will be able to be forwarded to the predetermined addresses (destinations). This can be applied to another fax, sending mail, SMB (sendfile) and FTP sending. Also, received images can be forwarded to the box being set in MFP, and then stored. This prevents unattended (received) fax sheets left on the tray of the device. *(Figure 9)*

Figure 9

6.8. Security Measures Against Unauthorized Access

The fax function and network function are structurally separated. Incoming data via a telephone line are processed by the fax function. The structure prevents unauthorized access from the telephone line into the network via a fax function, which operates on a MFP.

7. Send Security

7.1. Destination Confirmation Prior to Send

Users can confirm on the send destination (i.e. address numbers) and subject on the screen before sending. Thus, this helps prevent sending to the wrong address. The information can always be shown on the operational panel prior to sending as user set.

7.2. Prohibition of Broadcast Transmission

Broadcast Transmission is a function that transmits the same document to the plural destinations by one-time operation. This function enables administrators to set prohibition or permission. When setting prohibition, the group including 2 or more send destinations cannot be selected. This prevents transmission to the unintended destinations caused by unintentionally adding send destinations to the group.

7.3. New (Address) Destination Entry

Direct entry through the operational panel is restricted so that the destinations registered earlier on the destination list such as an address book or one-touch keys, can only be the designated destinations. This effectively prevents unauthorized use or wrong sending caused by wrong fax number entry.

7.4. Encrypted PDF

The Encrypted PDF function enables users to choose PDF file or high-compressed PDF for the file format, and securely protects the scanned data by encrypting and setting password. Restriction can be applied when opening, printing, or modifying the received PDF file by entering the correct password.

7.5. FTP Encrypted Send

The FTP Encrypted Send is performed using TLS to encrypt the communication channel. Thus data in transit maintains secure. This can highly minimize risks of modifying data in transit or wiretapping.

8. Device Management

8.1. Job Management

Information concerning jobs in queue or logs can be checked at the device. Four types of status including “Print Job”, “Send Job”, “Stored Job” and “Reserved Job”, and three types of job log including “Print job”, “Send Job” and “Stored Job” can be available. Detailed information for specified job like user name, time and destination, can be referred and used to help trace as needed. Also, when printing job using printer driver, whether or not the file is used for job name, can be set. *(Figure 10)*

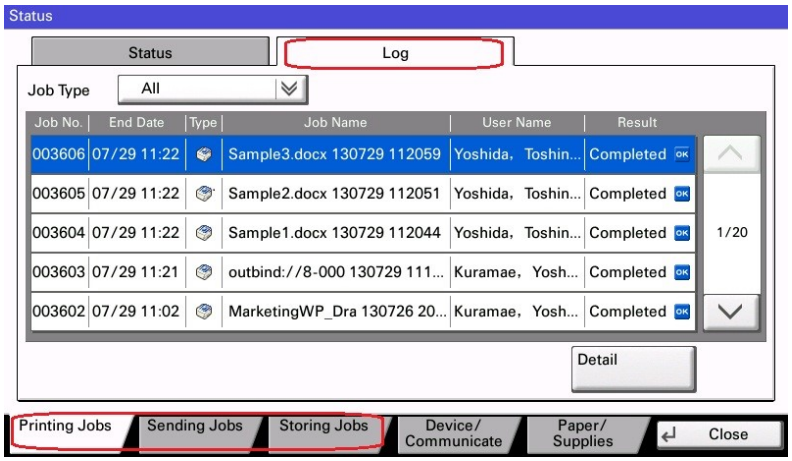

Figure 10

8.1.1. Authorization to Refer Job Information

The Job Log Reference Screen can be switched corresponding to the user’s authorization. Authorization to refer to job information and fax transmission log are set for the detailed job status information and job log, respectively. When user authentication is on, only user can view and check his/her own job log information. All job jog information is displayed on the screen after login as an administrator.

8.2. Audit Log

Audit log for MFPs/Printers can be obtained. A record of operating the device with user name, date & time and its result can be checked. Audit log includes login log, device log and security communication error log. By referring to the log, the administrator of the MFPs/Printers can check if the device is securely used or not exposed to risks.

8.2.1. Login Log

User authentication login log can be stored. In the event of unauthorized operation, alteration or leakage of documentations in the MFPs/Printers, login log is used to investigate and help trace the unauthorized access.

8.2.2. Device Log

FW update and setting changes on MFPs/Printers can be logged. The contents being changed from system menu by the administrator will be recorded as well.

8.2.3. Security Communication Error Log

Administrator can confirm if the network communication is properly performed by checking the security network communication error log. In the event that a record of frequent communication failures is found, the potential unauthorized access will be able to be investigated.

8.3. Log Management

The Log Management helps manage audit log and job log, and will be used to help trace the potential source of the security incidents.

8.3.1. Send Job Log (e-mail address)

The respective logs can be sent by e-mail to the e-mail address specified by the administrator when the number of the logs reaches a predetermined number.

8.4. Integrity Verification of the Security Functions

The following functions are used to verify the integrity of the security functions on our products.This is used to verify if the execution modules of the security functions have not been altered and have been properly working. Similarly, data integrity that the security functions use can be verified.

8.4.1. Digitally-Signed Firmware

Digital signature is attached to the firmware to ensure its validity. The firmware controls the operation of MFPs/Printers. The digitally-signed firmware prevents alteration by malicious persons. MFPs/Printers can be protected against damage and unauthorized use as stepping stones for intrusion into networks.

8.4.2. Secure Boot

Secure Boot is a feature that makes sure that an MFP starts up with using the authorized firmware before execution. Firmware validity can be verified by applying a digital signature to the firmware. When the MFP starts up, the firmware is deployed on the RAM. At this time, it is confirmed that the hash value of the firmware uploaded to the MFP and the hash value created from the signature are the same. Even if a malicious person creates unauthorized firmware, it cannot pass through the validity verification using the digital signature. Therefore, even if a firmware is altered by a malicious person, it can never be executed. The Secure Boot prevents the destruction of the devices by using the MFP as a stepping stone.

8.4.3. Run Time Integrity Check (RTIC)

Run Time Integrity Check is a feature that regularly verifies if the validity of the firmware is maintained during the operation of the MFP without altering the firmware deployed on RAM after the MFP starts up. Even if the firmware is maliciously re-written, it can be detected and a warning is issued as a system error. RTIC can be expected to be more effective as a security measure against firmware alteration when used with the Secure Boot feature.

8.5. Usage Restriction

The following usage restrictions can be applied to the TA TRIUMPH-ADLER MFPs/Printers. Since operations on the MFPs/Printers can be restricted, access to data stored on the MFPs/Printers will be able to be restricted as well.

8.5.1. Interface Block

Access through the device's interface such as USB device, USB host, Optional Interface (Slot 1) and Optional Interface (Slot 2) can each be blocked. Network interface can be restricted on a protocol basis.

8.5.2. USB Storage Class Logical Block

When a USB memory is connected to a USB port of MFPs/Printers, risks for data leakage or unauthorized access to data on the MFPs/Printers can exist. Administrator can enable the USB storage class feature to be turned off (disabled), but still allows using ID card reader connected to a USB host interface of the MFPs/Printers. On the other hand, TA TRIUMPH-ADLER MFPs/Printers have the feature that can restrict usage for the USB memory, even if the USB memory is inserted into the USB host interface of the MFPs/Printers. This prevents data leakage from the USB interface via USB memory as well as viruses from spreading.

8.5.3. Operational Panel Lock

Operation through the operational panel of MFPs/Printers can be restricted. Partial Lock function has three stages that are; setting concerning input/output through the panel, setting concerning job execution and setting concerning papers. Settings, which are associated with prohibition level that administrator wishes, are enabled. The operational panel lock has ability to prohibit a system menu operation and a job cancelation operation. This prevents unauthorized operations on MFPs/Printers