IF IT WORX, IT'S UTAX

Security White Paper

für UTAX MFPs & Drucker

Version 01/2024

23. Januar 2024

1. Einführung

Multifunktionsgeräte (MFPs) und Drucker von UTAX werden standardmäßig in ein Betriebssystem integriert. Wie bei einem PC lässt sich in einem MFP/Drucker eine Festplatte oder SSD installieren. MFPs/Drucker in Büroumgebungen verarbeiten verschiedene Arten sensibler Daten. Darum sind MFPs/Drucker diversen aktuellen Bedrohungen ausgesetzt, dazu gehören unerlaubte Zugriffe auf Geräte über ein Netzwerk, das Abfangen oder Verändern von in einem Netzwerk übertragenen Daten oder Datenverluste von einer Festplatte. UTAX stellt Kunden auf seinen MFPs/Druckern unterschiedliche Sicherheitsfunktionen zur Verfügung. Wir implementieren kontinuierlich proaktive Sicherheitsmaßnahmen zur Abwehr dieser Bedrohungen, damit unsere Kunden die MFPs/Drucker von UTAX sicher nutzen können. Zudem hat UTAX die Zertifizierung Common Criteria (bekannt als ISO15408) erhalten, mit der objektiv festgehalten wird, ob Sicherheitsfunktionen beim Kunden vom Drittanbieter richtig ausgeführt werden. Diese Prüfung umfasst auch ein strenges Verfahren für Produktdesign, Herstellung und Lieferung. UTAX-Produkte beinhalten die erforderlichen Sicherheitsfunktionen und Leistungsmerkmale und wurden zertifiziert, da sie mit IEEE 2600.1 konform sind. Hierbei handelt es sich um einen internationalen Sicherheitsstandard für Druckgeräte, der 2009 in Kraft getreten ist. UTAX Produkte werden künftig mit dem Protection Profile für Kopiergeräte (kurz HCD-PP) konform sein und nach dessen Sicherheitsanforderungen zertifiziert. Dies ist ein Kriterium, welches bei der Auftragsvergabe an Regierungen von den MFPs zu erfüllen ist. Außerdem ist auf UTAX-Geräten ein FIPS-140-2 / FIPS-140-3*1 zertifiziertes Verschlüsselungsmodul installiert, das den Sicherheitsstandard des amerikanischen National Institute of Standards and Technology (NIST) erfüllt. UTAX wird die Sicherheit weiter erhöhen, wenn neue Standards und Technologien eingeführt werden, mit denen sich unsere Geräte noch besser schützen lassen.

*1: Die FIPS 140-3-Zertifizierung für das Modul befindet sich in der Prüfungsphase.

Dieses Dokument richtet sich an Mitarbeiter der Vertriebsgesellschaften von UTAX sowie an lokale Händler und Kunden. Es informiert darüber, wie auf unseren MFPs/Druckern installierte Sicherheitsfunktionen vor Bedrohungen schützen und für maximale Sicherheit sorgen. Wir hoffen, dass dieses Dokument im Rahmen der Vertriebs- und Kundendienstaktivitäten von UTAX sowie von unseren Kunden gründlich genutzt wird.

In diesem Dokument sind alle Funktionen zur Erhöhung der Datensicherheit beschrieben, die von UTAX Drucker und MFP unterstützt werden. Es werden allerdings nicht alle Funktionen von allen Systemen unterstützt. Für nähere Informationen nutzen Sie bitte die jeweilige Bedienungsanleitung.

Hinweis: Technische Änderungen und Irrtümer vorbehalten.

2. Identifizierung, Authentifizierung und Autorisierung

2.1. Identifizierung und Authentifizierung

Die Identifizierung und Authentifizierung ist ein wichtiges Verfahren, mit dem überprüft wird, ob ein Benutzer dazu berechtigt ist, auf ein Gerät zuzugreifen oder es zu verwenden. Benutzer müssen Zugangsdaten für die Anmeldung eingeben (wie einen Benutzernamen und ein Kennwort). Der Benutzername dient dabei der Identifizierung des Benutzers, das Kennwort muss geheim sein. (Abbildung 1)

Zur Nutzung der Identifizierungs- und Authentifizierungsfunktion müssen Benutzer zunächst mit einem Benutzernamen und Kennwort bei ihrem MFP/Drucker registriert werden. So können ausschließlich Benutzer, die sich registriert haben, auf den MFP/Drucker zugreifen. MFPs/Drucker von UTAX helfen Administratoren dabei, Autorisierungen zu verwalten. So können sie einzelnen Personen individuelle Autorisierungsstufen zuweisen (z. B. „ Benutzer“ oder „Administrator“). Bestimmte MFP-/Druckerfunktionen lassen sich auch auf einzelne Benutzer beschränken. Bevor Benutzer auf MFPs/Drucker zugreifen können, müssen sie sich zunächst authentifizieren, indem sie einen gültigen Anmeldenamen sowie ein gültiges Kennwort eingeben. So werden MFPs/Drucker vor einer nicht autorisierten Verwendung geschützt. Mithilfe von Benutzerzugriffsprotokollen lässt sich verfolgen, wer wann und wie oft auf MFPs/Drucker zugegriffen hat.

2.1.1. Benutzerauthentifizierung

Mit dieser Funktion werden Daten geschützt, indem der Zugriff auf Informationen nach der Identifizierung eines autorisierten Benutzers des MFP/Druckers kontrolliert wird.

Ist die Benutzerauthentifizierung aktiviert, ist die Zugangskontrolle aktiv und eine Einschränkung der Funktionen des MFPs möglich.

Wenn Benutzername und Kennwort, die ein Benutzer eingibt, mit den zuvor registrierten Daten übereinstimmen, wird der Benutzer authentifiziert und erhält Zugriff auf den MFP/Drucker.

Kennwortrichtlinie

Die Kennwortrichtlinie fordert die Benutzer auf, sichere Kennwörter zu verwenden, die eine Mindestlänge und eine bestimmte Komplexität aufweisen, wobei die 200 häufigsten Kennwörter abgelehnt werden und eine Gültigkeitsdauer festgelegt wird. Die Funktion lehnt auch Kennwörter ab, die nicht in die Kennwortrichtlinie passen. Dies trägt dazu bei, schwache Passwörter sowie unbefugten Zugriff zu verhindern.

Richtlinie zur Kontosperrung

Bei der Kontosperrung handelt es sich um eine Funktion, mit der ein Konto zeitweise gesperrt wird, wenn eine bestimmte Zahl an Anmeldeversuchen in einem vordefinierten Zeitraum fehlschlägt. Dabei lassen sich die Zahl der Versuche (1 bis 10) vor der Sperrung sowie eine Sperrdauer (1 bis 60 Minuten) festlegen. Wenn eine Anmeldung aufgrund falsch eingegebener Kennwörter häufiger fehlschlägt, als dies im vordefinierten Zeitraum festgelegt ist, wird das Benutzerkonto deaktiviert. Mit den Einstellungen für die Richtlinie zur Kontosperrung lässt sich das Risiko der Entschlüsselung von Kennwörtern bei MFPs/Druckern minimieren.

2.1.2. Authentifizierungsmodus

MFPs/Drucker von UTAX beinhalten folgende Authentifizierungsmöglichkeiten:

Lokale Anmeldung

Beim lokalen Anmeldungsmodus werden Benutzer anhand der Benutzerdaten authentifiziert, die in der lokalen Benutzerliste von MFPs/Druckern aufgeführt sind. Erst jetzt können registrierte Benutzer auf die MFPs/Drucker zugreifen.

Netzwerkauthentifizierung

Im Netzwerkauthentifizierungsmodus werden Benutzer mithilfe eines Authentifizierungsservers geprüft. Benutzer können sich mit ihren Benutzerdaten anmelden. Die Benutzerdaten werden im Authentifizierungsserver gespeichert. Dabei kann es sich um NTLM- oder Kerberos-Server handeln. Verknüpfungen zu Servern von Drittanbietern sind ebenfalls möglich. Eine gesicherte Benutzerauthentifizierung kann zum Beispiel über LDAP Security (LDAP über TLS), Kerberos, SASL

(mit/ohne Signatur) und NTLM eingerichtet werden. Bei einer sicheren TLS-Verbindung werden die Daten für Übertragungen verschlüsselt. Es wird überprüft, ob die Benutzer für die Datenübertragung zuverlässig sind. Bei der Verknüpfung der TLS Verbindung mit Kerberos/NTLM-Benutzern wird der unbefugte Zugriff mit Hilfe von Autorisierung über Ticket/Token verhindert.

Kerberos-Authentifizierung

Kerberos authentifiziert Benutzer zwischen einem Client und einem Authentifizierungsserver in einem Netzwerk. So lassen sich verschiedene Server und Anmeldedaten für Benutzer zusammenfassen, damit Single Sign-On (SSO) möglich wird. Außerdem können die Kommunikationskanäle verschlüsselt werden.

NTLM-Authentifizierung

NTLM wird für die Netzwerkanmeldung verwendet, wenn Verbindungen zwischen MFPs/Druckern und einem Netzwerk hergestellt werden sollen. Die NTLM-Authentifizierung wird zwischen dem MFP/Drucker und einem Server ausgeführt. Hierbei kommt ein Challenge-Response-Verfahren zum Einsatz, das verhindert, dass nicht verschlüsselte Kennwörter über das Netzwerk übertragen werden. Die Challenge-Daten des Servers werden verschlüsselt. Dabei wird ein NTLM-Hash als Schlüssel verwendet.

Abbildung 1

2.1.3. Anmeldung MFP/Drucker

Statt der Eingabe eines Benutzernamens und Kennworts über ein Bedienfeld lassen sich auch folgende Anmeldemodi verwenden.

Authentifizierung mit ID-Karten (Option)

Es gibt zwei Möglichkeiten zur Authentifizierung mit ID-Karten. Eine Option ist die Anmeldung mit einer ID-Karte. Bei der anderen Option muss die ID-Karte an oder über einen Kartenleser gehalten und zusätzlich ein Kennwort eingegeben werden. Eine Authentifizierung mit ID-Karten kann für die lokale Anmeldung genutzt werden. (Abbildung 2)

Wenn die ID-Kartendaten zuvor in der Benutzerliste der MFPs/Drucker, eines externen Authentifizierungsservers oder des Authentifizierungsservers eines Drittanbieters registriert wurden, kann der authentifizierte Benutzer mit seiner ID-Karte Zugriff auf Geräte erhalten.

Bei einer Authentifizierung mit ID-Karte (zum Beispiel einer vorhandenen Mitarbeiterkarte) lassen sich Funktionen für das Abteilungsmanagement und Benutzermanagement verwenden. Dabei lassen sich einzelne Funktionen anhand der mit einer ID-Karte verknüpften Benutzerdaten beschränken. *(Abbildung 3)*

Abbildung 2

Abbildung 3

2.2. Autorisierung

Die Verwendung einzelner Funktionen wie Farbdruck, Farbkopie, Senden, Faxübertragung, Speicherung in Boxen, externe Speicherung usw. lässt sich anhand der autorisierten Benutzer beschränken. So wird das Risiko von Datendiebstahl oder -missbrauch bei der Verwendung von MFPs deutlich verringert. Außerdem kann der Zugriff auf Einstellungen des MFPs/Druckers mit den verschiedenen Benutzerauthentifizierungen eingeschränkt werden (z. B. „Benutzer“, „Administrator“ oder „Geräteadministrator“).

2.2.1. Autorisierungsmodus

MFPs/Drucker von UTAX unterstützen die folgenden Authentifizierungsmodi.

Lokale Autorisierung

Lokale Autorisierung ist eine Autorisierungsfunktion, die sich bei lokaler Anmeldung mit einer lokalen Benutzerliste verwenden lässt, die im MFP hinterlegt ist. Die Funktionen des MFP/Printer können für einzelne Benutzer eingeschränkt werden.

Netzwerkautorisierung (Gruppenautorisierung/Serverautorisierung)

Die Netzwerkautorisierung umfasst die Gruppenautorisierung und die Serverautorisierung. Bei der Gruppenautorisierung werden die bei der Netzwerkauthentifizierung erhaltenen Informationen und die auf den MFPs vorab gespeicherten Autorisierungsinformationen verwendet. Einschränkungen können auf der Grundlage der jeweiligen im Authentifizierungsserver registrierten Gruppen vorgenommen werden.

Die Serverautorisierung erfolgt anhand der bei der Netzwerkauthentifizierung erhaltenen Benutzerinformationen und der im Voraus auf dem Server*2 gespeicherten Benutzerinformationen.

Beschränkungen können auf der Grundlage der im Authentifizierungsserver registrierten Benutzer angewendet werden.

Die Nutzung der MFPs kann durch Gruppenautorisierung/Serverautorisierung eingeschränkt werden, wodurch die MFPs sicherer für die Nutzung durch eine bestimmte Gruppe/Benutzer werden.

*2: Der Server muss in der Umgebung des Benutzers konfiguriert werden.

OAuth2

Nach der OAuth-Autorisierung stellt der Autorisierungsserver ein Zugriffstoken bereit. Mit dem Token kann Microsoft Exchange E-Mails senden und empfangen. In der Vergangenheit gab es Sicherheitsrisiken, da bei der traditionellen Basisauthentifizierung Authentifizierungsinformationen wie ID und Kennwort mit Extern verknüpft werden mussten. Mit OAuth2.0 können Benutzer die Geräte sicherer nutzen, ohne Authentifizierungsinformationen weiterzugeben

Anmeldung nach Funktion

Die Anmeldung wird für bestimmte Funktionen eingeschränkt, z. B. für Drucken, Kopieren, EcoPrint, Fax, Scan to Box und Scan to Send, wenn die Gastautorisierung aktiviert ist. Benutzer, die Funktionen mit Anmeldebeschränkung verwenden möchten, müssen eine Anmeldeauthentifizierung vornehmen. So können ausschließlich eingeschränkte Benutzer, die zuvor in die Liste aufgenommen wurden, auf diese Funktionen zugreifen. Durch diesen Schutz können Datenverluste auf UTAX-Geräten zuverlässig verhindert werden – bei gleichzeitig hoher Anwenderfreundlichkeit.

2.2.2. Benutzerautorisierungsmanagement

Mit dem Benutzerautorisierungsmanagement kann die Nutzung von Funktionen auf autorisierte Benutzer beschränkt werden – unter Berücksichtigung der verschiedenen Zugangsstufen einzelner Benutzer. Die Benutzerautorisierung umfasst Geräteadministratoren, Administratoren und allgemeine Benutzer. Somit können Benutzer die keine Freigabe haben, gesperrte Funktionen auch nicht nutzen.

2.3. Sitzungsmanagement

Beim Sitzungsmanagement handelt es sich um eine Funktion, mit der ein bestimmter Zeitraum als Sitzung verwaltet wird: vom Zeitpunkt, an dem sich der Benutzer bei einem MFP anmeldet, bis zu dem Zeitpunkt, an dem er sich wieder abmeldet. Zuvor muss der Benutzer authentifiziert werden.

Folgende Verwaltungsfunktionen stehen zur Verfügung.

2.4. Automatisches Zurücksetzen des Bedienfelds

Das automatische Zurücksetzen des Bedienfelds ist eine Funktion, die eine automatische Abmeldung vornimmt, wenn innerhalb einer bestimmten Zeitspanne keine Bedienung erfolgt ist. Der Benutzer kann festlegen, wann das Zurücksetzen nach dem letzten Bedienvorgang erfolgen soll. Das automatische Zurücksetzen hilft, den unbefugten Zugriff auf die MFPs zu verhindern, wenn sich der letzte Benutzer nicht vom System abgemeldet hat.

3. Netzwerksicherheit

3.1. Einstellungen für sichere Kommunikation

MFPs/Drucker von UTAX können die Kommunikation im Netzwerk auf eine bestimmte Auswahl an IP-Adressen und Portnummern beschränken. Der sichere Hash-Algorithmus ist auch für TLS-Server-Zertifikate verfügbar. Dieser Algorithmus verhindert die Änderung und das Ausspionieren von Daten und das Masquerading über ein Netzwerk.

Mithilfe der Sicherheits-Schnelleinrichtungsfunktion (Security Quick Setup) kann ein Administrator entsprechend seiner Sicherheitsrichtlinie eine angemessene Sicherheitsstufe zwischen Stufe 1 und 3 auswählen. Je nach festgelegter Sicherheitsstufe ist es möglich mehrere Sicherheitsfunktionen wie Netzwerkeinstellungen, Benutzeroberflächeneinstellungen und Berichterstellung in einem einzigen Arbeitsschritt zusammengefasst auszuführen. Anschließend ist es möglich die Einstellungen noch weiter an die Gegebenheiten und benötigten Sicherheitseinstellung anzupassen. So wird gewährleistet, dass UTAX Geräte stets entsprechend der Sicherheitspolitik des Kunden verwendet werden können.

3.1.1. IP-Filtereinstellungen

Der IP-Filter ist eine Funktion, die den Netzwerkzugriff auf die MFPs/Drucker einschränkt, indem sie Bereiche von IP-Adressen oder Protokolltypen festlegt. Der IP-Filter gibt die Bereiche von IP-Adressen (und Subnetzmasken-Kombinationen) an, für die der Zugriff erlaubt/verweigert wird. Der IP-Filter erlaubt nur den Zugriff von Clients mit IP-Adressen, die in dem angegebenen Bereich liegen. Bestimmte zulässige Kommunikationsprotokolle können ausgewählt und dann aktiviert werden. Hinsichtlich der IPv4- und IPv6-Unterstützung kann die Kommunikation von einem einzelnen PC oder die Kommunikation von mehreren PCs und bestimmten Protokollen eingestellt werden. Auf diese Weise helfen die angegebenen Einstellungen, den unbefugten Zugriff auf die MFPs/Drucker einzuschränken.

3.1.2. Port-Einstellungen und -filter

Ausschließlich erforderliche Anschlussnummern werden aktiviert, um mit Protokollen wie IPP oder SMTP kommunizieren zu können. Dabei werden Anschlussnummern deaktiviert, die sich nicht verwenden lassen sollen.

Protokoll	Anschlussnummer	Einstellung	Hinweis
FTP Server	TCP 21	Aktivieren/Deaktivieren	FTP Server ist ein Protokoll für den Empfang von Dokumenten.
HTTP	TCP 80	Aktivieren/Deaktivieren	HTTP ist ein Protokoll, das zum Empfangen/Senden von Daten einer Webseite zwischen dem Internetserver und Browser verwendet wird.
NetBEUI	TCP 139	Aktivieren/Deaktivieren	NetBEUI ist ein Protokoll für kleine Netzwerke, das für File-Sharing- und Druckdienste sowie für den Empfang von Dokumenten verwendet wird.
HTTPS	TCP 443	Aktivieren/Deaktivieren	HTTPS ist ein Protokoll, das Verschlüsselung mithilfe von TLS bietet.
IPP over TLS	TCP 443	Aktivieren/Deaktivieren	IPP over TLS ist ein Protokoll, das TLS zur Verschlüsselung von Kanälen und IPP zur Verwendung beim Drucken über das Internet miteinander kombiniert. Außerdem kann IPP over TLS ein gültiges Zertifikat aufweisen.
LPD	TCP 515	Aktivieren/Deaktivieren	LDP ist ein Druckprotokoll, das für den Druck von Dateien oder PostScripts verwendet wird.

IPP	TCP 631	Aktivieren/Deaktivieren	IPP ist ein Protokoll, welches das Senden/Empfangen von Druckdaten über TCP/IP (auch Internet) oder Druckgeräte ermöglicht.
ThinPrint	TCP 4000	Aktivieren/Deaktivieren	ThinPrint ist eine Drucktechnologie, die in Thin-Client-Umgebungen verfügbar ist und auch TLS unterstützt.
WSD Scan	TCP 5358	Aktivieren/Deaktivieren	Windows Vista WSD ist ein Protokoll, mit dem MFPs/Drucker eine Netzwerkverbindung herstellen können. So können Benutzer MFPs/Drucker erkennen (installieren) bzw. Daten leichter senden und empfangen. Bilder aus Originaldokumenten, die mit einem MFP/Drucker gescannt werden, lassen sich in WSD PC als Datei speichern.
WSD Print	TCP 5358	Aktivieren/Deaktivieren	Windows Vista WSD ist ein Protokoll, mit dem MFPs/Drucker eine Netzwerkverbindung herstellen können. So können Benutzer MFPs/Drucker erkennen (installieren) bzw. Daten leichter senden und empfangen.
Enhanced WSD	TCP 9090	Aktivieren/Deaktivieren	Enhanced WSD beinhaltet ein Verfahren für die einfache Verbindung und Nutzung der verschiedenen Geräte, die mit einem Netzwerk verbunden sind. Außerdem kann der Status des MFP/Druckers auf dem Status Monitor angezeigt werden.
Enhanced WSD over TLS	TCP 9091	Aktivieren/Deaktivieren	Enhanced WSD (TLS) ist ein Sicherheitsprotokoll und erweiterter WSD mit TLS. Es bietet durch Verschlüsselung, Authentifizierung und Sicherheit Schutz vor Veränderungen.
RAW	TCP 9100-9103	Aktivieren/Deaktivieren	Das RAW-Protokoll beinhaltet beim Drucken andere Schritte als LPR. Im Allgemeinen nutzen MFPs/Drucker die Anschlussnummer 9100 sowie SNMP oder MIB zur Konfiguration und Überwachung des Druckerstatus.
SNMP v1/v2	UDP161	Aktivieren/Deaktivieren	Das SNMP-Protokoll wird im Netzwerkmanagement verwendet. Reguläre Kommunikation erfolgt unter Nutzung von Lese- und Schreib-Community-Namen.
SNMPv3	UDP161	Aktivieren/Deaktivieren	Das SNMP-Protokoll wird im Netzwerkmanagement verwendet. Reguläre Kommunikation erfolgt unter Nutzung von Benutzernamen und Kennwörtern. Bei Bedarf lassen sich Authentifizierungs- oder Verschlüsselungsoptionen anwenden.
DSM Scan		Aktivieren/Deaktivieren	DSM (Distributed Scan Management) nutzt Windows Server 2008 R2 für die Verarbeitung großer Mengen von Benutzerdaten in großen Unternehmen.
FTP Client		Aktivieren/Deaktivieren	FTP Client ist ein Kommunikationsprotokoll für die Weiterleitung von Dateien in einem Netzwerk.
LDAP		Aktivieren/Deaktivieren	Das Adressbuch auf einem LDAP-Server wird als externes Adressbuch bezeichnet. Als Ziel lassen sich Faxnummern und E-Mail-Adressen auswählen.
LDAP over TLS		Aktivieren/Deaktivieren	LDAP over TLS ist ein Protokoll, dass TLS für die Verschlüsselung eines Kanals verwendet, um die LDAP Kommunikation zu sichern.
POP3		Aktivieren/Deaktivieren	POP3 ist ein Standardprotokoll für den Empfang von E-Mails.
POP3 over TLS		Aktivieren/Deaktivieren	POP3 over TLS ist ein Protokoll, das POP3 (für den Empfang von E-Mails) mit TLS (zur Verschlüsselung von Kanälen) kombiniert.
SMTP		Aktivieren/Deaktivieren	SMTP ist ein Protokoll für den Versand von E-Mails.
SMTP over TLS		Aktivieren/Deaktivieren	SMTP over TLS ist ein Protokoll, das SMTP (für den Versand von E-Mails) mit TLS (zur Verschlüsselung von Kanälen) kombiniert.
SMB Client		Aktivieren/Deaktivieren	SMB ist ein Protokoll, das in Netzwerken File- oder Printer-Sharing-Dienste übernimmt.
eSCL		Aktivieren/Deaktivieren	eSCL ist ein Protokoll von Ma OS X zur Überprüfung der Systeme aus der Ferne.
eSCL over TLS		Aktivieren/Deaktivieren	eSCL over TLS ist das Kommunikationsprotokoll eSCL unter Verwendung eines TLS Zertifikates. Die Gesamte Kommunikation bei eSCL over TLS ist verschlüsselt.
LLTD		Aktivieren/Deaktivieren	LLTD ist ein Protokoll für die Netzwerk Topologie suche sowie zu Analyse der Dienst Qualität.

Privet		Aktivieren/Deaktivieren	Privet ist ein Protokoll was die Entdeckung von Cloud verbundenen Geräten in einem lokalen Netzwerk ermöglicht. Bestimmte Schnittstellen ermöglichen den Informationsaustausch zwischen den Geräten, sowie einige Aktionen, z.B. Senden eines Druckauftrags.
DNS over TLS	TCP 853	Aktivieren/Deaktivieren	DNS over TLS ist ein Protokoll, welches DNS Abfragen und Anfragen über das TLS Protokoll verschlüsselt
SCEP		Aktivieren/Deaktivieren	Simple Certificate Enrollment Protocol (SCEP) ist ein Protokoll, das Geräten automatisch Zertifikate ausstellt.
OCSP/CRL		Aktivieren/Deaktivieren	Die Certificate Revocation List (CRL) ist eine Liste, die Seriennummer von Zertifikaten ausweist, welche von der Zertifizierungsstelle wiederrufen wurden. Das Online Certificate Status Protocol (OCSP) ist ein Protokoll, das Webbrowsern Echtzeitabfragen über den Status von Zertifikaten ermöglicht.
REST		Aktivieren/Deaktivieren	REST ist ein Software-Architektur Stil für Web Anwendungen.
REST over TLS		Aktivieren/Deaktivieren	REST over TLS ist das Kommunikationsprotokoll REST unter Verwendung eines TLS Zertifikates. Die Gesamte Kommunikation bei REST over TLS ist verschlüsselt.
Bonjour		Aktivieren/Deaktivieren	Bonjour ist eine Netzwerktechnologie, die es Benutzern ermöglicht, Geräte automatisch zu entdecken.
VNC		Aktivieren/Deaktivieren	Virtual Network Computing (VNC) ist eine Fernsteuerungssoftware, welche die Bedieneroberfläche eines Gerätes mit Hilfe des RFB Protokolls über das Netzwerk fernsteuern kann.
VNC over TLS		Aktivieren/Deaktivieren	VNC over TLS ist eine Fernsteuerungssoftware, welche mit Hilfe des RFB Protokolls in Verbindung mit dem TLS Protokoll die Steuerung der Bedieneroberfläche eines Gerätes von einem Desktop PC aus ermöglicht.
Enhanced VNC over TLS		Aktivieren/Deaktivieren	Enhanced VNC over TLS ist UTAX's eigene Fernsteuerungssoftware, welche das RFB Protokoll nutzt um mit Einmal-Passwörtern (OTP) eine Verbindung zu einem Gerät herzustellen. Die Fernsteuerung ist nur durch einen autorisierten Administrator möglich. Der auf Einmal-Passwörtern basierende Fernzugriff auf die Systeme erhöht die Sicherheit der Zugriffskontrolle.

3.1.3. Secure Hash Algorithm Settings

Der leistungsstarke Secure Hash Algorithmus, der in der TLS-Verschlüsselungstechnologie verwendet wird, soll für selbst ausgegebene Zertifikate und das CSR-Zertifikat unterstützt werden.

Diese Funktion kann auch für Benutzerumgebungen verwendet werden, die sichere Maßnahmen ergreifen.

3.2. Authentifizierungsprotokoll

Beim Authentifizierungsprotokoll handelt es sich um ein Kommunikationsprotokoll, das durch Authentifizierung für eine sichere Kommunikation sorgen soll. MFPs/Drucker von UTAX unterstützen IEEE802.1x-Netzwerkauthentifizierung, SMTP-Authentifizierung und das POP-before-SMTP-Authentifizierungsprotokoll mit einer Funktion zum Senden von E-Mail. So lässt sich ein Masquerading verhindern.

3.2.1. IEEE802.1x

IEEE802.1x ist ein Standard für anschlussbasierte Authentifizierungen, der vom IEEE (Institute of Electrical and Electronics Engineers) definiert wurde. Mit diesem Protokoll ist bei Verbindungen zum

Netzwerk die Kommunikation ausschließlich mit autorisierten Benutzern (authentifizierten Geräten) zulässig. So lässt sich verhindern, dass nicht autorisierte Geräte Verbindungen zum Netzwerk herstellen. Wie bereits erwähnt unterstützen Geräte von UTAX den Standard IEEE802.1x, der unerlaubte Zugriffe von nicht authentifizierten Clients auf das Netzwerk unterbindet und somit eine unzulässige Offenlegung von Daten verhindert. Die MFPs/Drucker von UTAX unterstützen vier verschiedene Authentifizierungsmodi (siehe folgende Beschreibung).

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

Der Client wird anhand des Benutzernamens und des Zertifikats authentifiziert. Gleichzeitig wird das Zertifikat des Authentifizierungsservers überprüft.

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

Der Client wird anhand des Benutzernamens/Kennworts authentifiziert. Dabei wird ausschließlich der Common-Name des Authentifizierungsserverzertifikats überprüft.

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

EAP-FAST ist eine IEEE802.1.x/EAP-Authentifizierungsmethode, die von Cisco System, Inc. entwickelt wurde. Anhand des Benutzernamens und Kennworts wird für den Client und den Authentifizierungsserver eine gegenseitige Authentifizierung vorgenommen. PAC (Protected Access Credential) richtet mithilfe des einzigartigen gemeinsamen geheimen Schlüssels einen Tunnel für den Benutzer ein.

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

Der Client wird anhand des Benutzernamens und Kennworts authentifiziert. Außerdem wird der Authentifizierungsserver auf Grundlage des elektronischen Zertifikats authentifiziert.

Wie bei EAP-TLS werden für die Authentifizierung elektronische Client- und Server-Zertifikate benötigt, während bei EAP-TTLS anstelle eines Client-Zertifikats der Benutzername und das Kennwort verwendet werden. So lässt sich EAP-TTLS im Vergleich zu EAP-TLS leichter nutzen. Zur Prüfung der Validität von Authentifizierungsservern werden elektronische Zertifikate verwendet. So kann die Kommunikation sicherer und zuverlässiger gestaltet werden.

3.2.2. SMTP-Authentifizierung

SMTP-Authentifizierung ist eine Funktion, die den Versand einer E-Mail nur dann zulässt, wenn der Benutzername und das Kennwort beim SMTP-Server erfolgreich authentifiziert wurden. Die Funktion verhindert, dass nicht autorisierte Benutzer E-Mails über den SMTP-Server senden können, indem der Zugriff auf den SMTP-Server beschränkt wird.

3.2.3. POP before SMTP

POP before SMTP nimmt eine POP-Authentifizierung vor, bevor E-Mails vom SMTP-Server versendet werden. E-Mails lassen sich nach erfolgreicher POP-Authentifizierung innerhalb des festgelegten Zeitraums senden. Durch eine POP-Authentifizierung vor dem Versand von E-Mails kann ein Masquerading verhindert werden.

3.3. Schutz von Kommunikationskanälen

Durch den Schutz von Kommunikationskanälen lässt sich die Sicherheit von Kommunikationskanälen im Netzwerk gewährleisten. Je nach Aufgabe und Verschlüsselungsmodell können verschiedene Protokolle verwendet werden. MFPs/Drucker von UTAX unterstützen folgende Protokolle (siehe Beschreibung), um Daten vor Veränderungen oder Verlusten im Netzwerk zu schützen.

3.3.1. SNMP v3

SNMP ist ein Standardprotokoll, mit dem sich Geräte, die mit dem Netzwerk verbunden sind, überwachen und steuern lassen. Außerdem sorgt SNMP v3 durch Authentifizierung und Verschlüsselung für maximale Vertraulichkeit der Daten.

3.3.2. IPv6

IPv6 ist ein im Vergleich zu IPv4 neueres Protokoll. Die IPv6-Unterstützung, die in den MFPs/Druckern verfügbar ist, kann eine Verbindung zum Router herstellen und grundlegende Steuerungsprotokolle wie Pings verwenden. Zusätzlich zu den oben genannten grundlegenden Verbindungen wird eine sicherere Verbindung durch die Implementierung strengerer Sicherheitsmaßnahmen gewährleistet.

3.3.3. IPSec

IPsec ist ein Protokoll mit einer Funktionalität, die Daten während der Übertragung durch Verschlüsselung der jeweiligen IP-Pakete vor Abhören oder Veränderung schützt. Zum Senden/Empfangen von Daten mit IPsec wird ein IPsec-fähiger PC mit dem Netzwerk verbunden. Auch IPsec-fähige MFPs/Drucker werden mit dem Netzwerk verbunden. Beide Systeme werden dann so eingestellt, dass sie IPsec aktiv ist. Die Verschlüsselung mit IPsec wird auf Druckdaten angewendet, die von einem PC an einen MFP/Drucker gesendet werden, und auf gescannte Daten, die von einem MFP an einen PC[*3] gesendet werden. Somit unterstützt IPsec einen sichereren Datenaustausch. Darüber hinaus kann der zuverlässige Secure Hash Algorithmus für die Kommunikation zwischen zwei Hosts (Host-to-Host) verwendet werden.

**3: Die Kommunikation mit IPsec ist eine verschlüsselte Kommunikation, die ein FIPS-zertifiziertes Verschlüsselungsmodul verwendet, das nur für den japanischen und US-amerikanischen Markt erhältlich ist.*

3.3.4. TLS

TLS ist ein System für die Verschlüsselung von Daten für Übertragungen wie Webzugriff und verfügt über eine Funktion zur gegenseitigen Prüfung, ob die Zielparteien der Kommunikation für eine Übertragung ausreichend zuverlässig sind. MFPs/Drucker von UTAX unterstützen TLS-Verschlüsselungsprotokolle inkl. TLS1.0, TLS1.1, TLS1.2 und TLS1.3 und verhindern so ein Verändern oder Abfangen von Daten im Netzwerk. Darüber hinaus kann der Secure Hash Algorithmus für eine Kommunikation zwischen einem Server und einem Client verwendet werden. Bei den folgenden Protokollen handelt es sich um TLS-Verschlüsselungsprotokolle.

IPP over TLS

IPP over TLS ist ein Protokoll, das IPP (für den Austausch von Druckdaten über das Internet oder ein TCP/IP-Netzwerk) mit TLS (für die Verschlüsselung von Kommunikationskanälen) verbindet. So können Benutzer Druckbefehle an MFPs/Drucker sicher über das Netzwerk versenden.

HTTP over TLS

HTTP over TLS ist ein Protokoll, das HTTP (zum Senden/Empfangen von Daten an und von einem Webbrowser oder anderen über ein TCP/IP-Netzwerk) mit TLS (für die Verschlüsselung von Kommunikationskanälen) verbindet. Bei der Übertragung von Daten zwischen einem PC und einem MFP/Drucker lässt sich so das Risiko eines Abfangens oder Veränderns von Daten durch nicht autorisierte Benutzer verringern.

FTP over TLS

FTP over TLS ist ein Protokoll, das FTP (zum Weiterleiten von Dateien über das TCP/IP-Netzwerk) mit TLS (zur Verschlüsselung von Kommunikationskanälen) verbindet. Wenn gescannte Daten von einem MFP/Drucker mit dem FTP-Protokoll versendet werden, wird der entsprechende Kanal mit TLS verschlüsselt. FTP over TLS sorgt für eine sicherere Übertragung von Daten.

ThinPrint over TLS (Option)

ThinPrint over TLS ist ein Protokoll, das ThinPrint (zum Steuern der Bandbreite und Komprimieren der Druckaufträge) mit TLS (zur Verschlüsselung von Kommunikationskanälen) verbindet. Hierdurch entsteht eine sichere und schnelle Druckumgebung.

SMTP over TLS

SMTP over TLS ist ein Protokoll, das E-Mail-Übertragung mit TLS (zum Verschlüsseln des Kommunikationskanals zwischen Server und MFP/Drucker) verbindet. Hierdurch lassen sich ein Masquerading sowie das Abfangen oder Verändern von übertragenen Daten verhindern.

POP3 over TLS

POP3 over TLS ist ein Protokoll, das POP3 (zum Empfangen von E-Mails) mit TLS (zum Verschlüsseln des Kommunikationskanals zwischen Server und MFP/Drucker) verbindet. Hierdurch lassen sich Masquerading sowie das Abfangen oder Verändern von übertragenen Daten verhindern.

3.3.5. S/MIME

Die Secure/Multipurpose Internet Mail Extension (S/MINE) ist eine Technologie zum Verschlüsseln und digitalen Signieren von E-Mails. Wenn ein Benutzerzertifikat in das UTAX Gerät importiert wurde, kann eine Nachricht die von dem Gerät aus gesendet wird mit dem Benutzerschlüssel des Nutzers verschlüsselt werden. Dies verhindert, dass Dritte die Nachricht während der Übermittlung abfangen können. Außerdem kann, sofern ein Gerätezertifikat auf dem UTAX Gerät installiert ist, eine digitale Signatur mit dem Identifikationsschlüssel (die Absenderidentifikation des MFP/Drucker) angehangen werden. So wird es unmöglich, dass die Nachricht durch Dritte gefälscht oder manipuliert wird (zusätzliche Sicherheit für Absender).

3.4. Wi-Fi Direct (Optional)

Wi-Fi Direct Geräte können sich, ohne Umweg über einen Access Point miteinander verbinden. Das

heißt du musst keinen Router verwenden. Dies liegt daran, dass Wi-Fi Direct Geräte ihre eigenen Ad-hoc-Netzwerke schaffen, wenn erforderlich. Das Netz wird betrieben in einer eigenen Sicherheitsdomäne, die unabhängig von jedem Infrastruktur-Netzwerk ist. Wi-Fi Direct nutzt Wi-Fi Protected Setup, die Benutzern auf einfache Weise ermöglicht die Verbindung und WPA2-PSK herzustellen (persönlich).

Darüber hinaus werden die neuen Sicherheitsstandards WPA3-Personal und WPA3-Enterprise*3 unterstützt, welche einen nochmals verbesserten Schutz bieten und somit zuverlässig Angriffe wie KRACKs und Brute-force verhindern. Dies verhindert, dass nicht authentifizierte Geräteverbindungen zu den unabhängigen Netzwerken vom MFP/Drucker entstehen und schützt so gegen unbefugte Benutzung.

**3: UTAX hat die Wi-Fi CERTIFIED WPA3 Zertifizierung erhalten.*

3.5. Beschränkungsfunktion für das Senden/Empfangen von E-Mails

Beim Senden/Empfangen von E-Mails sorgt das UTAX-System wie im Folgenden beschrieben für Einschränkungen beim Senden und Empfangen von E-Mails. So wird ein Versand falscher E-Mails oder bösartiger Angriffe durch nicht autorisierte Benutzer verhindert.

3.5.1. Beschränkungsfunktion für Versandziele von E-Mails (zulassen/ablehnen)

Versandziele von E-Mails lassen sich mit einer entsprechenden Beschränkungsfunktion für Zulassung oder Ablehnung einschränken. Zugelassene Versandzieladressen werden im Voraus registriert, damit E-Mails ausschließlich an die zuvor registrierten, zugelassenen Zieladressen gesendet werden können. Abgelehnte Versandzieladressen werden ebenfalls im Voraus registriert, damit E-Mails an die zuvor registrierten, abgelehnten Zieladressen zurückgewiesen werden. So lässt sich ein Versand von E-Mails an falsche Adressen verhindern.

3.5.2. Beschränkungsfunktion für E-Mail-Absender (zulassen/ablehnen)

MFPs/Drucker von UTAX weisen eine Funktion auf, mit der sich an E-Mails angehängte Dateien ausdrucken lassen. Der Empfang von E-Mails kann jedoch durch die Beschränkungsfunktion für E-Mail-Absender je nach Voreinstellung eingeschränkt werden. Zugelassene Absenderadressen werden im Voraus registriert, damit E-Mails ausschließlich von zuvor registrierten, zugelassenen Absenderadressen empfangen werden können. Abgelehnte Absenderadressen werden ebenfalls im Voraus registriert, sodass eingehende E-Mails von den zuvor registrierten, abgelehnten Absender-adressen zurückgewiesen werden. Hiermit lassen sich Maßnahmen zur Abwehr bösartiger Angriffe (wie Spam-E-Mails) implementieren.

3.6. Automatisches Zertifizierungsmanagement

Benutzer können die Sicherheit bei hochkomplexen Betriebsabläufen durch das Hinzufügen des UTAX ACM (Automated Certificate Management) zusätzlich erhöhen. ACM enthält Authentifizierungs- und TLS-Verschlüsselungsfunktionen und kann die Anmeldungen und Neu-anmeldungen beaufsichtigen und das Ablaufdatum von Zertifikaten mithilfe von SCEP (Simple Certificate Enrollment Protocol), OCSP (Online Certificate Status Protocol) und CRL (Certificate Revocation List) überwachen. ACM eliminiert die Sicherheitsrisiken, die bei Benutzung eines ungültigen Zertifikates entstehen könnten. So werden Zertifikate automatisch hinsichtlich des Ablaufdatums überprüft und falls diese abgelaufen sind, erneuert. Zusätzlich ist eine 4096bit Verschlüsslung verfügbar. Diese sichert das Zertifikat auch

gegen fortschrittliche PKI Attacken ab. Damit kann sichergestellt werden, dass die Sicherheitsrichtlinien der Kunden eingehalten werden.

3.6.1. Erhalten eines von der CA verifizierten Gerätezertifikates mit Hilfe des Simple Certificate Enrollment Protocol Servers

Eine Zertifizierungsanfrage wird an einen SCEP (Simple Certificate Enrollment Protocol) Server gesendet, der Gerätezertifikate zusammen mit einer CRL (Certificate Revocation List) verwaltet, die auf von Administratoren eingegebenen Informationen basiert. Ein von dieser Zertifizierungsstelle ausgestelltes Zertifikat wird automatisch erkannt und direkt als verifiziertes Gerätezertifikat registriert. Das Verwalten von Prüfstellenzertifikaten wird durch diesen automatisierten Prozess vereinfacht und die Sicherheit durchgängig gewährleistet.

Nur Nutzer mit Administratorrechten haben die Möglichkeit SCEP Einstellungen vorzunehmen.

3.6.2. Überprüfen des Sperrstatus eines Zertifikates

Eine Zertifikatsanfrage wird an einen SCEP-Server (Simple Certificate Enrollment Protocol) gesendet, der Gerätezertifikate verwaltet, zusammen mit einer CSR (Certificate Signing Request), die auf der Grundlage der von Administratoren eingegebenen Informationen erstellt wird. Ein von einer Zertifizierungsstelle ausgestelltes Zertifikat wird automatisch als Gerätezertifikat registriert.

Die Verwaltung von CA-ausgestellten Zertifikaten wird durch diesen automatisierten Prozess vereinfacht.

Nur Benutzer mit Administratorrechten können SCEP-Einstellungen vornehmen.

3.6.3. Einstellung der Server-Zertifikat-Verifizierungsebene pro Protokoll

Die Zertifikatsüberprüfungsstufe eines Servers kann je nach Zielserver in der Sicherheitsumgebung eines Benutzers unterschiedlich sein. Die Serverzertifizierung ermöglicht für jedes Protokoll eine Verifizierungsstufe zwischen 0 und 3 (z.B. SMTP/POP3/FTP/LDAP/DNS). Die Serverzertifikatverifizierung kann auf Stufe 0 (keine Zertifizierung), Stufe 1 (Überprüfung des Ablaufdatums), Stufe 2 (Ablaufdatum und Verifizierungskette) und Stufe 3 (Ablaufdatum, Verifizierungskette und Widerrufsbestätigung) eingestellt werden.

Beachten Sie bitte, dass die Verbindung zum Zielserver durch eine TLS Verschlüsselung gesichert sein muss. So werden das zulässige Verbindungsziel und das autorisierte Zertifikat bestätigt. Nur Nutzer mit Administratorrechten können diese Einstellungen festlegen.

3.6.4. Einstellung der Gerätezertifikate mit Verifizierungsebenen

Diese Funktion legt die Überprüfungsstufen für Gerätezertifikate fest (0 bis 3). Die Verifizierungsstufe für Gerätezertifikate kann auf Stufe 0 (keine Verifizierung), Stufe 1 (Überprüfung des Ablaufdatums), Stufe 2 (Ablaufdatum und Verifizierungskette) und Stufe 3 (Ablaufdatum, Verifizierungskette und Widerrufsbestätigung) eingestellt werden.

Beachten Sie bitte, dass die Verbindung zum Zielserver durch eine TLS Verschlüsselung gesichert sein muss.So werden das zulässige Verbindungsziel und das autorisierte Zertifikat bestätigt. Nur Nutzer mit Administratorrechten können diese Einstellungen festlegen.

4. Schutz gespeicherter Daten

4.1. Datenschutz

Auf Festplatten oder SSDs gespeicherte sensible oder vertrauliche Daten dürfen sich auf MFPs/Druckern nicht auslesen lassen. UTAX implementiert Maßnahmen zum Schutz der gespeicherten Daten mithilfe der im Folgenden beschriebenen Funktionen und stellt so sicher, dass Kunden MFPs/Drucker von UTAX ohne Risiko nutzen können.

4.1.1. HDD/SSD-Verschlüsselung

Bei der HDD/SSD-Verschlüsselung handelt es sich um eine Sicherheitsfunktion, mit der Dokumente, Benutzereinstellungen und Gerätedaten, die auf einer Festplatte oder SSD im MFP gespeichert werden sollen, verschlüsselt werden. Die Verschlüsselung erfolgt anhand des 256-Bit-AES-Algorithmus (Advanced Encryption Standard: FIPS PUB 197). Außerdem verfügen die UTAX MFPs über ein kryptografisches Modul[*5], welches die Sicherheitsanforderungen der FIPS 140-3 Stufe 2 erfüllt. Selbst wenn verschlüsselte Festplatten oder SSDs in die Hände von Kriminellen gelangen, lassen sich die darauf gespeicherten sensiblen oder vertraulichen Daten nicht auslesen.

*5: Das kryptographische Modul ist implementiert.

Die FIPS 140-3-Zertifizierung für das kryptografische Modul befindet sich in der Prüfungsphase

4.1.2. Trusted Platform Module (TPM)

Das Trusted Platform Module (TPM) ist ein in UTAX MFPs integriertes Modul, welches sensible Information wie Bilddateien oder Zertifikate schützt. Der Schlüssel zum Verschlüsseln der Festplatte wird zusätzlich durch einen weiteren direkt im TPM enthaltenen kryptographischen Schlüssel gesichert. Alle Daten werden hierbei von demselben TPM Schlüssel verschlüsselt. Dieser ist tiefgehend innerhalb des Modules gesichert und kann nicht außerhalb des manipulationssicheren Chips ausgelesen werden. Der Festplatten Schlüssel und der TPM Schlüssel werden separat voneinander gespeichert. Wenn die Festplatte aus dem MFP entfernt wird, können keine auf der Festplatte gespeicherten Daten offengelegt werden. Die Daten sind somit stets sicher geschützt.

4.1.3. Überschreiben/Löschen von Daten

Bei der Funktion zum Überschreiben/Löschen von Daten auf Festplatten handelt es sich um eine Sicherheitsfunktion, die verhindert, dass Dritte Daten wie Benutzereinstellungen, Geräteinformationen und Bilddaten, die auf der Festplatte gespeichert sind, lesen können.

Gescannte Daten werden temporär auf der Festplatte gespeichert und anschließend an den MFP ausgegeben. Benutzer können verschiedene Einstellungen registrieren. Die tatsächlichen Daten verbleiben auf der Festplatte, bis die Daten durch andere Daten überschrieben werden – auch nach dem Ausgeben oder Löschen der Daten durch Benutzer. Das bedeutet, dass die verbleibenden ursprünglichen Daten mithilfe spezieller Tools wiederhergestellt und entwendet werden könnten. Mit der Funktion zum Überschreiben/Löschen von Daten wird der Bereich der ausgegebenen oder gelöschten Daten mit Zufallsdaten überschrieben, sodass sich die ursprünglichen Daten nicht wiederherstellen lassen.

Das Überschreiben/Löschen von Daten auf Festplatten wird automatisch ausgeführt. Es sind also keine manuellen Eingriffe nötig. Festplattendaten werden umgehend überschrieben, selbst wenn die Aufträge während des Vorgangs abgebrochen werden – oder spätestens dann, wenn der Auftrag vollständig abgeschlossen ist.

Die folgenden 2 Methoden sind je nach Modell für das Überschreiben und Löschen verfügbar:

◆ Einmaliges Überschreiben

Nicht benötigte Datenbereiche werden einmalig mit einem festen Wert überschrieben, wodurch die Daten nur noch schwer wiederherzustellen sind.

◆ Dreimaliges Überschreiben (A)

Die dreimalige Überschreibung entspricht der U.S. Department of Defense DoD 5220.22-M Methode und überschreibt nicht mehr benötigte Daten der Festplatte. Die Bereiche werden zunächst mit einem festen Wert, anschließend mit dessen Komplement und zuletzt mit zufälligen Daten überschrieben. Abschließend wird eine Verifizierung durchgeführt. Diese Methode macht es sehr schwierig gelöschte Daten wiederherzustellen. (Abbildung 4)

Beim Überschreiben und Löschen von Massendaten kann die dreifache Überschreibmethode (A) im Vergleich zur einmaligen Überschreibungsmethode länger dauern.

Abbildung 4

4.2. Löschen von Sicherheitsdaten

Am Ende des Leasing- oder Gerätelebenszyklus von MFPs/Druckern können Datenverluste auftreten, wenn vertrauliche oder sensible Daten auf den MFPs/Druckern verbleiben. Um solche Datenverluste zu verhindern, gibt es die Funktion zum Löschen von Sicherheitsdaten. Hiermit werden die auf den Geräten verbliebenden Daten je nach Modell durch die dreimalige Überschreibungsmethode (A)_DoD 5220.22-M, die siebenmalige Überschreibungsmethode (A)_DoD 5220.22-M ECE oder die siebenmalige Überschreibungsmethode (B)_BSI/VSITR, wie im Folgenden beschrieben, gelöscht.

◆ Dreimaliges Überschreiben (A)

Das dreimalige Überschreiben (A) entspricht der U.S. Department of Defense DoD 5220.22-M Methode und überschreibt sämtliche Bereiche der Festplatte. Sämtliche Daten werden zunächst mit einem festen Wert, anschließend mit dessen Komplement und zuletzt mit zufälligen Daten überschrieben. Folgend wird der abgeschlossene Prozess verifiziert. Dadurch wird es selbst mit aufwendig gestalteten Wiederherstellungsprozessen extrem schwierig die Daten zurückzuholen. Daten werden

dreimal überschrieben und anschließend einmalig verifiziert.

◆ Siebenmaliges Überschreiben (A)

Das siebenmalige Überschreiben (A) entspricht der U.S. Department of Defense DoD 5220.22-M ECE Methode und überschreibt sämtliche Bereiche der Festplatte. DoD 5220.22-M ECE ist eine Erweiterung der DoD 5220.22-M Methode. Sämtliche Daten durchlaufen zweimal die DoD 5220.22-M Methode und werden anschließend noch einmalig mit zufälligen Daten überschrieben. Dadurch wird es selbst mit aufwendig gestalteten Wiederherstellungsprozessen extrem schwierig die Daten zurückzuholen. Daten werden siebenmalig überschrieben.

◆ Siebenmaliges Überschreiben (B)

Das siebenmalige Überschreiben (B) entspricht der vom Bundesamt für Sicherheit und Informationstechnik definierten VSITR Methode und überschreibt sämtliche Bereiche der Festplatte. Alle Daten werden zunächst mit Null- und anschließend mit festen Werten (0xff) überschrieben. Dies wird dreimal hintereinander durchgeführt. Anschließend werden die Daten nochmals mit einem festen Wert (0xAA) überschrieben. Dadurch wird es selbst mit aufwendig gestalteten Wiederherstellungsprozessen extrem schwierig die Daten zurückzuholen. Daten werden siebenmalig überschrieben.

4.3. SSD Sichere Löschung

Zwei Methoden, Secure Erase und Cryptography Erase, werden zur Bereinigung von Daten verwendet. (Die Verfügbarkeit der Methode hängt vom MFP/Druckermodell ab).

- Secure Erase erfüllt die Anforderungen der Clear-Kategorie der NIST Guideline for Media Sanitization und löscht alle Datenbereiche der SSD. Alle Datenbereiche werden mit dem ATA-Befehl SECURITY ERASE UNIT gelöscht. Die Funktionalität bietet eine zuverlässige Löschung der SSD. Die Daten werden einmalig gelöscht.
- Cryptography Erase löscht einen Kryptoschlüssel, der zur Verschlüsselung der Daten verwendet wird, vollständig. Dies macht eine Wiederherstellung der auf der SSD im MFP gespeicherten Daten unmöglich.

Die Sicherheitsdatenbereinigung hat die folgenden Funktionen: Es kann ein Zeitplan konfiguriert werden, welcher sicherstellt, dass die Bereinigungen zu einem geplanten Zeitpunkt durchgeführt werden; Automatische Benachrichtigungen im Vorfeld der geplanten Bereinigungen um Administratoren und Servicetechniker zu informieren; Ein Durchführungsbericht (beinhaltet Informationen über Inhalt und die Zeitangaben der Bereinigung) kann automatisch bei abgeschlossener Säuberung gedruckt werden; Eine Systemsperrung, welche die Anwender daran hindert die Geräte nach der Durchführung erneut zu benutzen, kann eingerichtet werden.

Die Einrichtung und Ausführungen dieser Funktionen werden durch einen Administrator verwaltet. Somit können sämtliche Geräteeinstellungen auf die Werksteinstellungen zurückgesetzt werden.

4.4. Zugriffsbeschränkung

In MFPs lassen sich „Benutzerboxen“, „Auftragsboxen“ und „Faxboxen“ zur Speicherung von Daten einrichten. Der Zugriff auf in diesen Boxen gespeicherte Daten kann beschränkt werden.

4.4.1. Benutzerbox

Benutzer können die „Benutzerbox“ erzeugen, um Daten in MFPs zu speichern. Für die jeweiligen Boxen lassen sich Nutzungseinschränkungen, Zeiträume für die Datenaufbewahrung sowie Kennwörter festlegen. *(Abbildung 5)*

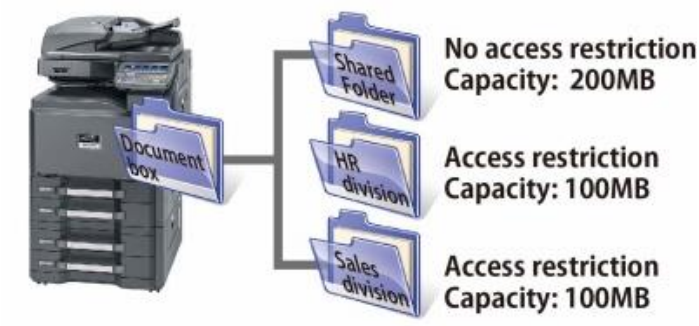

Abbildung 5

Kennwort für Boxen

Benutzer, die auf eine Box zugreifen können, lassen sich per Kennwort einschränken. In diesem Fall müssen Benutzer ein passendes Kennwort eingeben, das bis zu 16 Zeichen umfassen kann (inkl. verschiedener Zeichen wie Großbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen).

Nutzungsbeschränkungen für Boxen

Zur Verwaltung der Festplattenkapazität lässt sich die Nutzung der Kapazität von Boxen einschränken.

Festlegung von Besitzern

Die Benutzerbox kann ausschließlich von einem Benutzer aufgerufen werden, der sich als Besitzer seiner Benutzerbox registriert hat. So lassen sich Zugriffe nicht autorisierter Benutzer verhindern. Mit „gemeinsamer Box“ kann festgelegt werden, ob die Box gemeinsam genutzt werden soll oder nicht. Bei gemeinsamer Verwendung können auch Benutzer, die nicht als Besitzer definiert sind, auf die Box zugreifen. Unter Wahrung der Anwenderfreundlichkeit lässt sich die Box effektiv vor unerlaubten Zugriffen schützen. Damit wird für hohe Sicherheit gesorgt.

Zeitraum der Dokumentenaufbewahrung

Nach einer bestimmten Zeit können gespeicherte Dokumentendaten automatisch gelöscht werden, damit sie nicht über längere Zeit aufbewahrt werden. So lässt sich das Risiko eines Verlusts von vertraulichen Daten weiter verringern.

Zeitpunkt des Löschens

Sobald ein Druckauftrag abgeschlossen ist, werden in einer Box gespeicherte Dokumentendaten automatisch gelöscht. Damit kann das Löschen von Daten nicht vergessen werden. Das Ergebnis: Die Daten lassen sich von nicht autorisierten Dritten nicht mehr anzeigen.

4.4.2. Auftragsbox

Daten für „Privater Druck“, Pin Print, „Schnellkopie“, „Prüfen und Aufbewahren“ sowie

„Auftragsspeicher“ lassen sich in einer Auftragsbox speichern. Diese Box kann von Benutzern weder erzeugt noch gelöscht werden. Die Box lässt sich mit einem PIN-Code schützen, um Zugriffe darauf zu beschränken. *(Abbildung 6)*

Abbildung 6

Automatisches Löschen des Datenspeichers für temporäre Dokumente

Daten, die temporär in einer Box für „Privater Druck“, Pin Print, „Schnellkopie“ oder „Prüfen und Aufbewahren“ gespeichert sind, lassen sich automatisch löschen, nachdem die Daten eine bestimmte Zeit lang gespeichert wurden. Daten werden also lediglich im benötigten Zeitraum gespeichert. So lässt sich das Risiko eines Verlusts von vertraulichen Daten verringern.

4.4.3. Faxbox

Eine Box für das Speichern empfangener Faxdaten, die sich in einem MFP befindet, heißt „Faxbox“. Die empfangenen Faxdaten lassen sich mithilfe einer Speicherweiterleitungsfunktion in der Faxbox speichern. Außerdem werden die empfangenen Faxdaten anhand der Subadressen des Absenders oder der Faxnummern den entsprechenden Boxen zugewiesen, damit wichtige Dokumente umgehend bestätigt werden können. So lassen sich per Fax empfangene Daten in einem Feld des MFP bestätigen. Erwünschte Faxdokumente können ausgedruckt und unerwünschte Faxdokumente sofort gelöscht werden. *(Abbildung 7)*

Abbildung 7

Kennwort für Boxen

Benutzer, die auf eine Box zugreifen dürfen, lassen sich per Kennwort einschränken. So müssen Benutzer ein passendes Kennwort eingeben, das bis zu 16 Zeichen umfassen kann (inkl. verschiedener Zeichen wie Großbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen).

Festlegung von Besitzern

Eine Box kann ausschließlich von einem Benutzer aufgerufen werden, der sich als Besitzer seiner Box registriert hat. So lassen sich Zugriffe nicht autorisierter Benutzer verhindern. Mit „gemeinsamer Box“ kann festgelegt werden, ob die Box gemeinsam genutzt werden soll oder nicht. Bei gemeinsamer Verwendung können auch Benutzer, die nicht als Besitzer definiert sind, auf die Box zugreifen. So lässt sich die Box unter Wahrung der Wartungsfreundlichkeit effektiv vor unerlaubten Zugriffen schützen. Damit wird für hohe Sicherheit gesorgt.

Zeitpunkt des Löschens

Sobald ein Druckauftrag abgeschlossen wurde, können in einer Box gespeicherte Empfangsdaten automatisch gelöscht werden. Eine längere Aufbewahrung von Daten würde nur unnötige Risiken verursachen. Durch ein zeitnahes Löschen lässt sich die Sicherheit deutlich verbessern.

5. Sicherheit beim Drucken

5.1. Sicheres Drucken

Sicheres Drucken ist eine Druckfunktion für MFPs/Drucker. Die Funktion zum sicheren Drucken kann für vertrauliche oder sensible personenbezogene Dokumente genutzt werden. Damit ist sichergestellt, dass unbeaufsichtigt ausgedruckte Dokumente nicht in die Hände Dritter gelangen oder von anderen Personen am Gerät eingesehen werden können.

5.1.1. Privater Druck

Der Private Druck ist eine Funktion, um Druckaufträge in MFPs/Druckern, die von einem PC gesendet wurden, solange zu halten, bis ein Benutzer im Bedienfeld des MFPs/Druckers das passende Kennwort eingibt. Die Anwendungssoftware verlangt dabei vom Benutzer die Einrichtung eines Zugangscodes im Druckertreiber, wenn ein Druckauftrag über einen PC gesendet wird. Zum Drucken des Dokuments muss der Benutzer dann im Bedienfeld des Geräts den entsprechenden Zugangscode eingeben. Nach Abschluss des Druckvorgangs werden die Daten gelöscht. Auch wenn vor dem Drucken der Ausschalter betätigt wird, werden die Daten gelöscht. So wird auf dem Gerät für hohe Sicherheit gesorgt.

5.2. Verhinderung unbefugter Kopien

Beim Kopieren können folgende Funktionen unbefugte Kopien verhindern, indem die Merkmale für Dokumentensicherheit verbessert werden.

5.2.1. Textstempel/Bates-Stempel

Dank einer Textstempelfunktion, die übersichtliche Informationen über die Bedeutung von Dokumenten liefert, können Benutzer zwischen verschiedenen Stempeln wie „Vertraulich“, „Nicht kopieren“ oder „Datenschutz“ wählen (abhängig von den verfügbaren Stempeln). Benutzer können Textstempel sogar nach Belieben anpassen. Mit der Bates-Stempelfunktion „Seriennummer“ lässt sich die Seriennummer des für den Ausdruck verwendeten Geräts aufdrucken, während die Funktion „Nummerierung“ dafür sorgt, dass auf ausgedruckte Dokumente nacheinander Seitennummern gedruckt werden. Außerdem stehen die Funktionen „Datum“ und „Benutzername“ zur Verfügung.

5.2.2. Sicherheitswasserzeichen

Dokumente können mit einem Sicherheitswasserzeichen oder -text versehen werden. Wenn gedrucktes Material kopiert wird, das mit einem Wasserzeichen versehen ist, wird dieses auf der Kopie sichtbar. Daran wird erkennbar, dass es sich hierbei um eine unerlaubte Kopie handelt. *(Abbildung 8)*

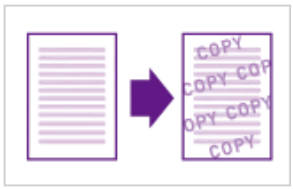

Abbildung 8

6. Fax-Sicherheit

6.1. FASEC (nur Japan)

FASEC ist eine Sicherheitsrichtlinie für Faxkommunikation, die von der Communication and Information Network Association of Japan (CIAJ) entwickelt wurde. Das FASEC-Logo wird auf Faxdokumente gedruckt, damit MFPs bestimmte Faxfunktionen nutzen können, um Folgendes zu verhindern: falsche Übertragungen, falsche Verbindungen durch Wähltonerkennung und ein Liegenlassen unbeaufsichtigter empfangener Faxdokumente. Außerdem kann überprüft werden, ob Daten richtig übertragen wurden. Die Fax-Sicherheitsfunktionen von UTAX erfüllen alle relevanten Anforderungen, sodass UTAX für seine MFPs das entsprechende Logo erhalten hat.

6.2. Verschlüsselte Faxkommunikation

Hierbei handelt es sich um eine Kommunikationsmethode, bei der Originaldaten vor dem Versand verschlüsselt werden. So können Bilddaten, die gerade übertragen werden, nicht von anderen Personen abgefangen werden. Das bedeutet, dass Dritte Inhalte weder anzeigen noch verwenden können. Eingehende Daten werden beim Empfänger zunächst entschlüsselt und dann gedruckt.
Dies ist eine effektive Methode für die Übertragung vertraulicher und sensibler Dokumente, die nicht offengelegt werden dürfen.

Die Funktion ist ausschließlich zwischen UTAX-Geräten verfügbar, welche die gleiche Funktion zur Verschlüsselung von Kommunikation unterstützen.

Für die Ver- und Entschlüsselung der ursprünglichen Kommunikationsdaten auf der Versand- und Empfängerseite (Gerät) wird der gleiche Verschlüsselungsschlüssel verwendet. Wenn der Schlüssel auf der Versand- und Empfängerseite (Gerät) nicht identisch ist, kann keine verschlüsselte Kommunikation durchgeführt werden. Darum müssen die beiden Parteien (d. h. Sender und Empfänger) einen gemeinsamen Schlüssel festlegen und registrieren, bevor die verschlüsselte Kommunikation gestartet werden kann.

6.3. Einschränkungen beim Senden/Empfangen

Diese Funktion sorgt dafür, dass Geräte Faxdokumente nur dann senden bzw. empfangen können, wenn eine vordefinierte Kommunikationsbedingung erfüllt wird (d. h. zugelassene Faxnummer und zugelassene ID-Nummer). Mit dieser Funktion können bei der Kommunikation die Faxziele eingeschränkt werden. Wenn auf eine Ablehnungsliste eine Empfangsbeschränkung angewendet wird, werden Faxdokumente von einem Absender, der in die Liste abgelehnter Faxnummern aufgenommen wurde oder seine lokale Faxnummer nicht registriert hat, abgelehnt. Faxdokumente lassen sich ausschließlich an Ziele übertragen, die in einer Liste mit zugelassenen Nummern oder einem zugelassen Adressbuch eingetragen sind.

6.4. Schutz vor falschen Übertragungen

Um zu verhindern, dass wichtige Dokumente an falsche Ziele übertragen werden, erhalten Benutzer die Aufforderung, die Faxnummer des Empfängers zweimal einzugeben. Die Funktion zur Verhinderung falscher Übertragungen lässt sich für Adressbücher, Zehnertastaturen und Kurzwahlen verwenden. Außerdem unterbindet die Funktion eine Wahlwiederholung bei Adresszielen. Das vorherige Ziel wird nicht gespeichert, sodass sich die Übertragung eines anderen Dokuments an das vorherige Empfangsziel verhindern lässt. So werden Datenverluste vermieden, da andere Personen das Ziel nicht sehen können. Außerdem werden die Zieldaten direkt nach dem Abmelden gelöscht (bei aktivierter Benutzerauthentifizierung).

6.4.1. Bestätigung von Eingaben

Benutzer werden dazu aufgefordert, die gleiche Faxnummer zweimal einzugeben, wenn sie ein Fax versenden möchten. Dabei müssen sie die Faxnummer direkt über die Zifferntasten eingeben. Das Empfangsziel wird erst dann aktiviert, wenn die Faxnummer zweimal eingegeben wurde. So lassen sich falsche Übertragungen verhindern, die durch die Betätigung falscher Tasten verursacht werden. Diese Funktion kann von Benutzern eingerichtet werden.

6.4.2. Verhinderung einer direkten Eingabe von Faxnummern über Zifferntasten

Eine direkte Eingabe von Faxnummern über Zifferntasten des Bedienfelds kann beschränkt werden. Bei Verwendung dieser Funktion können Benutzer Faxdokumente ausschließlich an Empfangsziele übertragen, die in einer Zielliste enthalten sind. Das bedeutet, dass Benutzer keine Faxdokumente versenden können, wenn sich die Empfänger nicht im Adressbuch oder auf den Kurzwahltasten befinden. So lassen sich falsche Übertragungen verhindern, die durch die Eingabe falscher Faxnummern oder eine unerlaubte Nutzung verursacht werden.

6.4.3. Zielbestätigung vor der Übertragung

Nach dem Betätigen der [Start]-Taste werden die Sendeziele auf dem Display angezeigt, damit die Benutzer prüfen können, wenn die Funktion für eine Zielbestätigung vor der Übertragung aktiviert ist. Der abschließende Bestätigungsschlüssel wird erst aktiviert, nachdem alle Ziele auf dem Display angezeigt wurden. Da Benutzer die Ziele vor dem Versand von Faxdokumenten erneut bestätigen müssen, verhindert diese Funktion falsche Übertragungen.

6.5. Verwendungssperrzeit

Hierbei handelt es sich um eine Sicherheitsfunktion, mit der sich ein Zeitraum festlegen lässt, in dem das Drucken empfangener Faxdokumente untersagt ist. Wenn eine Verwendungssperrzeit festgelegt wurde, werden alle Aktivitäten wie Drucken, Kopieren, Druck, empfangene Mail bzw. USB-Übertragung und Faxübertragung im Netzwerk sowie das Drucken von Faxdokumenten im angegebenen Zeitraum verboten. Diese Funktion ist PIN-geschützt und kann zeitweise außer Kraft gesetzt werden. So lässt sich eine unerlaubte Nutzung von MFPs verhindern (zum Beispiel nachts, wenn sich weniger Mitarbeiter im Büro aufhalten).

6.6. Kommunikation mit Subadressen

Bei der Kommunikation mit Subadressen handelt es sich um eine Kommunikationsfunktion, die Daten mit einer Subadresse und einem Kennwort versendet/empfängt. Die Funktion entspricht dabei den Empfehlungen von ITU-T (International Telecommunication Union Telecommunication

Standardization Sector). Die Funktion unterstützt auch eine Kommunikation mit Geräten anderer Unternehmen, zum Beispiel eine vertrauliche Kommunikation (Versand an eine bestimmte Box des Empfangsgeräts) oder Abrufkommunikation (Empfang des Originals vom sendenden Gerät durch eine Aktion des Empfangsgeräts). Bislang war eine solche Kommunikation nur mit Geräten von UTAX möglich. Bei Verwendung der Funktion zur Kommunikation mit Subadressen werden die eingehenden Daten zum Beispiel in der Subadressenbox gespeichert. Damit sorgt die Funktion für eine sicherere Kommunikation.

6.6.1. Vertrauliche Übertragung mit Subadressen (senden/empfangen)

Nach der Einrichtung einer vertraulichen Box mit Subadresse auf dem Empfangsgerät können wichtige Dokumente, die nicht für die Augen anderer Personen bestimmt sind, an diese Box gesendet werden. Durch die Nutzung einer Subadresse und eines Kennworts wird dabei für Vertraulichkeit gesorgt. Das empfangene Dokument wird in der zuvor registrierten Box gespeichert, ohne nach dem Empfang sofort ausgedruckt zu werden. So lassen sich die empfangenen Daten ohne die neugierigen Blicke anderer ausdrucken.

6.6.2. Übertragung von Bulletinbords mit Subadressen (senden/empfangen)

Wenn Empfangsgeräte die Funktion zur Übertragung von Bulletinbord mit Subadressen unterstützen, lassen sich Dokumente des Benutzers ohne Datenverluste sicher übertragen.

6.7. Speicherweiterleitung

Mit dieser Funktion lassen sich die empfangenen Bilder nach Erhalt des Faxdokuments an andere Faxgeräte oder Computer weiterleiten bzw. ausdrucken. Wenn die Weiterleitungsfunktion aktiviert ist, können alle eingehenden Bilder an die vordefinierten Adressen (Ziele) weitergeleitet werden. Dies gilt für andere Faxgeräte, den Versand von Mail, SMB (sendfile) und FTP-Versand. Außerdem lassen sich erhaltene Bilder an die im MFP eingerichtete Box weiterleiten und anschließend speichern. So wird verhindert, dass in der Ablage des Geräts unbeaufsichtigte (empfangene) Faxblätter liegen bleiben. *(Abbildung 10)*

Abbildung 10

6.8. Maßnahmen zum Schutz vor nicht autorisierten Zugriffen

Die Fax- und Netzwerkfunktion sind strukturell voneinander getrennt. Über eine Telefonleitung eingehende Daten werden von der Faxfunktion bearbeitet. Diese Struktur verhindert unerlaubte Zugriffe von der Telefonleitung auf das Netzwerk über eine Faxfunktion, die im MFP verfügbar ist.

7. Sicherheit beim Senden

7.1. Zielbestätigung vor dem Senden

Benutzer können das Sendeziel (d. h. die Adressnummern) und den Betreff vor dem Senden auf dem Display überprüfen. So lässt sich ein Versand an falsche Adressen verhindern. Je nach Einstellung werden diese Daten vor dem Senden stets im Bedienfeld angezeigt.

7.2. Verbot von Broadcast Übertragungen

Broadcast-Übertragung ist eine Funktion, die das gleiche Dokument zu mehreren Zielen als einmaligen Vorgang überträgt. Diese Funktion ermöglicht Administratoren, Verbote oder Erlaubnisse zu erstellen. Wenn ein Verbot festgelegt wurde, kann keine Gruppe mit 2 oder mehr Zielen ausgewählt werden. Dies verhindert die Übermittlung an mehrere Ziele durch unabsichtliches Hinzufügen in die Gruppe.

7.3. Neueingabe von (Adress-)Zielen

Die direkte Eingabe über das Bedienfeld ist eingeschränkt, damit die zuvor in die Zielliste (z. B. Adressbuch oder Kurzwähltasten) aufgenommenen Ziele die einzigen zulässigen Ziele darstellen.
So lässt sich eine unerlaubte Verwendung oder ein falscher Versand aufgrund der Eingabe einer falschen Faxnummer verhindern.

7.4. Verschlüsselte PDF (Option)

Mit der Funktion PDF (verschlüsselt) können Benutzer PDF-Dateien oder stark komprimierte PDF-Dateien als Dateiformat auswählen und gescannte Daten durch Verschlüsselung und Einrichtung eines Kennworts schützen. Beim Öffnen, Drucken oder Verändern der empfangenen PDF-Datei können Einschränkungen aufgehoben werden, wenn das richtige Kennwort eingegeben wird.

7.5. Dateiverschlüsselung mittels digitaler Signatur

Dieses Feature ermöglicht dem Nutzer durch das Hinzufügen einer digitalen Signatur die Vertrauenswürdigkeit einer Datei zu verbessern.

Hierzu werden zunächst ein Gerätezertifikat sowie ein asymmetrisches Verschlüsselungsverfahren mit einem öffentlichen und einem geheimen Schlüssel auf dem Triumph Alder MFP registriert. Nach dem Scannen eines Dokumentes werden das Gerätezertifikat und das Schlüsselpaar dahingehend genutzt, um eine digitale Signatur zu erstellen und die Datei mit dieser zu versehen.

Durch diesen Prozess hat der Empfänger stets die Möglichkeit nachzuvollziehen, welcher MFP das mit der Signatur versehene Dokument erstellt hat und ob diese Datei im Nachhinein noch verändert wurde.

7.6. Senden mit FTP-Verschlüsselung

Die Funktion Senden mit FTP-Verschlüsselung nutzt TLS zur Verschlüsselung des Kommunikationskanals. So wird die Sicherheit übertragener Daten gewährleistet. Das Risiko einer Veränderung von übertragenen Daten bzw. eines Abhörens kann damit deutlich verringert werden.

8. Gerätemanagement

8.1. Auftragsmanagement

Informationen über Aufträge in der Warteschlange oder Protokolle lassen sich am Gerät prüfen. Zur Verfügung stehen vier Status („Druckauftrag“, „Auftrag senden“, „Gespeicherter Auftrag“ und „Reservierter Auftrag“) sowie drei verschiedene Protokolle („Druckaufträge“, „Sendeaufträge“ und „Speicheraufträge“). Es lassen sich detaillierte Informationen für einzelne Aufträge aufrufen und ggf. zur weiteren Verfolgung verwenden (inkl. Benutzername, Uhrzeit und Ziel). Beim Drucken von Aufträgen mit dem Druckertreiber kann außerdem festgelegt werden, ob der Dateiname als Auftragsname angezeigt werden soll. *(Abbildung 11)*

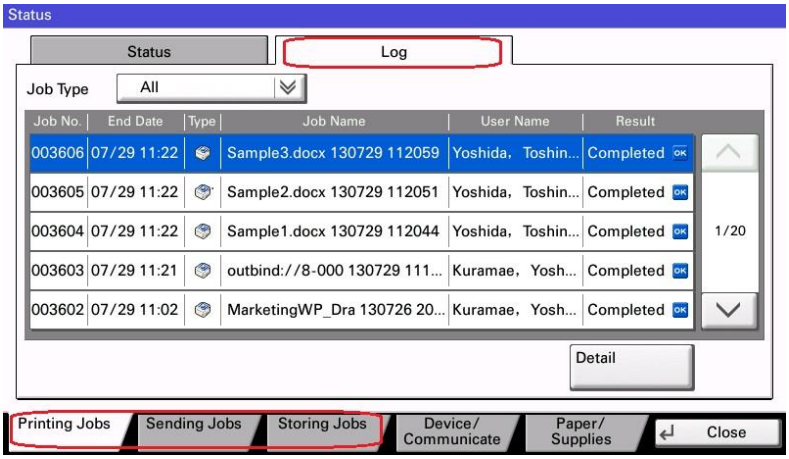

Abbildung 11

8.1.1. Einsicht von Job-Informationen

Je nach Autorisierung des Benutzers variiert das Fenster für die Anzeige von Auftragsprotokollen. Eine Genehmigung zur Anzeige von Auftragsdaten und Faxübertragungsprotokollen lässt sich für die genauen Auftragsstatusdaten und das Auftragsprotokoll einrichten. Wenn die Benutzerauthentifizierung aktiviert ist, können Benutzer ausschließlich eigene Auftragsprotokolldaten anzeigen und überprüfen. Nach einer Anmeldung als Administrator werden im Display alle Auftragsprotokolldaten angezeigt.

8.2. Protokoll Log-Daten

In MFPs/Druckern werden Prüfprotokolle unterstützt. So gibt es einen Datensatz mit Informationen über die Nutzung des Geräts (inkl. Benutzername, Datum & Zeit und Ergebnisse). Das Prüfprotokoll umfasst das Anmelde-, Geräte- und Kommunikationsfehlerprotokoll. Durch eine Konsultation des Protokolls kann der Administrator der MFPs/Drucker überprüfen, ob das Gerät sicher genutzt wird und frei von Risiken ist.

8.2.1. Anmeldeprotokoll

Die Anmeldedaten der Benutzerauthentifizierung lassen sich speichern. Im Fall einer unerlaubten Aktivität, Änderung oder Freigabe von Dokumenten in den MFPs/Druckern kann das Anmeldeprotokoll zur Untersuchung und Verfolgung des unerlaubten Zugriffs verwendet werden.

8.2.2. Geräteprotokoll

Firmware-Updates und veränderte Einstellungen von MFPs/Druckern lassen sich ebenfalls protokollieren. Außerdem können jene Inhalte erfasst werden, die vom Administrator im Systemmenü verändert wurden.

8.2.3. Kommunikationsfehlerprotokoll

Durch eine Analyse des Kommunikationsfehlerprotokolls kann der Administrator prüfen, ob die Netzwerkkommunikation richtig funktioniert. Wenn ein wiederholter Kommunikationsfehler entdeckt wird, lässt sich der potenziell unerlaubte Zugriff untersuchen.

8.3. Protokollverwaltung

Mit der Protokollverwaltung lassen sich Prüf- und Auftragsprotokolle verwalten und die mögliche Quelle von Sicherheitsvorfällen untersuchen.

8.3.1. Auftragsprotokoll versenden (an E-Mail-Adresse)

Die einzelnen Protokolle lassen sich per E-Mail an die vom Administrator angegebene E-Mail-Adresse senden, sobald die Zahl der Protokolle eine vordefinierte Zahl erreicht.

8.4. Syslog

Mithilfe des Syslog-Protokolls kann ein Audit-Protokoll für MFPs/Drucker in Echtzeit an einen SIEM-Server (Security Information and Event Management) gesendet werden*6. Das Audit-Protokoll kann gesammelt und zentral verwaltet werden.

*6: Der SIEM-Server muss in der Umgebung des Benutzers konfiguriert werden.

8.5. Integritätsprüfung der Sicherheitsfunktionen

Die folgenden Funktionen werden zur Überprüfung der Integrität der Sicherheitsfunktionen unserer Produkte eingesetzt.

8.5.1. Softwareverifizierung

Hiermit wird geprüft, ob die Ausführungsmodule der Sicherheitsfunktionen verändert wurden bzw. richtig funktionieren. Außerdem lässt sich die von den Sicherheitsfunktionen genutzte Datenintegrität prüfen.

8.5.2. Digital Signierte Firmware

Die Digitale Signatur ist ein Bestandteil der Firmware zur Sicherstellung und Validierung des Firmwarepaketes. Die Firmware steuert den Betrieb der MFP/Drucker. Die Digital signierte Firmware verhindert Veränderung durch böswillige Personen. MFP/Drucker werden gegen Beschädigung und unbefugte Nutzung sowie gegen Eindringen ins Netzwerk geschützt.

8.5.3. Secure Boot

Secure Boot ist eine Funktion der MFPs, welche vor jeder Inbetriebnahme sicherstellt, dass eine autorisierte Firmware verwendet wird. Die Gültigkeit der Firmware wird durch die Verwendung einer digitalen Signatur verifiziert. Während das Gerät hochfährt, wird die Firmware auf dem RAM bereitgestellt. Hierbei wird bestätigt, dass der auf der Firmware aufgespielte Hash-Wert mit dem Hash-Wert der

digitalen Signatur übereinstimmt. Selbst wenn eine exakte Nachbildung der Firmware kreiert wird, kann diese nicht die Verifizierung der digitalen Signatur passieren. Somit würde durch die Secure Boot Funktion eine solche Firmware niemals von MFPs ausgeführt und die Zerstörung des Gerätes präventiv verhindert werden.

8.5.4. Laufzeit-Integritätsprüfung

Die Laufzeit-Integritätsprüfung ist eine Funktion die während des laufenden Betriebes regelmäßig die Gültigkeit der Firmware verifiziert ohne dabei Änderungen an der im RAM bereitgestellten Version vorzunehmen. Falls doch Veränderungen vorgenommen werden sollten, wird dies in der Prüfung erkannt und ein Systemfehler sowie eine Warnung ausgegeben. In Verbindung mit der Secure Boot Funktion ist dies eine sehr effektive Sicherheitsmaßname gegen unerlaubte Firmware-Veränderungen.

8.5.5. Whitelist

Als Präventionsmaßnahme gegen Malware ist es möglich eine Whitelist einzusetzen. Für den unerwarteten Fall, dass eine nicht autorisierte Datei, welche Malware enthalten könnte, installiert wird, blockiert diese Whitelist die Ausführung des Programms. Die auf dem MFP/Drucker installierte Whitelist enthält nur vertrauenswürdige Programme. Dies könnten z.B. von UTAX bekannte, zugelassene oder autorisierte sein. Wenn eine nicht vertrauenswürdige Datei gefunden wurde, welche nicht in der Auflistung enthalten ist, verhindert die Whitelist automatisch die Ausführung

9. Nutzungsbeschränkung

9.1. Nutzungsbeschränkung

Auf die MFPs/Drucker von UTAX lassen sich folgende Nutzungsbeschränkungen anwenden. Da sich die Nutzung der MFPs/Drucker einschränken lässt, kann auch der Zugriff auf Daten, die in den MFPs/Druckern gespeichert sind, beschränkt werden.

9.1.1. Schnittstellensperre

Der Zugriff über Schnittstellen des Geräts wie USB-Gerät, USB-Host, optionale Schnittstelle (Steckplatz 1) und optionale Schnittstelle (Steckplatz 2) kann ebenfalls gesperrt werden. Die Nutzung der Netzwerkschnittstelle lässt sich je nach Protokoll beschränken.

9.1.2. Logische Sperre der USB-Speicher

Wenn ein USB-Speicher mit einem USB-Anschluss von MFPs/Druckern verbunden wird, kann es zum Verlust vertraulicher Daten oder unerlaubten Zugriffen auf Daten der MFPs/Drucker kommen. Der Administrator kann die Host-Schnittstelle für USB-Speicher deaktivieren, aber gleichzeitig zulassen, dass ein ID-Kartenleser an einer USB-Host-Schnittstelle des MFPs/Druckers verwendet wird. Außerdem verfügen MFPs/Drucker von UTAX über eine Funktion, mit der sich die Nutzung von USB-Speicher einschränken lässt – auch dann, wenn der USB-Speicher mit der USB-Host-Schnittstelle der MFPs/Drucker verbunden wird. So lassen sich Datenverluste über die USB-Schnittstelle sowie eine Verbreitung von Viren verhindern.

9.1.3. Sperrung des Bedienfelds

Die Verwendung des Bedienfelds von MFPs/Druckern kann eingeschränkt werden. So gibt es eine partielle Sperrung mit drei Stufen: Einstellungen für Input/Output über das Bedienfeld, Einstellungen für die Auftragsausführung und Einstellungen für das Papier. Einstellungen, die mit der vom Administrator gewünschten Sperrstufe verbunden sind, werden aktiviert. Durch die Sperrung des Bedienfelds kann die Verwendung des Systemmenüs sowie von Auftragsabbrüchen unterbunden werden. So lässt sich eine unerlaubte Nutzung von MFPs/Druckern verhindern.