IF IT WORX, IT'S UTAX

UTAX Fleetmanager (UTAX FM):

Security White Paper

Version 2.5

Dokumentenversion: 04/2026

09. April 2026

1. Einführung

1.1. Aufgabe

Die Aufgabe dieses Dokuments besteht darin, Kunden über die Sicherheitsmaßnahmen im UTAX Fleetmanager (UTAX FM) zu informieren.

Bei UTAX hat der zuverlässige Schutz der Datenressourcen, die von UTAX FM bearbeitet werden, oberste Priorität. Datenressourcen werden durch die robusten Konfigurations- und Sicherheitseinstellungen von UTAX FM rundum geschützt.

1.2. Zielgruppe

Zielgruppe dieses Dokuments sind die Kunden von UTAX.

1.3. Aufbau des Dokuments

Dieses Dokument teilt sich in folgende Abschnitte auf:

- ✧ Überblick über den UTAX FM
- ✧ Schutz von Datenressourcen
- ✧ Sicherheit
- ✧ KYOCERA‘s Maßnahmen zum Schutz von UTAX FM
- ✧ Sicherheit: technische Details
- ✧ Health Insurance Portable & Accountability Act (HIPAA)
- ✧ Anhang

1.4. Impressum

Die in diesem Dokument enthaltenen Informationen können ohne Ankündigung geändert werden. Das Dokument kann kleine Fehler enthalten. Änderungen und Optimierungen in UTAX FM können in spätere Ausgaben ohne Ankündigung integriert werden.

2. Überblick über den UTAX Fleetmanager

Dieser Abschnitt enthält einen Überblick über den UTAX Fleetmanager (UTAX FM) sowie Informationen zur Konfiguration.

2.1. Was ist UTAX FM?

UTAX FM ist ein Clouddienst, der für Kunden entwickelt wurde, die MFPs/Drucker (Geräte) verwenden; er dient der Reduzierung von Wartungskosten und Verbesserung des Betriebssupports. UTAX FM kann Daten von Geräten, die auf eine bestimmte Region verteilt sind, remote erfassen und zentral verwalten.

UTAX FM verfügt über eine **Verwaltungsfunktion** und **Aufgaben**.

Die **Verwaltungsfunktion** ermöglicht eine zentrale Verwaltung und Überwachung der Geräte von UTAX und anderen Anbietern, eine verbesserte Ressourcenauslastung sowie eine Steigerung der Produktivität. Mit der Verwaltungsfunktion können Sie:

- Zähler auslesen
- Berichte erstellen
- den Status von Verbrauchsmaterialien prüfen
- das Bestellsystem fördern
- den Betriebsstatus von Geräten überwachen

Aufgaben sind ausschließlich bei Geräten von UTAX verfügbar. Sie können zur Erhöhung der Kundenzufriedenheit beitragen, da Kunden raschen Remote-Support erhalten, inklusive:

- Systemeinrichtung
- detaillierter Gerätedaten
- Gerätediagnosen
- Problembehebung bei Geräten
- Remote-Firmware-Upgrades
- Remote-Wartung

2.2. Konfiguration von UTAX FM

Der UTAX FM besteht aus **UTAX FM, UTAX FM Device, UTAX FM Mobile** und **UTAX FM Gateway.**

UTAX FM dient als Grundlage für UTAX FM und nutzt das Cloudsystem von Microsoft Azure.

UTAX FM kommuniziert mit UTAX FM Device, UTAX FM Mobile und UTAX FM Gateway und verwaltet Geräte mithilfe dieser Komponenten. Außerdem stellt UTAX FM diesen Komponenten Gerätedaten bereit.

UTAX FM bietet verschiedene Funktionen wie Remote-Firmware-Upgrades, Neustart von Geräten und Remote-Einstellung des Wartungsmodus. Darüber hinaus verfügt UTAX FM über eine webbasierte Benutzeroberfläche sowie eine mobile Anwendung mit Benutzeroberfläche, mit denen sich Geräte, Komponenten und Benutzer verwalten lassen.

Um bidirektionale Kommunikation zu ermöglichen, müssen UTAX FM Device, UTAX FM Mobile und UTAX FM Gateway im UTAX FM registriert werden.

UTAX FM Device ist ein Modul, das am Kundenstandort in Geräte eingebettet ist.

UTAX FM Device stellt anhand der Abfragen und des Zeitplans vom UTAX FM Geräteprotokolle, Zähler sowie Statusseiten bereit. Gerätedaten sendet UTAX FM Device über Bluetooth™, USB™ oder Wi-Fi Direct™ an UTAX FM Mobile.

UTAX FM Mobile ist eine Anwendung, die auf mobilen Geräten (wie Smartphones und Tablets) von Servicemitarbeitern installiert wird.

UTAX FM Device/ UTAX FM Gateway kommunizieren mit UTAX FM über das Netzwerk des Kunden (d. h. das LAN). UTAX FM Mobile kommt zum Einsatz, wenn UTAX FM Device/ UTAX FM Gateway keine Verbindung zum Kundennetzwerk (d. h. das LAN) aufbauen kann. UTAX FM Mobile nutzt Peer-to-Peer-Kommunikation (wie Bluetooth, USB oder Wi-Fi Direct) zur Herstellung von Verbindungen mit Geräten sowie zum Abrufen verschiedener Daten von diesen Geräten.

Ähnlich wie UTAX FM Device sendet UTAX FM Mobile Gerätedaten an UTAX FM. Darüber hinaus bietet UTAX FM Mobile Funktionen zur Anzeige von Gerätedaten und Ereignisprotokollen.

UTAX FM Mobile lässt sich als mobile Anwendungsoberfläche für UTAX FM verwenden.

UTAX FM Gateway ist ein UTAX FM Gateway für Windows-Anwendung auf einem PC, welches UTAX FM Device als Legacy-Geräte unter UTAX FM Gateway verwaltet.

UTAX FM Gateway verbindet Geräte von UTAX und anderen Anbietern über das Internet mit UTAX FM.

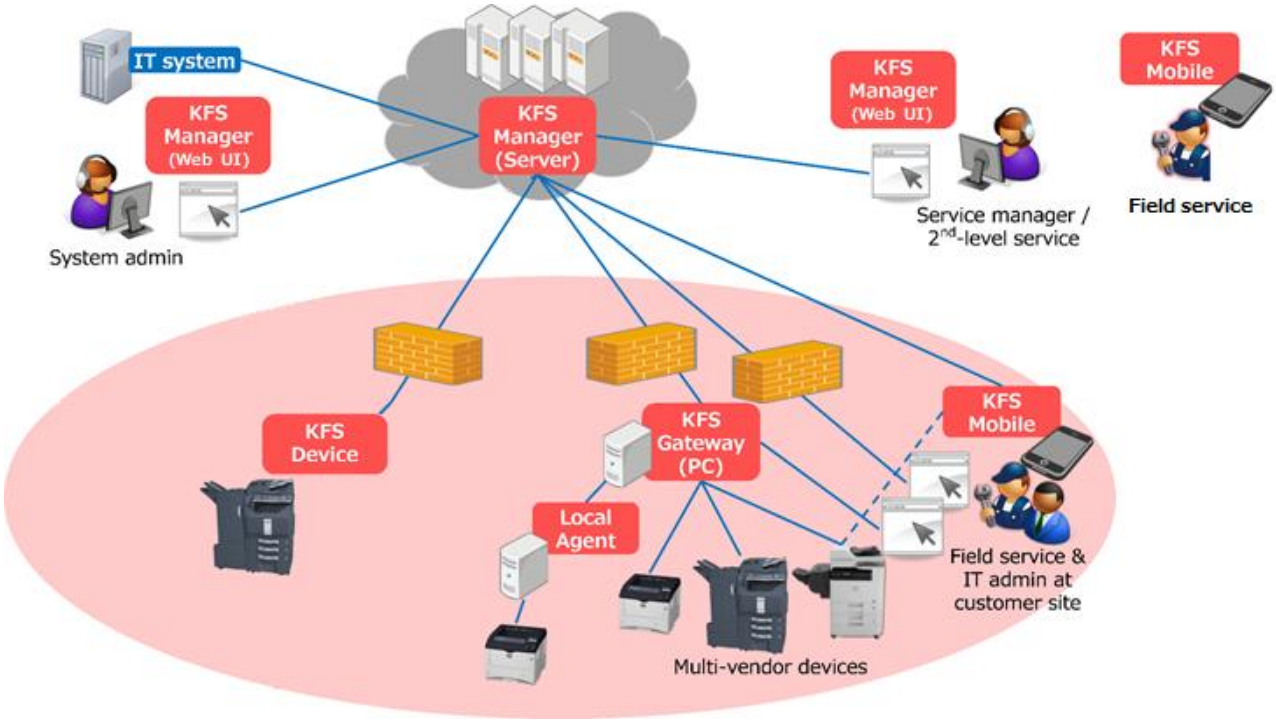

Abbildung 1: Konfiguration vom UTAX FM

3. Schutz von Datenressourcen

Bei Verwendung von UTAX FM werden folgende Datenressourcen, die von UTAX FM verarbeitet werden, streng geschützt(*2).

(*2) Mehr Informationen über Schutzmaßnahmen finden Sie im Abschnitt „Sicherheit“

3.1. Aus der Kundenumgebung abgerufene Gerätedaten

Die von Kunden abgerufenen Gerätedaten enthalten ausschließlich Informationen, die für die Verwaltung und Wartung der Geräte erforderlich sind. Ohne vorherige Zustimmung des Kunden werden keine personenbezogenen Daten übertragen.

Tabelle 1 und Tabelle 2 zeigen beispielhafte Daten, die vom UTAX FM abgerufen werden. Die Geräteinformationen werden regelmäßig einmal am Tag an UTAX FM Manager gesendet. Zur Aufrechterhaltung einer XMPP-Verbindung/MQTT-Verbindung zwischen dem UTAX FM Manager und dem Gerät/Gateway wird die XMPP Keep-Alive-Verbindung/MQTT Keep-Alive-Verbindung jede Minute/alle vier Minuten(*3) ausgeführt. Die Gesamtzahl der Verbindungsvorgänge von XMPP Keep-Alive/MQTT Keep-Alive pro Tag beträgt etwa 1.300 Kbytes/108Kbytes, dies hängt jedoch von den verwendeten Paketgrößen ab. Die gesamte Datenmenge, die pro Tag von einem MFP-Gerät erhaltenen wird, beträgt etwa 100 KByte. Zur Aufrechterhaltung einer XMPP- und einer MQTT-Verbindung beträgt die Gesamtdatenmenge also etwa 1.400 KByte bzw. 208 KByte.

(*3) Im Monitormodus wird weder eine XMPP-Verbindung noch eine MQTT-Verbindung zwischen UTAX FM Device und UTAX FM Manager hergestellt. Weitere Einzelheiten finden Sie unter Verbindungsmodus.

IF IT WORX, IT'S UTAX

Tabelle 1: Menge an Daten

Aufrechterhaltung einer XMPP-Verbindung

Übertragene Daten	Häufigkeit der Datenübertragung	Menge der übertragenen Daten pro Tag	Gesamtmenge der übertragenen Daten pro Tag
• Zähler • Tonerstand • Geräteprotokoll	Einmal am Tag - Zähler/Tonerstand können bis zu viermal am Tag übermittelt werden; die Standardeinstellung lautet jedoch einmal am Tag.	80 kByte	1.400 kByte
• Gerätemeldung	Pro Warnereignis	20 kByte	
• Verbindung: Keep-Alive	Jede Minute	1.300 kByte	
• Geräteeinstellung • Snapshot • Gerätestatus • Einstellung des Wartungsmodus • Datenerfassung • On-Demand-USB-Protokolle • Backup-Daten	Bei einer Remote-Wartung	0 kByte - Daten werden nur bei einer Remote-Wartung übertragen. - Die Datenmenge hängt vom Gerätemodell und Wartungsinhalt ab.	

Tabelle 2: Menge der vom UTAX FM Gateway (NetGateway) an UTAX FM übertragenen Daten

Aufrechterhaltung einer MQTT-Verbindung

Daten	Die Häufigkeit der Datenübertragung	Datenmengen	Die Gesamtmenge pro Tag
•Zähler •Tonerstand •Geräteprotokoll	Einmal täglich - Die Zähler-/Tonerstandsdaten können bis zu viermal täglich übertragen werden, die Standardeinstellung ist jedoch einmal täglich.	80 Kbytes	208 Kbytes
•Gerätebenachrichtigung	Pro Ereignis	20 Kbytes	
•Verbindungsprüfung : Keep- Alive	Alle 4 Minuten	108 Kbytes	
• Geräteeinstellung	Bei einer Fernwartung	0 Kbytes	

• Snapshot • Gerätestatus • Wartungseinstellung • Datenerfassung • On-Demand USB Protokolle • Daten sichern während einer Fernwartung		-Wird ohne Fernwartungsbetrieb nicht übertragen. - Die Datenmenge ist abhängig vom Gerätemodell und Arbeitsinhalt.	

Aus Tabelle 3 wird die Menge der vom UTAX FM Gateway (NetGateway) an UTAX FM übertragenen Daten deutlich. Gerätedaten werden einmal am Tag an UTAX FM gesendet. Die Gesamtmenge der von einem MFP-Gerät abgerufenen Daten beträgt etwa 7,3 kByte am Tag. Zum Gateway-Protokoll: Das Prüfprotokoll ist 1 kByte groß, während das Systemprotokoll bei Erkennung und Registrierung von 10 Geräten 94 kByte groß ist. Außerdem ist die Erkennungseinstellung beim Speichern von 10 Erkennungseinstellungen 13 kByte groß. Die Datenmenge kann jedoch je nach dem Wert der Erkennungseinstellungen variieren.

Tabelle 3: Die Datenmenge von UTAX FM Gateway zu UTAX FM Manager

Daten	Die Häufigkeit der Datenübertragung	Die Gesamtmenge pro Tag
Zähler	Einmal pro Tag - Die Zähler-/Tonerstandsdaten können bis zu viermal täglich übertragen werden	4 Kbytes (1 Gerät)
Tonerstand		2 Kbytes (1 Gerät)
Gerätebenachrichtigung	Pro Ereignis	1.3 Kbytes (1 Ereignis)
Geräteprotokoll	Einmal pro Tag für jede Datei (zwei Zip-Dateien) - Audit Protokoll - System Protokoll	Audit Protokoll: 1 Kbyte System Protokoll: 94 Kbytes (Der Test wurde nach der Erfassung und Registrierung von 10 Geräten durchgeführt)
Geräteregistrierung	Einmal pro Tag für jede Geräteregistrierung - Ab V2.1 kann der Benutzer dies bis zu 6 Mal pro Tag ausführen.	13 Kbytes (10 Geräteregistrierung) (Die Anzahl der Datenübertragungen pro Tag erhöht sich je nach Häufigkeit. z.B. wenn 6 mal eingestellt ist, 78 Kbytes (10 Intervalle))

Aus Tabelle 4 wird die Menge der vom UTAX FM Gateway (NetGateway) an die Geräte übertragenen Daten deutlich; dabei wird die durchschnittliche Nutzung eines NetGateway angegeben, dass weniger als 25 registrierte Geräte aufweist. Die Menge der übertragenen Daten hängt von der Zahl der registrierten Geräte ab. Informationen zur Häufigkeit der Datenübertragung können Sie Tabelle 5-1 und 5-2 entnehmen. Die Menge der übertragenen Daten pro Tag für Zähler, Tonerstand und Gerätemeldung pro Gerät beläuft sich auf 1.776 kByte, 144 kByte bzw. 21.600 kByte. Damit beträgt die Gesamtmenge der übertragenen Daten pro Tag 23.520 kByte.

Hinweis: Je mehr registrierte Geräte ein NetGateway aufweist, desto größer wird das automatische Abfrageintervall. Dadurch reduziert sich die Gesamtmenge der übertragenen Daten pro Tag.

Tabelle 4: Menge der vom UTAX FM Gateway (NetGateway) an die Geräte übertragenen Daten

Übertragene Daten	Häufigkeit der Datenübertragung	Menge der übertragenen Daten pro Tag	Gesamtmenge der übertragenen Daten pro Tag
Zähler	Alle 60 Minuten	74 kByte für jedes Gerät × 24 Stunden = 1.776 kByte	23.520 kByte
Tonerstand	Alle 60 Minuten	6 kByte für jedes Gerät × 24 Stunden = 144 kByte	
Gerätemeldung	Jede Minute	15 kByte für jedes Gerät × 24 Stunden × 60 Minuten = 21.600 kByte	

Tabelle 5-1: Abrufintervall

Bei der Aktualisierung von UTAX FM Gateway auf die neueste Version

	Warnung					Zähler/Verbrauchsmaterialien				
Zahl der Geräte	2,000-1,001	1,000-301	300-101	100-26	25-1	2,000-1,001	1,000-601	600-201	200-101	100-26
Kategorie mit sehr hoher Priorität	120 (Min.)	60 (Min.)	15 (Min.)	5 (Min.)	1 (Min.)	24 (Std.)	12 (Std.)	6 (Std.)	2 (Std.)	60 (Min.)
Kategorie mit hoher Priorität	150 (Min.)	75 (Min.)	30 (Min.)	10 (Min.)	2 (Min.)	30 (Std.)	15 (Std.)	7.5 (Std.)	2.5 (Std.)	75 (Min.)
Kategorie mit mittlerer Priorität	180 (Min.)	90 (Min.)	45 (Min.)	15 (Min.)	3 (Min.)	36 (Std.)	18 (Std.)	9 (Std.)	3 (Std.)	90 (Min.)
Kategorie mit niedriger Priorität	210 (Min.)	105 (Min.)	60 (Min.)	20 (Min.)	4 (Min.)	42 (Std.)	21 (Std.)	10.5 (Std.)	3.5 (Std.)	105 (Min.)

Tabelle 5-2: Abrufintervall

Bei Installation des UTAX FM Gateways

	Warnung					Zähler/Verbrauchsmaterialien				
Zahl der Geräte	2,000-1,001	1,000-301	300-101	100-26	25-1	2,000-1,001	1,000-601	600-201	200-101	100-26
Kategorie mit sehr hoher Priorität	5 (Min.)					60 (Min.)				
Kategorie mit hoher Priorität	10 (Min.)					75 (Min.)				
Kategorie mit mittlerer Priorität	15 (Min.)					90 (Min.)				
Kategorie mit niedriger Priorität	20 (Min.)					105 (Min.)				

Beachten Sie, dass die von Benutzern üblicherweise verwendeten MFPs/Drucker als hohe Priorität behandelt werden.

- **Gerätemeldung/Protokoll** (Systemfehler, Ereignis, Verbrauch, Zähler)

  Wenn Systemfehler oder bestimmte Ereignisse auftreten (z. B. ein Papierstau oder niedriger Tonerstand), sendet das Gerät Ereignisdaten an UTAX FM.

  UTAX FM informiert die zugewiesenen Benutzer unmittelbar über

  das Ereignis.

- **Geräteeinstellung**

  Folgende Geräteeinstellungsdaten werden abgerufen:

  - Netzwerkeinstellung (z. B. Enhanced WSD)
  - Systemeinstellung (z. B. Datum/Uhrzeit, Zeitzone)
  - E-Mail-Einstellung (z. B. SMTP, Einstellungen zum E-Mail-Versand)
  - Druckeinstellung (z. B. Eco Print)
  - Kopiereinstellung (z. B. Originalbild, Durchscheinen verhindern)
  - Faxeinstellung (z. B. Mehrfachscan, Faxauflösung beim Senden)
  - Standardeinstellung (z. B. Scanauflösung)

  Das Wartungspersonal sorgt nach Erhalt von Kundenanfragen und -genehmigungen remote für eine optimale Geräteeinstellung am Kundenstandort.

  Das Wartungspersonal speichert die Geräteeinstellung UTAX FM und sendet die Geräteeinstellung an das Gerät, wenn es gerade nicht verwendet wird.

- **Snapshot** (Status, Wartungsstatus, Ereignisprotokoll, Wartungsbericht, USB-Protokoll und Faxbericht, Anwendungsstatus)

  Das Wartungspersonal kann Snapshot-Daten abrufen, um Geräteprobleme remote zu diagnostizieren.

  Das Wartungspersonal erhält den Snapshot vom Gerät mithilfe von UTAX FM.

- **Gerätestatus** (Nachricht im Bedienfeld und Warnungsliste)

  Wartungspersonal kann Nachrichten im Bedienfeld sowie die Warnungsliste anzeigen, um den Gerätestatus remote zu überprüfen.

  Das Wartungspersonal erhält die Nachrichten im Bedienfeld sowie die Warnungsliste vom Gerät mithilfe von UTAX FM.

- **Einstellung des Wartungsmodus**

  Das Wartungspersonal sorgt remote für eine optimale Einstellung des Wartungsmodus am Kundenstandort.

  Das Wartungspersonal ruft die Einstellung des Gerätewartungsmodus von UTAX FM ab.

  Das Wartungspersonal ändert die Einstellung des Wartungsmodus und sendet diese mit UTAX FM an das Gerät.

- **Datenerfassung(*4)**

  Druckdaten des Kunden werden an UTAX FM gesendet.

(*4) Datenerfassung ist nur möglich, wenn im Bedienfeld des Zielgeräts die Bestätigungsmeldung angezeigt und im Voraus eine Genehmigung des IT-Administrators eingeholt wird. Der Wartungsmanager kann einen Zeitraum von bis zu 7 Tagen (Standard: 1 Tag) festlegen, nach dem die erfassten Daten entfernt werden. Diese Einstellung kann für einzelne Gruppen vorgenommen werden. Bei Erreichen des angegebenen Zeitraums werden die erfassten Daten automatisch entfernt.

- **On-Demand-USB-Protokolle(*5)**

  Das Wartungspersonal wählt ein Gerät aus und ruft On-Demand-USB-Protokolle ab.

  UTAX FM Device erzeugt USB-Protokolle und sendet diese an UTAX FM.

  UTAX FM speichert die USB-Protokolle, die es von UTAX FM Device erhalten hat.

  Das Wartungspersonal kann die USB-Protokolle von UTAX FM via Snapshot-Liste auf einen PC herunterladen.

(*5) On-Demand-USB-Protokolle lassen sich nur dann abrufen, wenn vom IT-Administrator am Kundenstandort eine entsprechende Genehmigung erteilt wurde. Während des Abrufs wird das Gerät für einige Minuten (drei bis vier Minuten) gesperrt. Danach wird das Gerät automatisch neu gestartet. Nach dem Neustart des Geräts werden die USB-Protokolle automatisch von UTAX FM auf den PC des Benutzers heruntergeladen.

- **Backup-Daten(*6)**

  Das Wartungspersonal (Systemadministrator/Manager/Wartung) kann Backup-Daten, die von einem Gerät an andere Geräte exportiert wurden, umgehend importieren.

(*6) Backup-Daten können erst dann abgerufen werden, wenn der Benutzer die Bestätigungsmeldung auf dem Bedienfeld des Zielgeräts akzeptiert hat. Jegliche Backup-Daten, die personenbezogene Daten enthalten, werden nicht in UTAX FM gespeichert. Empfangene Backup-Daten sind verschlüsselt. Eine Verwendung dieser Funktion ist auf Personen beschränkt, die befugt sind, auf Gruppengeräte zuzugreifen. Das Importieren/Exportieren von Backup-Daten wird aufgezeichnet.

Alle Funktionen von UTAX FM sind standardmäßig aktiviert. Bei der Erstellung einer Gruppe hat der Manager jedoch die Möglichkeit, Funktionen zu deaktivieren. Deaktivierte Funktionen erscheinen in der Benutzeroberfläche ausgegraut und können von Benutzern der Gruppe nicht aufgerufen werden.

Wenn mehrere Benutzer via E-Mail benachrichtigt und mit Berichten informiert werden sollen, dürfen deren E-Mail-Adressen gegenseitig nicht preisgegeben werden, da E-Mail-Adressen als personenbezogene Daten gelten können. Zum Schutz personenbezogener Daten können Benutzer die BCC-Option verwenden.

Tabelle 6: Daten und Attributdaten

Daten	Attributdaten
Gerätemeldung/Protokoll	• Systemfehler • Ereignis (z. B. Papierstau, niedriger Tonerstand) • Verbrauch • Zähler
Dateneinstellung	• Netzwerkeinstellung (z. B. Enhanced WSD) • Systemeinstellung (z. B. Datum/Uhrzeit, Zeitzone) • E-Mail-Einstellung (z. B. SMTP, Einstellungen zum E-Mail-Versand) • Druckeinstellung (z. B. Eco Print) • Kopiereinstellung (z. B. Originalbild, Durchscheinen verhindern) • Faxeinstellung (z. B. Mehrfachscan, Faxauflösung beim Senden) • Standardeinstellung (z. B. Scanauflösung)
Snapshot	• Status • Wartungsstatus • Ereignisprotokoll • Wartungsbericht • USB-Protokoll • Faxbericht

	• Anwendungsstatus
Gerätestatus	• Nachricht im Bedienfeld • Warnungsliste
Einstellung des Wartungsmodus	• Geräteanpassung
Datenerfassung	• Druckdaten des Kunden
On-Demand-USB-Protokolle	• USB-Protokolle
Backup-Daten	• Adressbuch • Kostenstelle • One Touch • Benutzerverwaltung • IC-Karte • Dokumentenbox • Programm • Schnelltaste • Faxweiterleitung • Systemeinstellung • Netzwerkeinstellung • Auftragseinstellung • Faxeinstellung • Druckereinstellung • Bedienfeldeinstellung

3.2. In UTAX FM verwendete Daten

UTAX FM-Komponente	Datenressourcen (verwendet zur Identifizierung und Kommunikation innerhalb von UTAX FM)
UTAX FM	• Authentifizierungsdaten von jedem UTAX FM-Benutzer • Von UTAX FM Devices verwendete Zugangscodes (UTAX FM Gateway und UTAX FM Mobile) • Serverzertifikate, die für sichere Kommunikation zwischen UTAX FM und verschiedenen Agenten oder Clients (z. B. Webbrowser, UTAX FM Devices, UTAX FM Gateways und UTAX FM Mobile) sowie zwischen internen Komponenten von UTAX FM verwendet werden • MAC-Adressen der einzelnen UTAX FM Devices oder UTAX FM Gateways • Netzwerkdaten (wie Hostname und IP-Adresse der einzelnen registrierten Geräte), die der Remote-Verwaltung oder -Wartung von Geräten dienen • SNMP-Anmeldedaten (z. B. SNMPv1/v2-Community-Name, SNMPv3-Benutzername und Kennwort usw.), eingegeben in UTAX FM oder UTAX FM Gateway in den Geräteerkennungseinstellungen und verwendet zur Herstellung von Verbindungen mit Geräten über SNMP • Seriennummern der einzelnen mobilen Geräte (Smartphone oder Tablet), auf denen UTAX FM Mobile installiert ist [Lässt sich die Seriennummer vom mobilen Gerät nicht abrufen, kann für denselben Zweck stattdessen seine IMEI-Nummer verwendet werden.]
UTAX FM Device	• MAC-Adresse des Geräts, in das UTAX FM Device eingebettet ist

	• Proxy-Authentifizierungsdaten, die über das Bedienfeld eines Geräts oder auf eine andere Weise eingegeben wurden und dem UTAX FM Gateway selbst oder UTAX FM Device dazu dienen, über den Proxyserver eine Verbindung mit UTAX FM herzustellen • Authentifizierungstoken, das von UTAX FM erzeugt und auf ein UTAX FM Device heruntergeladen wird • Server-Zertifikat, das von UTAX FM Gerät generiert und bei einem MQTT-Server registriert wurde.
UTAX FM Gateway	• Authentifizierungsdaten, die von einem IT-Administrator zur Anmeldung bei UTAX FM Gateway verwendet werden • Authentifizierungsdaten, die von einem Wartungstechniker vor Ort zur Anmeldung bei UTAX FM Gateway verwendet werden(*7) • MAC-Adresse des Geräts, auf dem UTAX FM Gateway installiert ist • Zugangscode, der von UTAX FM Gateway zur eigenen Registrierung bei UTAX FM verwendet wird [Bei automatischer Erkennung und Registrierung kann UTAX FM Gateway den gleichen Code auch zur Registrierung von Geräten nutzen.] • Proxy-Authentifizierungsdaten, die einem UTAX FM Gateway oder UTAX FM Device dazu dienen, über den Proxyserver eine Verbindung mit UTAX FM herzustellen • Authentifizierungstoken, das von UTAX FM erzeugt und in UTAX FM Gateway heruntergeladen wird

	• SNMP-Anmeldedaten (z. B. SNMPv1/v2-Community-Name, SNMPv3-Benutzername und Kennwort usw.), eingegeben in UTAX FM oder UTAX FM Gateway in den Geräteerkennungseinstellungen und verwendet zur Herstellung von Verbindungen mit Geräten über SNMP • Authentifizierungsdaten, die von UTAX FM Gateway zur Kommunikation mit Geräten über proprietäre Protokolle verwendet werden
UTAX FM Mobile	• Seriennummern der einzelnen mobilen Geräte (Smartphone oder Tablet), auf denen UTAX FM Mobile installiert ist [Lässt sich die Seriennummer vom mobilen Gerät nicht abrufen, kann für denselben Zweck stattdessen seine IMEI-Nummer verwendet werden.] • Authentifizierungstoken, das von UTAX FM erzeugt und in UTAX FM Mobile heruntergeladen wird • Authentifizierungsdaten, die vom Benutzer von UTAX FM Mobile eingegeben werden, um sich bei UTAX FM anzumelden • Proxy-Authentifizierungsdaten, die von UTAX FM Mobile und einem gekoppelten UTAX FM Device genutzt werden, um über den Proxyserver eine Verbindung mit UTAX FM herzustellen.

(*7) von UTAX FM Gateway (NetGateway) nicht unterstützt

4. Sicherheit

In diesem Abschnitt wird im Detail beschrieben, wie die im vorherigen Abschnitt erwähnten Datenressourcen mittels verschiedener in UTAX FM implementierter Sicherheitseinstellungen zuverlässig geschützt werden und Daten von Kunden, falls diese keine Genehmigung dazu erteilt haben, von keinen Benutzern (wie Vertriebsgesellschaften oder anderen Mandanten(*8)) aufgerufen werden können.

(*8) Mandanten stehen für Benutzer, die UTAX FM verwenden.

4.1. Gruppen und Benutzer Accounts

UTAX FM realisiert mehrere Mandanten (* 9) für mehrere Händler und Vertriebsunternehmen und verwendet das Konzept der „Gruppenverwaltung“, um eine angemessene Zugriffskontrolle für Benutzer- und Gerätedaten zu erzwingen und das Weitergeben von Informationen an andere Mandanten zu verhindern. Diese Gruppenverwaltung behandelt eine Vertriebsgesellschaft oder einen Händler als eine Einheit, und die Zugriffskontrolle wird durch Anwenden der hierarchisch strukturierten Gruppen erzwungen. In jeder Gruppe gibt es Benutzerkonten, deren Kombination zur Steuerung des Zugriffs auf UTAX FM verwendet wird. Daher kann ein Händler die Daten eines anderen Händlers nicht einsehen

(*9) Multi-Mandant gibt ein System an, das von mehreren Kunden verwendet wird.

4.1.1. Gruppenmanagement

Gruppenverwaltung bedeutet, Benutzerdaten und Gerätedaten, die zu einer Gruppe (* 10) gehören, nur innerhalb einer Organisation bestehend aus diesen Gruppen, zu verwalten und gemeinsam zu nutzen. Eine solche Organisation ist hierarchisch strukturiert, wobei eine übergeordnete Gruppe an der Spitze steht. Die übergeordnete Gruppe kann nur auf die untergeordneten Gruppen in der Struktur zugreifen, die untergeordneten Gruppen können jedoch nicht auf die übergeordnete Gruppe zugreifen.

Beispielsweise ist eine Händlerzentrale (DLA), die für den Verkauf einer bestimmten Region zuständig ist, die übergeordnete Gruppe für diese Region. Unter dieser Muttergruppe befinden sich Untergruppen von Händlern (DLB), die für den Vertrieb in verschiedenen Ländern der Region verantwortlich sind. Unter den Händler-Untergruppen befinden sich andere Händler (DLC), die für den Verkauf in bestimmten Regionen eines Landes verantwortlich sind.

Die übergeordnete DLA-Gruppe kann auf die darunter liegenden DLBs und DLCs zugreifen und diese verwalten, die darunter liegenden Gruppen können jedoch nicht auf die übergeordnete DLA-Gruppe zugreifen. Dies gilt auch für die DLB-Untergruppen, die auf alle Gruppen unter jeder einzelnen Untergruppe zugreifen und diese verwalten können, die Untergruppen können die Gruppe über ihnen jedoch nicht sehen.

Die Gruppenverwaltung greift nicht auf verschiedene DLAs, DLBs oder verschiedene DLCs zu. Außerdem kann ein Benutzer nur einer Gruppe angehören.

Als zusätzliche Sicherheitsmaßnahme können Benutzerkonten mit Service-, Analysten- oder Kundenrollen erst dann auf Gruppen zugreifen, zu denen sie gehören, wenn ihnen ein Manager oder Systemadministrator Zugriff gewährt.

Gruppenverwaltungseinheiten können eine delegierte Gruppe oder eine Gruppe sein.

Eine delegierte Gruppe ist eine Einheit zum Verwalten von Geräten, Benutzern, UTAX FM-Gateways und anderen Ressourcen (z. B. Berichtsvorlagen, Benachrichtigungsvorlagen, Firmware-Paketen usw.). Die „Stammgruppe“ oben in der Hierarchie wird als delegierte Gruppe betrachtet, da sie alle diese Ressourcen verwaltet.

Eine Gruppe ist eine Einheit zur Verwaltung von Geräten und UT-Gateways. Wenn ein Manager für DLC3 nicht vorhanden ist (siehe Abbildung 2), werden die Geräte und das UT-Gateway von DLC3 von der DLB verwaltet.

Verwaltungsdaten wie Benutzerdaten und Gerätedaten, die pro Gruppe verwaltet werden, können nur innerhalb einer hierarchisch strukturierten Organisation, zu der diese Gruppen gehören, gemeinsam genutzt und verwaltet werden. Benutzer in der Gruppe, die oben in der Hierarchie positioniert sind, können nur auf Daten in ihren untergeordneten Gruppen zugreifen. Daher sind die Daten logisch getrennt und der Zugriff von Gruppen, die zu einer anderen Organisation gehören, ist nicht zulässig.

(* 10) Gruppendaten, Benutzerdaten und Gerätedaten werden nach Erhalt einer Löschanforderung der Gruppe sofort logisch gelöscht. Selbst wenn die Daten irrtümlich gelöscht werden, können sie wiederhergestellt werden. Die Daten, die 14 Tage nach der Anforderung zum Löschen der Gruppe vergangen sind, werden jedoch vollständig gelöscht. Wenn Sie einen einzelnen Benutzer oder ein einzelnes Gerät löschen, werden die Daten sofort dauerhaft gelöscht (Gerätedaten sind Informationen, die das Gerät identifizieren.).

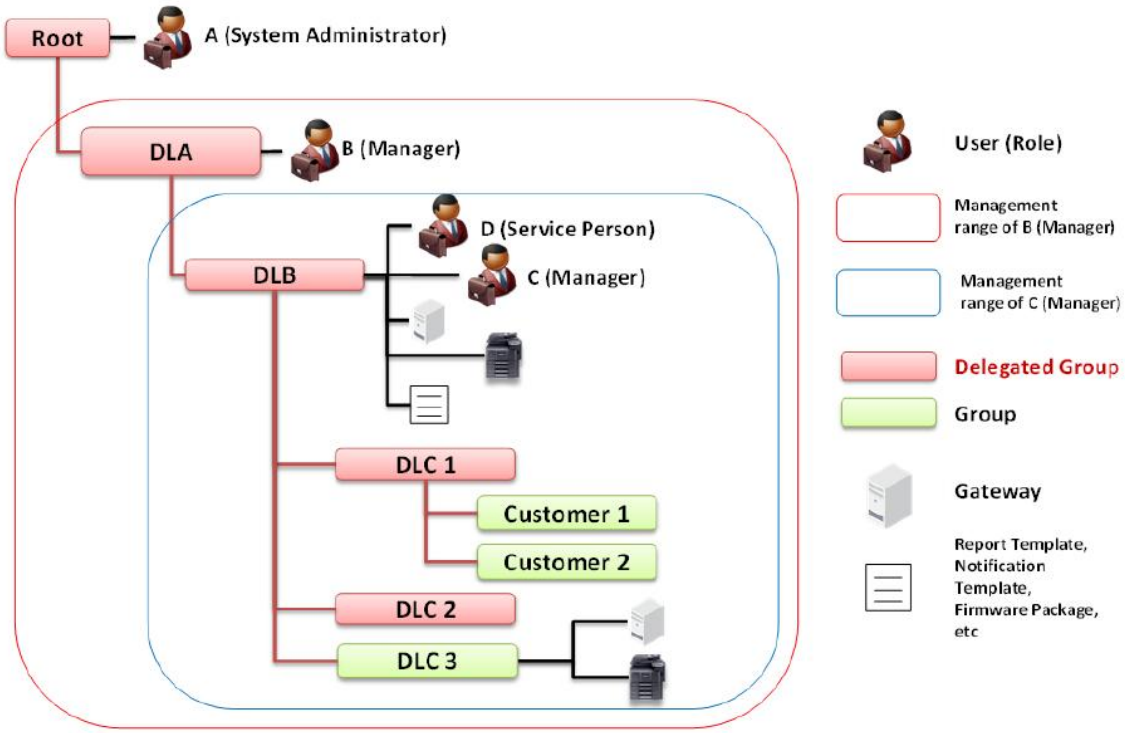

Abbildung 2: Datenmanagement

4.1.2. Verwaltung der Benutzerkonten

Benutzerkonten werden innerhalb einer Gruppe erstellt und verwaltet.

Jedem Benutzer wird eine der folgenden Rollen zugewiesen.

In der Reihenfolge Systemadministrator, Manager, Service, Analyst, und Kunde umfassen die Berechtigungen einer der Benutzergruppe stets auch die der untergeordneten Gruppen.

- Systemadministrator
- Manager
- Service
- Analyst
- Kunde

- **Systemadministrator**

  Systemadministratoren haben die höchste Zugriffsstufe aller Benutzerkonten. Die Rolle ist Nutzern zugeordnet, welche auf der höchsten Stufe der Hierarchie Strukturen stehen. Der Systemadministrator verwaltet den UTAX FM. Somit führt dieser Konfigurationen, Änderungen, Wartungen und Monitoring durch.

- **Manager**

  Der Manager verwaltet und pflegt untergeordnete Gruppen der Gruppe, für die er zuständig ist.

  Manager können neue Gruppen hinzufügen bzw. Gruppen, die zu der Gruppe gehören, für die sie zuständig sind, bearbeiten oder löschen. Außerdem können Manager neue Benutzerkonten hinzufügen, Benutzerkonten bearbeiten und löschen sowie den Status ändern. Wird ein Benutzerkonto gelöscht, können Manager darüber hinaus die Berichtsplanung, Benachrichtigungskriterien sowie Vorlagen, die von ihnen verwaltet werden, einem anderen Benutzer in der gleichen Gruppe übertragen.

- **Service**

  Der Service kann Wartungsarbeiten (Firmwareupgrades, Snapshots, usw.) durchführen und neue Benutzer auf Kundenseite anlegen.

- **Analyst**

  Der Analyst kann Berichte über den Status eines Gerätes (z.B. Zählerstände) erstellen und somit die Kundenumgebung analysieren. Analysten können eine Berichtsvorlage erstellen und mit dieser den Bericht ausgeben. Dieser kann mit Benutzern derselben delegierten Gruppe ausgetauscht werden. Im Gegensatz zum Service können Analysten keine Wartung an dem Gerät durchführen.

- **Kunde**

  Der Kunde verwaltet Geräte am Kundenstandort. Zudem können Kunden eine Berichtsvorlage erstellen und veröffentlichen, die vom Kunden verwendet wird.

Kennworteinstellungen

Bei der anfänglichen Einrichtung eines Benutzerkontos in UTAX Fleetmanager sendet UTAX Fleetmanager per E-Mail eine Nachricht an den Benutzer. Diese E-Mail enthält einen Benutzernamen, ein temporäres Kennwort sowie einen Link zur Service-URL. Falls das Benutzerkonto erstellt wurde, aber einen ungültigen Status aufweist, sendet UTAX Fleetmanager erst dann eine E-Mail-Nachricht an den Benutzer, wenn das Konto gültig ist.

Das temporäre Kennwort ist 24 Stunden gültig. Wenn sich Benutzer erstmals mit ihrem Benutzernamen anmelden, werden sie zur Änderung des Kennworts aufgefordert. Sobald Benutzer das Kennwort ändern, wird das temporäre Kennwort ungültig.

Diese strikte Sicherheitseinstellung verhindert, dass das Kennwort von böswilligen Personen gestohlen wird.

4.1.3. Richlinie für die Datenzugriffskontrolle

Zugriff auf in UTAX FM gespeicherte Daten wird durch die Benutzerrolle sowie den mit der Gruppe des Benutzers verknüpften Zugangscode kontrolliert. Der Zugriff auf Daten wird anhand der Benutzerrollen streng beschränkt.

Manager können standardmäßig auf alle Daten ihrer Gruppe sowie alle Daten in untergeordneten Gruppen zugreifen. Zugriffsrechte können jedoch später vom Manager der jeweiligen Gruppe und übergeordneten Gruppen eingerichtet oder geändert werden.

Service kann auf Gerätedaten ihrer eigenen und der untergeordneten Gruppen zugreifen. Die Zugriffsrechte müssen alleridngs durch einen Manager zugewiesen werden. Die Gerätedaten umfassen Geräteeigenschaften, Snapshots, Bilddaten, Erfassungsdaten und Bedienpanelscreenshots.

Analysten und Kunden können auf die Geräteeinstellung in ihrer Gruppe und untergeordneten Gruppen zugreifen. Zugriffsrechte müssen jedoch vom Manager festgelegt werden.

Benutzer (**Manager, Service, Analyst** und **Kunde**) können nur dann auf Daten in verschiedenen Gruppen zugreifen, wenn vom Manager der betroffenen Gruppe ein externer Zugang für die Benutzer oder ihre übergeordneten Gruppen eingerichtet wurde. Diese Einstellung kann durch Eingabe der E-Mail-Adresse des Benutzers und der eindeutigen externen Zugangscodes, die der oben genannte Manager im Assistenten für die Bearbeitung von Benutzern erstellt, vorgenommen werden.

System Administrator, Manager und Service haben Zugriff auf Protokolldaten während Analysten und Kunden keinen Zugriff auf diese Daten haben

4.2. Registrierung bei UTAX FM

Damit UTAX FM ein MFP-Gerät über UTAX FM Device/ UTAX FM Gateway/ UTAX FM Mobile verwalten kann, muss im Voraus eine gegenseitige Registrierung zwischen UTAX FM und UTAX FM Device/ UTAX FM Gateway/ UTAX FM Mobile ausgeführt werden.

Wenn Geräte in UTAX FM registriert werden, können sie den Status „Ausstehend“ oder „Verwaltet“ aufweisen. Der Status hängt jedoch von den registrierten Komponenten ab. Im Folgenden wird als Beispiel das Verhalten für eine Art von UTAX FM Device-Registrierung beschrieben.

- Wird die Registrierung nur mit dem Zugangscode der Gruppe vorgenommen, lautet der Status „Ausstehend“. Um eine Änderung in „Verwaltet“ zu bewirken, muss ein dazu autorisierter Benutzer den Status ändern.
- Wird die Registrierung mit dem Benutzernamen, Kennwort und Zugangscode vorgenommen, lautet der Status „Verwaltet“.

Indem sich Benutzer identifizieren müssen, um ein Gerät als „Verwaltet“ registrieren zu können, wird unbefugter Zugriff verhindert.

Die Zugriffsprotokolle (wer hat wann wo zugegriffen) lassen sich verwenden, um nicht autorisierte Zugriffsversuche zu verfolgen.

4.3. Verbindungsmodus

Bei der Registrierung von UTAX FM Device/ UTAX FM Gateway in UTAX FM Manager können Benutzer einen Verbindungsmodus auswählen: Verwaltungsmodus oder Überwachungsmodus. Benutzer, die eine UTAX FM Device verwenden, können ausschließlich den Überwachungsmodus wählen. Beim Verwaltungsmodus kann der Benutzer die Ablaufzeit so einrichten, dass ein automatischer Wechsel vom Verwaltungs- in den Überwachungsmodus erfolgt; so lässt sich die Länge der Netzwerkverbindung mit UTAX FM Manager beschränken.

Im Verwaltungsmodus nutzt das UTAX FM Device eine bidirektionale Verbindung. Zwischen UTAX FM Device/ und UTAX FM Manager wird eine XMPP- oder ine MQTT Verbindung hergestellt.

Im Überwachungsmodus wird nur dann eine unidirektionale Verbindung von UTAX FM Device/ UTAX FM Gateway zu UTAX FM Manager eingerichtet, wenn die Gerätedaten wie Zähler, Tonerstand, Geräteprotokoll und Gerätemeldungen in UTAX FM Manager hochgeladen werden. Es wird weder eine XMPP- noch eine MQTT-Verbindung zwischen UTAX FM Device/ UTAX FM Gateway und UTAX FM Manager hergestellt. Zugriff von UTAX FM Manager auf UTAX FM Device/ UTAX FM Gateway wird blockiert. Das verhindert ein Eindringen von UTAX FM Manager über das Internet in das Kundennetzwerk und kann zudem die Netzwerklast verringern. UTAX FM Device/ UTAX FM Gateway können die Datenressourcen von UTAX FM Manager von der Kundenumgebung getrennt halten. Ein IT-Administrator kann die Sicherheit der UTAX FM -Umgebung erhöhen. Der Überwachungsmodus hilft IT-Administratoren bei der Verwaltung eines zuverlässigen UTAX FM-Sicherheitsstatus.

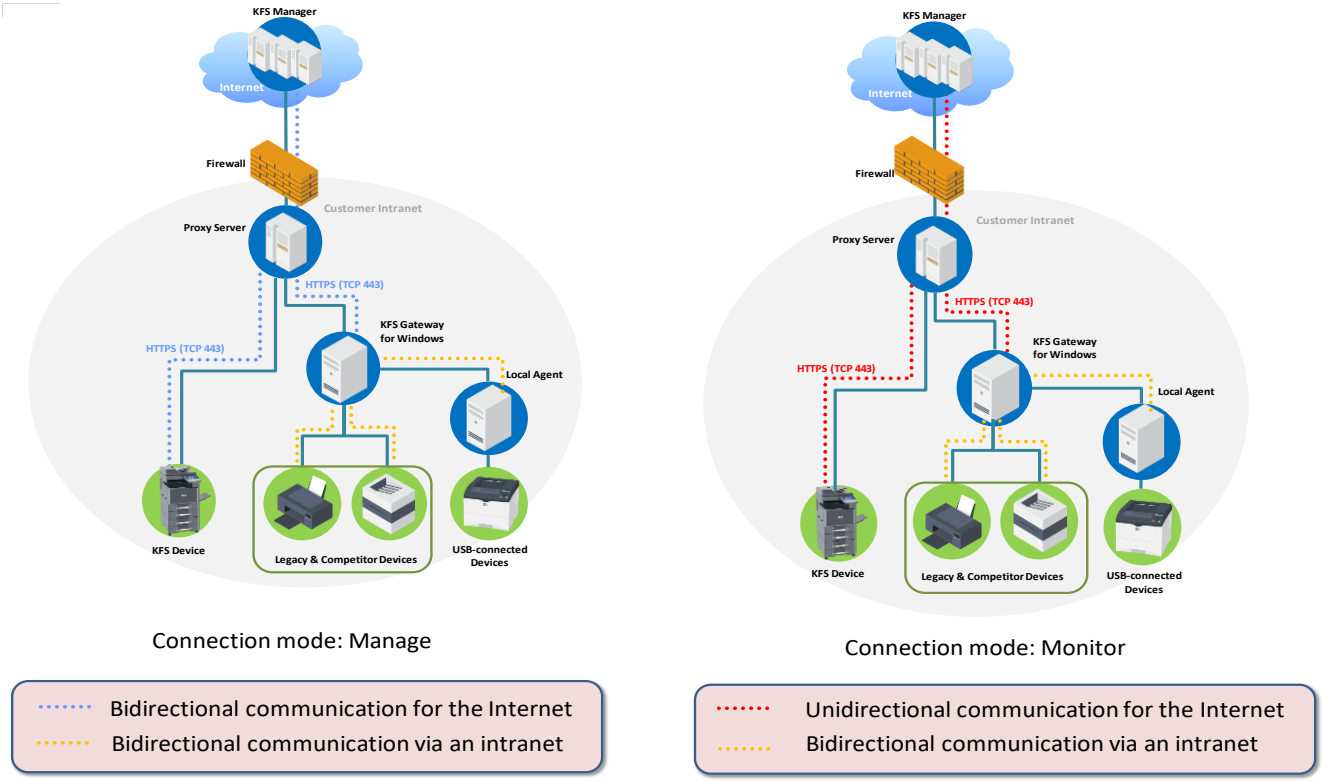

Abbildung 3: Verbindungsmodus

4.4. Zentraler Punkt für ausgehende Verbindungen

UTAX FM Gateway unterstützt mit einer Möglichkeit zur Konsolidierung des Kontaktpunkts mit dem externen Internet an einer Stelle einen zentralen Punkt für ausgehende Verbindungen. Daher muss der Whitelist der ausgehenden Firewall lediglich eine Adresse hinzugefügt werden.

Das stellt eine ideale Alternative für sichere Standorte dar, die Bedenken wegen der Sicherheit haben und deren Geräte direkten Zugriff auf das öffentliche Netzwerk haben.

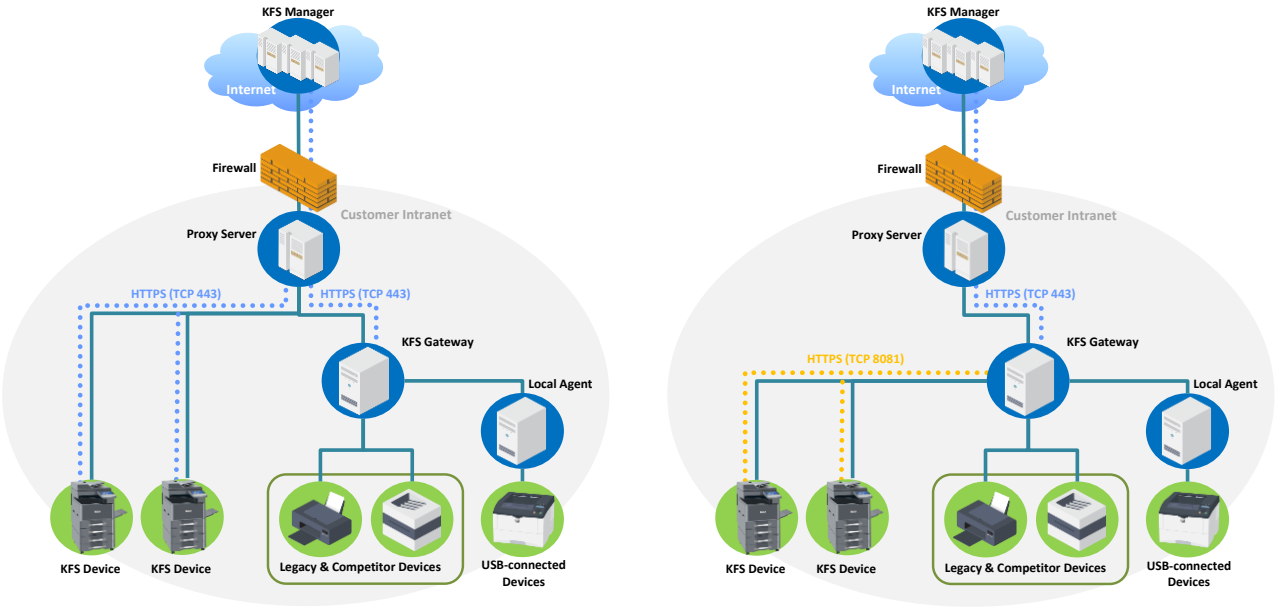

Abbildung 4: Verbindungsvergleich mit (rechte Abbildung) und ohne (linke Abbildung) den zentralen Punkt für ausgehende Verbindungen

Hinweis: Die Verfügbarkeit von UTAX FM Gateway variiert nach Region.

4.5. Automatische Upgrades für UTAX FM Gateway

Die automatische Upgradefunktion stellt eine Sicherheitsverbesserung dar, die täglich dafür sorgen soll, dass die Gateway-Version auf dem neuesten Stand und der Betrieb von UTAX FM Gateway sicher und stabil sind. Nach der Aktivierung sucht die automatische Upgradefunktion jeden Tag zu einer angegebenen Zeit bzw. basierend auf der Zeit der anfänglichen Gateway-Registrierung nach Softwareupdates. Dadurch werden manuelle Eingriffe überflüssig. Die Einstellung wird im Bereich „Sicherheitseinstellungen“ auf der Registerkarte „UTAX FM Gateway – Einstellungen“ vorgenommen. Aus Sicherheits- und Komfortgescihtspunkten wird eine Verwendung der automatischen Upgradefunktion für UTAX FM Gateway empfohlen.

4.6. Datenanonymisierungsmodus durch UTAX FM Gateway

UTAX FM Gateway (NetGateway) Informationen Anonymisierungsmodus kann nur während der Installation aktiviert werden. Wenn er aktiviert ist, werden die Erkennungseinstellungen nicht mit dem UTAX FM Manager synchronisiert.

Um unbefugten Zugriff oder unbefugte Offenlegung zu verhindern, können Benutzer den Modus auf UTAX FM Gateway (NetGateway) so konfigurieren, dass die folgenden Geräteinformationen und UTAX FM Gateway (NetGateway)-Informationen nicht an UTAX FM Manager gesendet werden:

- Geräteinformationen (z. B. IP-Adresse, Subnetzmaske, Standard-Gateway-IP-Adresse, DNS-

Serveradressen, Computer-/Hostname und Standort-/Standortinformationen)

- Informationen zum UTAX FM Gateway (NetGateway) (z. B. IP-Adresse, Subnetzmaske, Hostname, Standard-Gateway-IP-Adresse, Adresse des primären DNS-Servers und Adresse des sekundären DNS-Servers)

4.7. Identifizierung und Authentifizierung

Beim Zugriff auf UTAX FM müssen sich Benutzer mit ihrem registrierten Benutzernamen anmelden(*11)(*17)(*18)(*19). Nicht autorisierte Benutzer können nicht auf UTAX FM zugreifen.

Zugriffsdaten werden bei Protokollierung erfasst und stehen für Prüfzwecke zur Verfügung.

Folgende Funktionen werden bei der Anmeldung als Sicherheitseinstellungen unterstützt.

(*11) Beachten Sie, dass die Benutzer dafür sorgen müssen, dass ihre Authentifizierungsdaten wie Kennwörter und in UTAX FM registrierte Benutzernamen vertraulich behandelt und aufbewahrt werden. Benutzer dürfen Authentifizierungsdaten nicht an Dritte weitergeben bzw. übertragen und müssen verhindern, dass andere Personen ihre Daten nutzen. Die Benutzer – und nicht UTAX – haften für alle Schäden, die durch eine unsachgemäße Handhabung, missbräuchliche Nutzung oder Verwendung der Authentifizierungsdaten seitens einer dritten Person entstehen.

Ab V2.1 kann eine Zwei-Faktor-Authentifizierung aktiviert werden. Benutzer können eine Methode auswählen, mit der sie einen Authentifizierungscode abrufen möchten, indem sie entweder die E-Mail-Methode (*17) oder – ab V2.2 - die Authentifizierungsanwendung (*18) verwenden, wie in der Tabelle 7 beschrieben:

Tabelle 7: Authentifizierungs-Methoden

	E-Mail Methode(*17)	Authentifizierungs-Anwendung(*18)
Methode zur Generierung des Authentifizierungscodes	Manueller Vorgang zur Neugenerierung im UTAX FM-Manager (Ein Authentifizierungscode wird an die E-Mail-Adresse des vorregistrierten Benutzers gesendet.)	Automatische Aktualisierung der Authentifizierungs-Anwendung (Die Authentifizierungs-Anwendung muss zuerst auf dem Mobiltelefon des Benutzers installiert werden. Anschließend wird eine 6-stellige Zahl generiert und in den UTAX FM Zwei-Faktor-Authentifizierungsbildschirm eingegeben.)
Ablaufintervall für den Authentifizierungscode	10 Minuten	30 Sekunden
Länge des Authentifizierungscodes	6-stellige Nummer	6-stellige Nummer

Auf diese Weise schützt die Zwei-Faktor-Authentifizierung mit zeitlich begrenzten Authentifizierungscodes (d. h. das Ablaufintervall des Authentifizierungscodes) sensible Daten, die über UTAX FM verarbeitet werden sowie die Kommunikation mit dem UTAX FM.

(*19) Eine erneute Authentifizierung ist erforderlich, bevor die Authentifizierungsinformationen des Benutzers bearbeitet werden können. Diese Funktion verhindert, dass ein Konto von einer böswilligen Person gehackt wird, die die E-Mail-Adresse des autorisierten Benutzers in eine nicht autorisierte E-Mail-Adresse ändert.

4.7.1. Kontosperrungsrichtlinie

Nach einer vordefinierten Anzahl von fehlgeschlagenen Anmeldeversuchen, wird das Benutzerkonto für einen bestimmten Zeitraum gesperrt.

Wie Tabelle 8 zeigt, wird das Konto bei Erreichen des Schwellenwerts für die Kontosperrung (drei fehlgeschlagene Anmeldeversuche) gesperrt. Nach 30 Minuten wird das Konto bei dieser Einstellung wieder entsperrt.

Tabelle 8: Kontosperrungsrichtlinie

Zahl der aufeinander folgenden fehlgeschlagenen Anmeldeversuche	3 Mal
Zeitpunkt der automatischen Entsperrung	30 Minuten später

Durch die Einrichtung einer Kontosperrungsrichtlinie kann UTAX FM vor dem Knacken von Kennwörtern geschützt werden.

4.7.2. Anmelderichtlinie

Diese Richtlinie dient dazu, die Nutzung von UTAX FM durch unbefugte Benutzer zu verhindern. Selbst wenn UTAX FM von einem berechtigten Benutzer genutzt wird, wird dieser 12 Stunden nach der Anmeldung abgemeldet und muss sich erneut anmelden. Die Sitzungsdauer beträgt 12 Stunden.

Tabelle 9: Anmelderichtlinie

Verfügbarkeit in der Version	UTAX FM V2.4	UTAX FM V2.5
Ablaufzeit der Anmeldesitzung	7 Tage	12 Stunden

4.7.3. Kennwortrichtlinie

Benutzer müssen ein starkes Kennwort verwenden, das sich schwer analysieren lässt und die UTAX FM - Kennwortrichtlinie erfüllt. Die vorgeschriebene Länge und Komplexität von Kennwörtern können Sie Tabelle 10 entnehmen.

Tabelle 10: Kennwortrichtlinie

Kennwortlänge	Mindestens 8 Zeichen Passwörter mit bis zu 64 Zeichen zulassen
Verwenden Sie Passwörter nicht mehrfach	Es kann nicht auf dasselbe Passwort wie zuvor geändert werden
Benutzername/E-Mail-Adresse nicht verwenden	Darf weder die Benutzer-ID noch die E-Mail-Adresse des Benutzers enthalten (beachten Sie, dass auch der Teil der E-Mail-Adresse vor dem „@“-Zeichen nicht verwendet werden darf).
Verwenden Sie keine gängigen Passwörter	Lehnen Sie Passwörter ab, die in der folgenden Liste gängiger Passwörter aufgeführt sind: SecLists/Passwords/Common-Credentials/10k-most-common.txt at master · danielmiessler/SecLists · GitHub Darf keine der folgenden Wörter enthalten, die sich auf UTAX FM beziehen: kyocera | ecosys | taskalfa | kfs | fleet | services | mobile | netgateway | device | registration | diagnostic | tool | drd |data | collection | dct | kdc

Kennwörter, die die Anforderungen der Kennwortrichtlinie nicht erfüllen, sind unzulässig. Die Richtlinie verhindert, dass Benutzer einfache Kennwörter verwenden, und schützt vor unbefugten Zugriffen durch Dritte.

Das Kennwort ist ein Jahr lang gültig. Der Benutzer kann sich nicht mehr anmelden, wenn sein Kennwort abgelaufen ist.

4.8. Prüfprotokolle

UTAX FM zeichnet Prüfprotokolle für verschiedene Ereignisse auf. Dadurch entsteht ein Datensatz, mit dem sich prüfen lässt, ob UTAX FM sicher ist. Benutzer, die Zugriff auf Prüfprotokolle in ihrer Umgebung haben, sind auf erforderliche Benutzer beschränkt.

4.8.1. Prüfprotokolle vom UTAX FM

Bei folgenden Ereignissen wird vom UTAX FM ein Prüfeintrag erstellt(*15):

- Erfolgreiche/fehlgeschlagene Benutzeridentifizierung und -authentifizierung

- Hinzufügen/Bearbeiten/Verschieben/Löschen von Gruppen und Benutzerkonten
- Registrieren/Beenden/Verschieben/Löschen von UTAX FM Device/ UTAX FM Gateway/ UTAX FM Mobile
- Zurücksetzen eines Benutzerkennworts per E-Mail
- Löschen/Archivieren von Aufgaben
- Exportieren von Geräteprotokollen
- Herunterladen erfasster Daten
- Importieren/Exportieren von Backup-Daten
- Importieren von Gerätedaten
- Anfragen zur Verwendung des Remote-Bedienfelds
- Empfangen einer Genehmigung vom Remote-Bedienfeld eines Geräts
- Herstellen einer Verbindung zum Remote-Bedienfeld
- Trennen einer Verbindung zum Remote-Bedienfeld

4.8.2. Prüfprotokolle vom UTAX FM Gateway

Bei folgenden Ereignissen erstellt UTAX FM Gateway einen Prüfeintrag(*15):

- Erfolgreiche/fehlgeschlagene Benutzeridentifizierung und -authentifizierung
- Zurücksetzung des Kennworts für den lokalen Administrator von UTAX FM Gateway
- Konfiguration der Wiederherstellungseinstellungen für ein Gerät
- Konfiguration der Sicherheitseinstellungen
- Beendigung inaktiver Sitzungen

Im Verlauf oben werden die Zeit und das Datum(*12) sowie das Ergebnis (erfolgreich/fehlgeschlagen) dargestellt. Im Fall einer Modifizierung oder Preisgabe von Daten können die Prüfprotokolle zur Untersuchung und Verfolgung des nicht autorisierten Zugriffs verwendet werden. Die Betriebsprotokolle werden zur Pflege von Prüfpfaden gespeichert.

(*12) Ein Zeitstempel für Prüfprotokolle gibt an, wann ein Vorgang stattgefunden hat. Der Zeitstempel ist stets mit der genauen Zeit in Azure synchron. Dabei wird die Zeitzone verwendet, die auf dem Benutzer-PC eingerichtet ist.
(*15) Wird spätestens 67 Tage nach Erstellung des Eintrages wieder gelöscht (inklusive der E-Mail Protokolle).

4.9. Schutz gespeicherter Daten

Die wichtigen Datenressourcen von UTAX FM müssen geschützt und dürfen nicht freigegeben werden bzw. verloren gehen. Mithilfe der im Folgenden beschriebenen Funktionen implementiert UTAX Maßnahmen zum Schutz gespeicherter Datenressourcen sowie Unterstützung für die Wiederherstellung von Daten.

4.9.1. Verschlüsselung/Hashing

Die vertraulichen Datenressourcen, die in UTAX FM -Komponenten wie UTAX FM(*16), UTAX FM Gateway, UTAX FM Device und UTAX FM Mobile gespeichert sind, werden unter Verwendung der folgenden Verschlüsselungsalgorithmen verschlüsselt. Die vertraulichen Datenressourcen, die in UTAX FM Mobile gespeichert werden, beinhalten zum Beispiel das Benutzerkennwort für UTAX FM, ein Auffrischungstoken für die Einrichtung eines sicheren Kommunikationskanals mit UTAX FM sowie ein Kennwort für die Authentifizierung beim Proxyserver. Diese vertraulichen Daten werden mittels Verschlüsselung geschützt.

Darüber hinaus werden sensible Informationen, wie z. B. das Anmeldepasswort und die im UTAX FM und UTAX FM Gateway gespeicherten Daten mit den in Tabelle 12 angegebenen Hash-Algorithmen abgesichert.

Die Datenbestände sind gegen Informationslecks durch unberechtigte Dritte geschützt.

(*16) Mit Transparenter Datenverschlüsselung (TDE) verschlüsseln Sie SQL Server- und Azure SQL-Datenbank-Dateien im archvierten Zustand.

Tabelle 10: Verschlüsselungsstärke

Verschlüsselungsalgorithmus	AES (Advanced Encryption Standard)
Schlüssellänge (Bit)	256

Tabelle 11: Schlüsselerzeugung und Verwaltungsmethode

Systemname	Schlüssellänge	Schlüsselerzeugung und Verwaltungsmethode
UTAX FM	128 Bit	Schlüssel werden für jede Umgebung einzeln erzeugt und für jeden bereitgestellten Server eingerichtet. Schlüssel werden in der Software für die Konfigurationsverwaltung (Azure DevOps) gespeichert, in der lediglich der Bereitstellungstechniker verweisen kann.
UTAX FM Gateway (NetGateway)	256 Bit	Schlüssel werden bei Registrierung in UTAX FM erzeugt und in der lokalen Datenbank gespeichert.
UTAX FM Mobile (Android)	256 Bit	Schlüssel werden beim ersten Start der Anwendung nach ihrer Installation automatisch erstellt. Schlüssel werden in der zu der Anwendung gehörenden Datenbank gespeichert.
UTAX FM Mobile (iOS)	256 Bit	Schlüssel werden zuvor erzeugt und in die Anwendung eingebettet (bei allen Geräten gleich).
UTAX FM Device	256 Bit	Für jedes Gerät werden beim Start Schlüssel erzeugt, sodass eindeutige Nummern für einzelne Geräte entstehen (unter Einsatz des eigenen Algorithmus von KYOCERA Documents Solutions), und im flüchtigen Speicher der Geräte gespeichert.

Tabelle 12: Hashing – Hash Algorithmus

System Name	Hash Algorithmus
UTAX FM	Salted SHA -256
UTAX FM Gateway (NetGateway)	Unsalted SHA -256

4.9.2. Daten-Backup

Die wichtigsten Datenressourcen werden als Backup-Daten gespeichert, damit sie sich bei Bedarf wiederherstellen lassen. Der Datenschutzplan basiert auf spezifischen Wiederherstellungszeiten.

Tabelle 13: Daten-Backup – Systemdaten & aktuelle Daten

	Zieltyp	Wiederherstellungszeit
Systemdaten & aktuelle Daten	RPO (Recovery Point Objective)	10 Minuten
	RTO (Recovery Time Objective)	4 Stunden

Systemdaten & aktuelle Daten	Backup-Planung:	Häufigkeit:	Aufbewahrungszeit
	- Transaktionsprotokoll	- Alle 10 Minuten	35 Tage
	- Differenzielles Backup	- Einmal am Tag	
	- Komplettes Backup	- Einmal am Tag	

Einmal pro Stunde werden alle Backups an einen sekundären Speicherstandort in einem anderen Rechenzentrum kopiert, um eine Wiederherstellung im Notfall zu ermöglichen.

Tabelle 14: Daten-Backup – Historische Daten

	Zieltyp	Wiederherstellungszeit
Historische Daten (Azure Storage-Daten)	RPO (Recovery Point Objective)	30 Minuten
	RTO (Recovery Time Objective)	48 Stunden

Historische Daten (Azure Storage-Daten)	Backup-Planung:	Häufigkeit:	Aufbewahrungszeit
	- Transaktionsprotokoll	- Alle 5 Minuten	30 Tage

Transaktionsprotokolle werden an drei verschiedenen Speicherorten innerhalb des gleichen Rechenzentrums gespeichert. Drei Protokolle werden in ein anderes Rechenzentrum kopiert, um eine Wiederherstellung im Notfall zu ermöglichen.

Die UTAX FM -Datensicherung nutzt die für Azure Storage verfügbare Georedundanz. Geo-redundant Storage (GRS) kopiert die Daten innerhalb eines Rechenzentrums. Es ist auch möglich, die kopierten Daten innerhalb einer primären Region in eine sekundäre Region zu kopieren. Dadurch wird sichergestellt, dass die Daten auch im Fall, dass die primäre Region nicht wiederhergestellt werden kann, dauerhaft erhalten bleiben. Tabelle 15 zeigt die Speicherorte für die Datensicherung.

Wenn die primäre Region (d. h. die Bereitstellungsumgebung) ausgewählt wird, wird die zugehörige

sekundäre Region automatisch festgelegt.

Tabelle 15: Daten-Backup – Historische Daten

Geographische Region	Primäre Region (Bereitstellungs-region)	Sekundäre Region
Europa (EU)	Westeuropa (Niederlande)	Nordeuropa (Irland)
USA (US)	Süd Zentral US (Texas)	Nord Zentral US (Illinois)
Asien Pazifik (AS)	Japan West (Osaka)	Japan Ost (Tokyo, Saitama)

4.10. Schutz übertragener Daten

UTAX FM sorgt beim Benutzerzugriff auf UTAX FM, der Übertragung von Daten zwischen UTAX FM und Geräten sowie Aufgaben für den Schutz der übertragenen Daten.

Damit sich in UTAX FM übertragene Daten nicht maskieren, abhören oder verändern lassen, werden die übertragenen Daten verschlüsselt. Außerdem authentifizieren sich UTAX FM -Komponenten gegenseitig.

4.10.1. Benutzerzugriff

Wenn ein UTAX FM -Benutzer über einen Webbrowser oder eine mobile Anwendung auf UTAX FM zugreift, wird ein authentifizierter Kommunikationskanal eingerichtet.

Kommunikation beim Zugriff auf UTAX FM über einen Webbrowser oder eine mobile Anwendung

UTAX FM -Benutzer können UTAX FM über die Client-UI des Webbrowsers bzw. die UI der mobilen Anwendung aufrufen – und zwar unabhängig von der Benutzerrolle. Wenn ein Benutzer auf UTAX FM zugreift, wird er stets identifiziert und authentifiziert. Wenn die Identifizierung und Authentifizierung erfolgreich verlaufen, kann der Benutzer je nach Rolle auf UTAX FM zugreifen. UTAX FM schützt die übertragenen Daten mittels HTTPS.

4.10.2. Datenübertragung

Über das Internet und das lokale Netzwerk (LAN) sendet und empfängt UTAX FM an bzw. von Geräten, die sich in der Umgebung eines Benutzers befinden, verschlüsselte Daten.

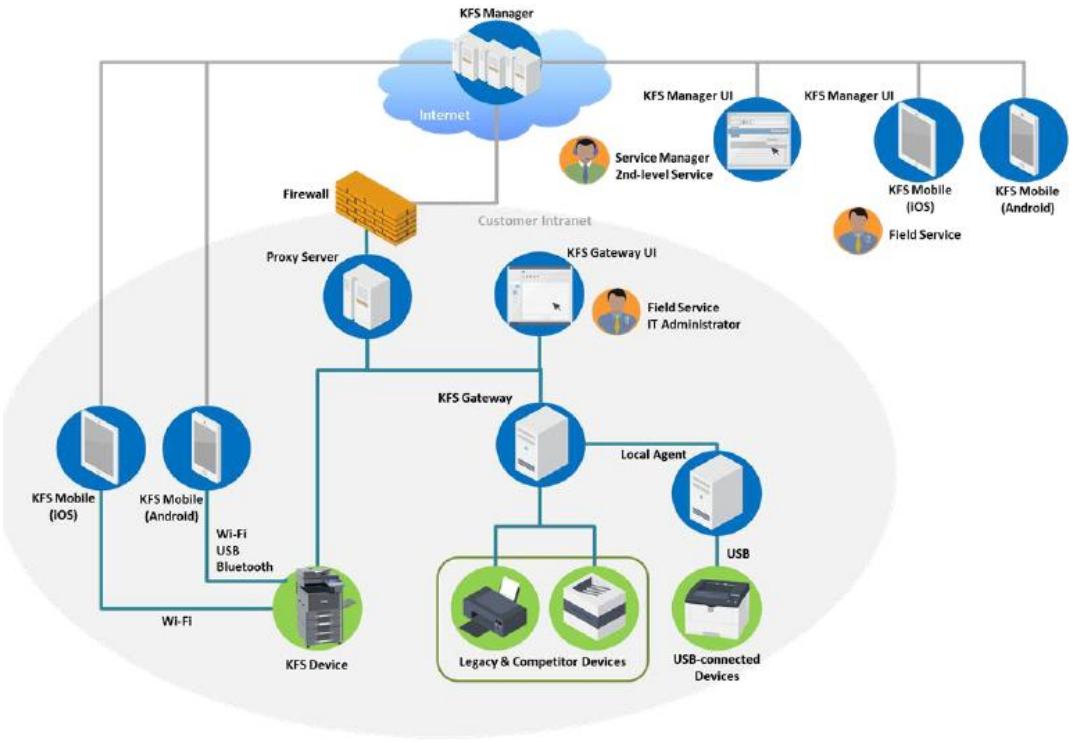

Abbildung 5: UTAX FM-Komponenten und Datenströme

Kommunikation mit UTAX FM über das Internet

UTAX FM -Netzwerkkommunikation wird vom XMPP/MQTT-Server und UTAX FM in der Cloud eingerichtet. Das XMPP/MQTT-Protokoll nutzt zur Übertragung das HTTPS-Protokoll. Das XMPP/MQTT-Protokoll dient der Kommunikation zwischen UTAX FM und dem XMPP/MQTT-Server in der Cloud bzw. der Kommunikation zwischen UTAX FM Gateway/ UTAX FM Device und dem XMPP/MQTT-Server via Firewall. Das HTTPS-Protokoll schützt die Daten im Kommunikationskanal, sodass über den normalen Pfad zur Datenübertragung keine Informationen an externe Quellen gelangen können.

Kommunikation mit UTAX FM via LAN

Der Webdienst zwischen UTAX FM Gateway und dem Gerät nutzt SOAP (WSDL) über HTTPS. Zwischen UTAX FM Gateway und dem Gerät wird SNMPv3 verwendet, dass die Authentifizierung und Verschlüsselung der im Netzwerk übertragenen SNMP-Pakete ermöglicht. Darüber hinaus steht für das oben genannte SNMPv3 ein Secure Hash Algorithm (z. B. SHA-2) zur Verfügung.

Die Übertragung von Daten über das lokale Netzwerk (LAN) wird durch Einrichtung eines Subnetzmaskenbereichs, einer IP-Adresse und eines Hostnamens kontrolliert. Es gibt keine unbeabsichtigte Übertragung über das Netzwerk.

Kommunikation mit anderen UTAX FM-Komponenten

Sichere Kommunikation zwischen UTAX FM Mobile und Geräten kann durch Pairing über eine verschlüsselte Bluetooth-, Wi-Fi Direct- oder USB-Verbindung erreicht werden – ohne Übertragung im lokalen Netzwerk.

Tabelle 16: Protokoll/Schnittstelle und Datenübertragung

Protokoll/Schnittstelle	Datenübertragung
• Extensible Messaging and Presence Protocol (XMPP)	➢ Kommunikation zwischen UTAX FM und dem XMPP-Server ➢ Kommunikation zwischen dem XMPP-Server und UTAX FM Gateway/ UTAX FM Device
• Message Queueing Telemetry Transport (MQTT)	➢ Kommunikation zwischen UTAX FM Manager und MQTT Server ➢ Kommunikation zwischen MQTT Server und UTAX FM Device
• Hyper Text Transport Protocol Secure (HTTPS)	➢ Kommunikation zwischen der Client-UI des Webbrowsers und UTAX FM ➢ Kommunikation zwischen UTAX FM Mobile und UTAX FM ➢ Kommunikation zwischen der Client-UI des Webbrowsers und UTAX FM Gateway ➢ Kommunikation zwischen UTAX FM und dem XMPP-Server ➢ Kommunikation zwischen dem XMPP-Server und UTAX FM Gateway/ UTAX FM Device ➢ Kommunikation zwischen dem Webbrowser und Relay-Server
• Simple Network Management Protocol (SNMPv3)	➢ Kommunikation zwischen UTAX FM Gateway und dem Gerät
• Simple Object Access Protocol (SOAP WSDL)	➢ Kommunikation zwischen UTAX FM Gateway und dem Gerät
• Bluetooth • Wi-Fi	➢ Kommunikation zwischen UTAX FM Mobile und UTAX FM Device
• USB	➢ Kommunikation zwischen UTAX FM Mobile (Android) und UTAX FM Device

4.10.3. Aufgaben

Wartungs- und Verwaltungsaufgaben können von UTAX FM -Benutzern über UTAX FM bzw. von Wartungspersonal erledigt werden, das die Büroumgebung des Kunden aufsucht. Diese Aufgaben dürfen nicht ohne Zustimmung des Kunden ausgeführt werden. Der Benutzerkreis, der zur Erledigung dieser Aufgaben in UTAX FM befugt ist, wird durch Identifizierung und Authentifizierung beschränkt. Daten, die im Rahmen der jeweiligen Aufgaben verarbeitet werden, werden durch Verschlüsselung der Kommunikationskanäle und gegenseitige Authentifizierungen geschützt.

Übertragung von Remote-Firmware-Upgrades

Hinweis:
Beim Hochladen von Firmware in UTAX FM wird die Softwarevalidierung mithilfe des ursprünglichen Algorithmus in der Firmware vorgenommen. Der Algorithmus des Pakets wird validiert, um die Integrität der Daten zu verifizieren; daher wird der Algorithmus vom Hauptcontroller im Gerät bei einem Firmware-Upgrade nach dem Herunterladen validiert.

Kommunikation bei Firmware-Upgrades von UTAX FM Gateway/ UTAX FM Device

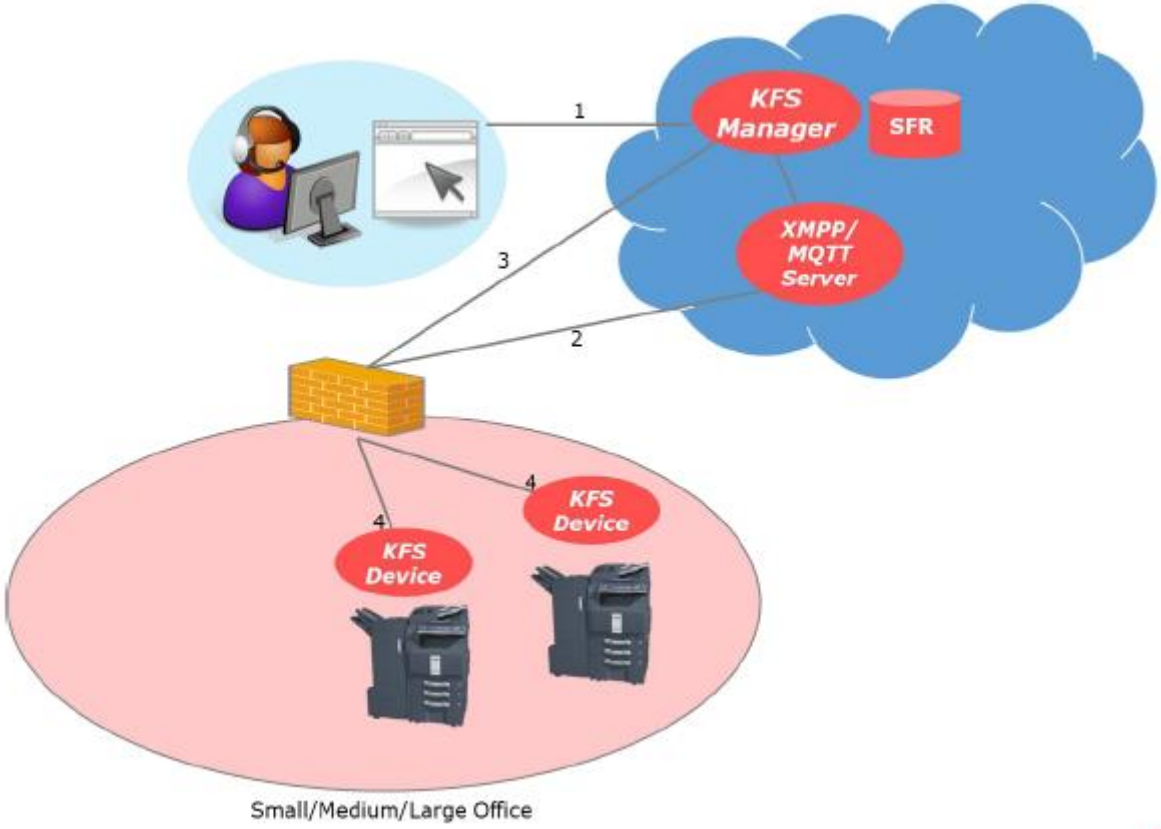

Abbildung 6: Kommunikationsfluss bei Firmware-Upgrades von UTAX FM Gateway/ UTAX FM Device

Wie in Abbildung 6 dargestellt, wird mit folgenden Schritten für die oben erwähnte sichere Übertragung und damit für sichere Firmware-Upgrades bei UTAX FM Gateway/ UTAX FM Device gesorgt.

1. Der Benutzer wählt über die Client-UI des Webbrowsers bzw. die UI der mobilen Anwendung von UTAX FM ein Firmwarepaket für das Gerät aus. Die Kommunikation zwischen der Client-UI des Webbrowsers und UTAX FM wird mit HTTPS geschützt.
2. UTAX FM Manager stellt über das XMPP/MQTT-Protokoll eine sichere Verbindung mit dem UTAX FM Device her und sendet einen Befehl für das Firmware-Upgrade an das UTAX FM Device.
3. UTAX FM Device lädt das Firmware-Paket sicher von UTAX FM Manager über HTTPS herunter.
4. UTAX FM Device aktualisiert die Firmware auf dem Gerät.

Kommunikation bei Firmware-Upgrades von UTAX FM Mobile

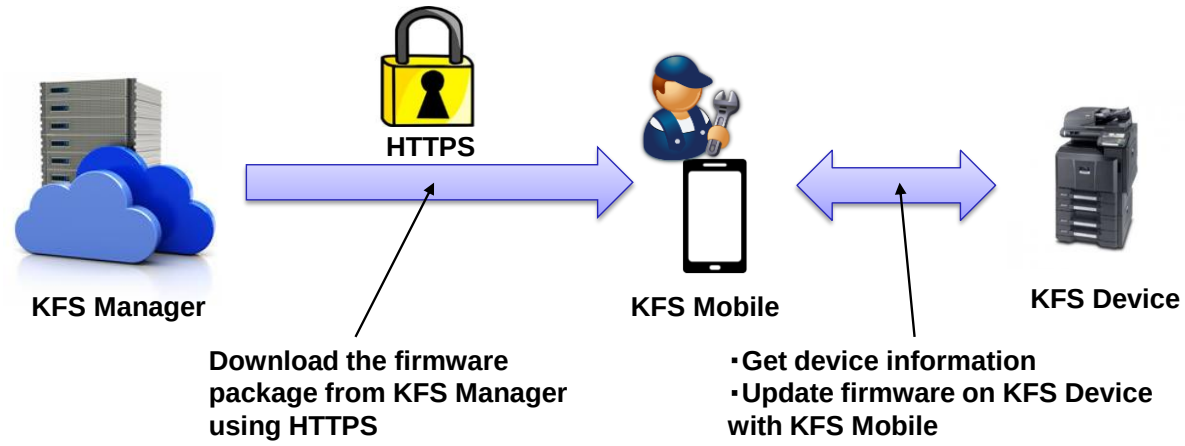

Abbildung 7: Kommunikationsfluss bei Firmware-Upgrades von UTAX FM Mobile

Falls sich das Netzwerk an einem Kundenstandort nicht über UTAX FM aufrufen lässt, können Firmware-Upgrades über ein Gerät mit UTAX FM Mobile vorgenommen werden. Dies wird mit folgenden Schritten unter Verwendung der oben erwähnten sicheren Verbindung erreicht:

1. Das Wartungspersonal nutzt UTAX FM Mobile, um in UTAX FM nach dem neuesten Firmwarepaket zu suchen.

   UTAX FM Mobile lädt das Firmwarepaket über HTTPS sicher von UTAX FM herunter.
2. UTAX FM Mobile stellt eine Verbindung mit UTAX FM Device her und sendet den Befehl für das Firmware-Upgrade nur dann an UTAX FM Device, wenn eine USB- oder Wi-Fi Direct-Verbindung verwendet wird, und aktualisiert anschließend die Firmware.

Kommunikation zur Firmware-Aktualisierung vom Gateway

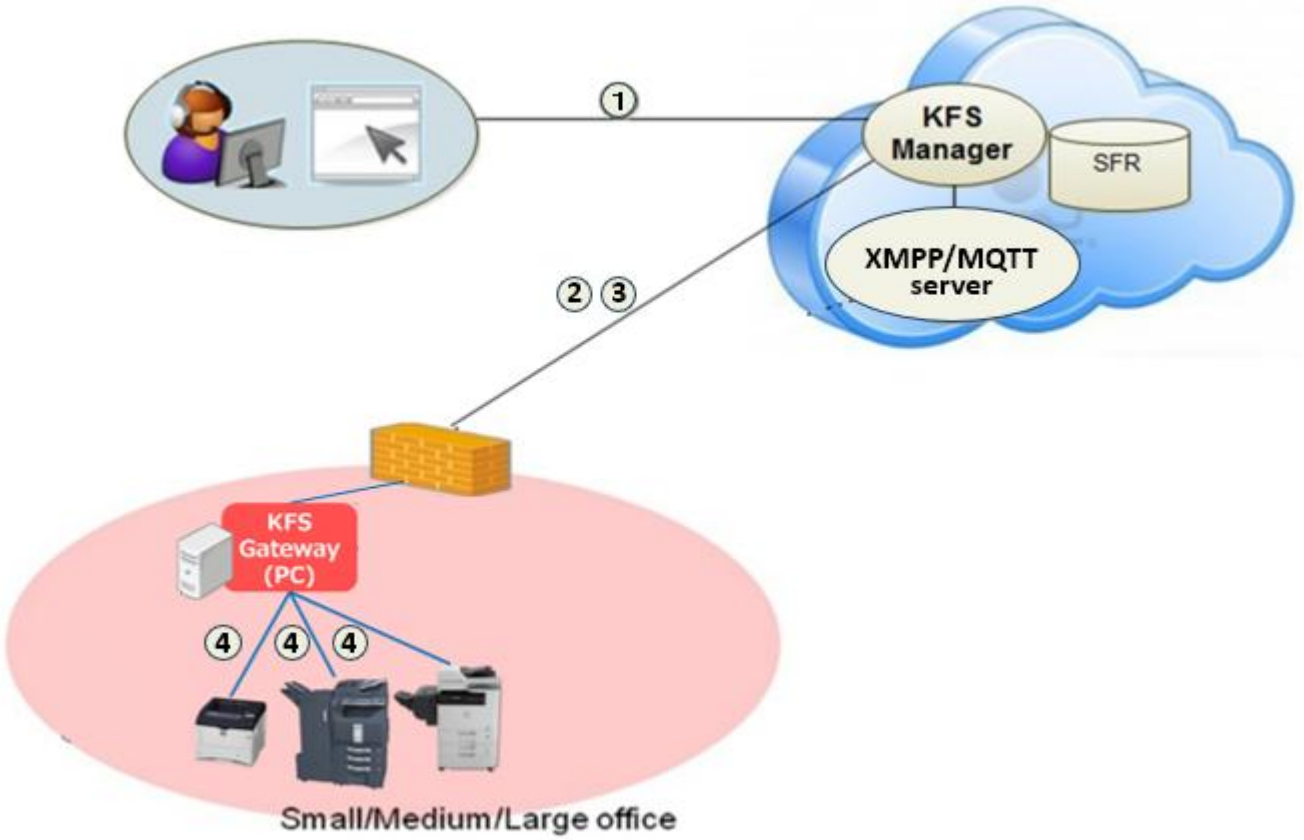

Abbildung 8: Kommunikation der Firmware-Aktualisierung vom Gateway

Wie in Abbildung 8 dargestellt, wird ein sicheres Firmware-Upgrade für Geräte über das Gateway mit der oben erwähnten Kommunikation durch die folgenden Schritte erzielt:

1. Der Benutzer wählt eine Firmware für ein Gerät über die Benutzeroberfläche des Webbrowsers oder der mobilen Anwendung aus. Die Kommunikation zwischen dem Client des Webbrowsers und Manager ist durch HTTPS geschützt.
2. Das Gateway initiiert die sichere Kommunikation über das HTTPS-Protokoll und ruft das Firmware-Upgrade ab.
3. Das Gateway lädt das Firmware-Paket über HTTPS sicher herunter.
4. Das Gateway initiiert die Kommunikation mit dem Gerät im lokalen Netzwerk, sendet den Firmware-Upgrade-Befehl an das Gerät und aktualisiert dann die Firmware.

Kommunikation der Remote-Geräte-Panel-Erfassung

UTAX FM bietet eine Remote-Geräte-Panel-Erfassungsfunktion, mit der das aktuelle Panel-Bild eines verwalteten Geräts auf der Benutzeroberfläche von UTAX FM angezeigt werden kann. Diese Funktion ruft Informationen zum Gerätepanel nur dann ab, wenn die Bestätigungsmeldung auf dem Panel des Zielgeräts angezeigt wird und die Zustimmung des Benutzers im Voraus erteilt wurde.

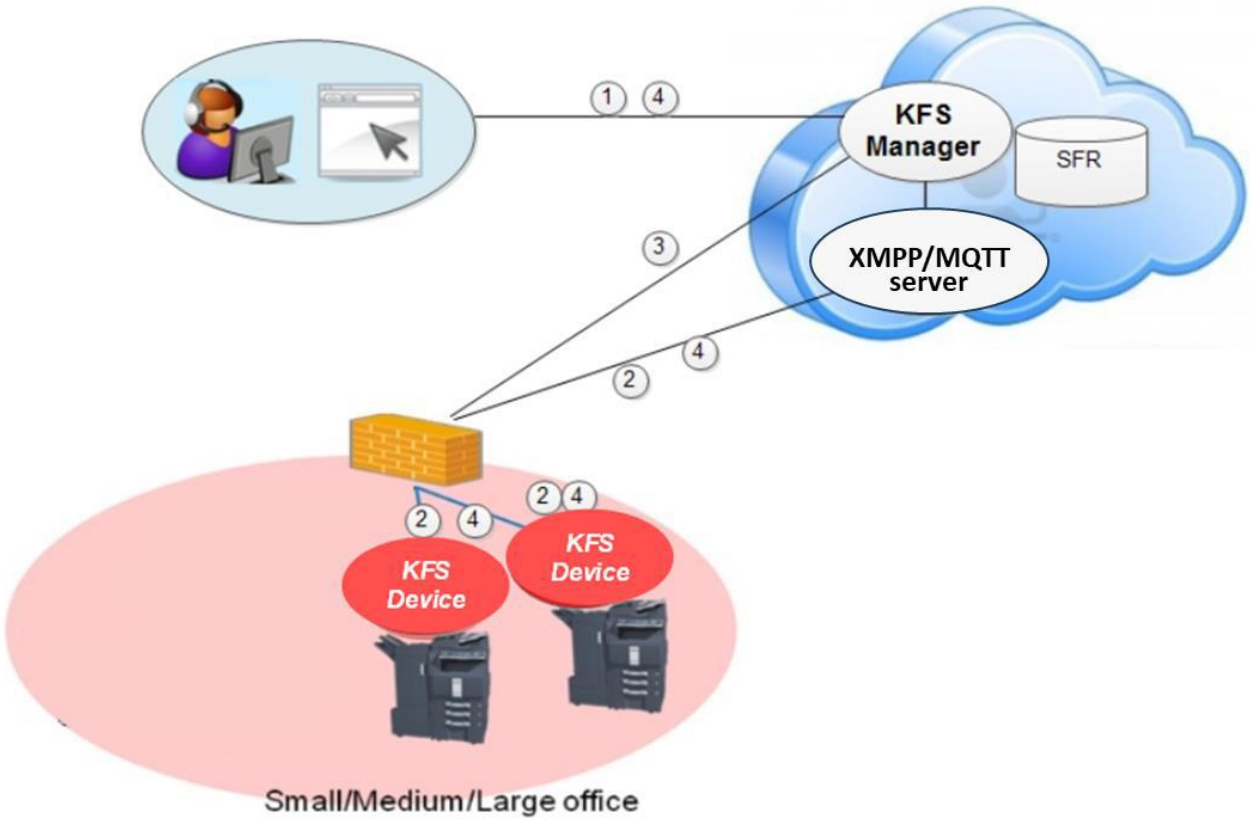

Abbildung 9: Kommunikationsfluss der Remote-Geräte-Panel-Erfassung

Wie in Abbildung 9 dargestellt, wird die Erfassung des Remote-Gerätepanels mit einer sicheren Kommunikation durch die folgenden Schritte erreicht:

1. UTAX FM-Benutzeranforderungen erfassen Gerätepanel-Informationen von der UTAX FM-Web-Benutzeroberfläche über HTTPS.
2. UTAX FM initiiert die Kommunikation mit dem UTAX FM-Gerät über eine sichere XMPP/MQTT-Protokollkommunikation und sendet erfasste Gerätepanel-Informationen an das UTAX FM-Gerät.
3. Das UTAX FM-Gerät sendet das Bild der aktuellen Panelinformationen des Geräts über HTTPS an UTAX FM. Das UTAX FM-Gerät aktualisiert das aufgenommene Bild jedes Mal, wenn der Bedienfeldbildschirm des Geräts aktualisiert wird.

4. UTAX FM kann diesen Prozess beenden, indem er über einen sicheren XMPP/MQTT-Kommunikationskanal einen Stoppbefehl an das UTAX FM-Gerät sendet.

Übertragung beim Abrufen von Snapshot-Daten eines Remotegeräts

Um UTAX FM -Benutzern die Ausführung von Gerätediagnosen zu erleichtern, können über die Web-UI von UTAX FM bzw. die UI der mobilen Anwendung folgende Snapshot-Daten von Geräten abgerufen werden.

- Statusseite
- Wartungsstatusseite
- Netzwerkstatusseite
- Wartungsbericht
- Anwendungsstatusseite
- Ereignisprotokoll
- USB-Protokoll
- Faxbericht
- Konfigurationsliste

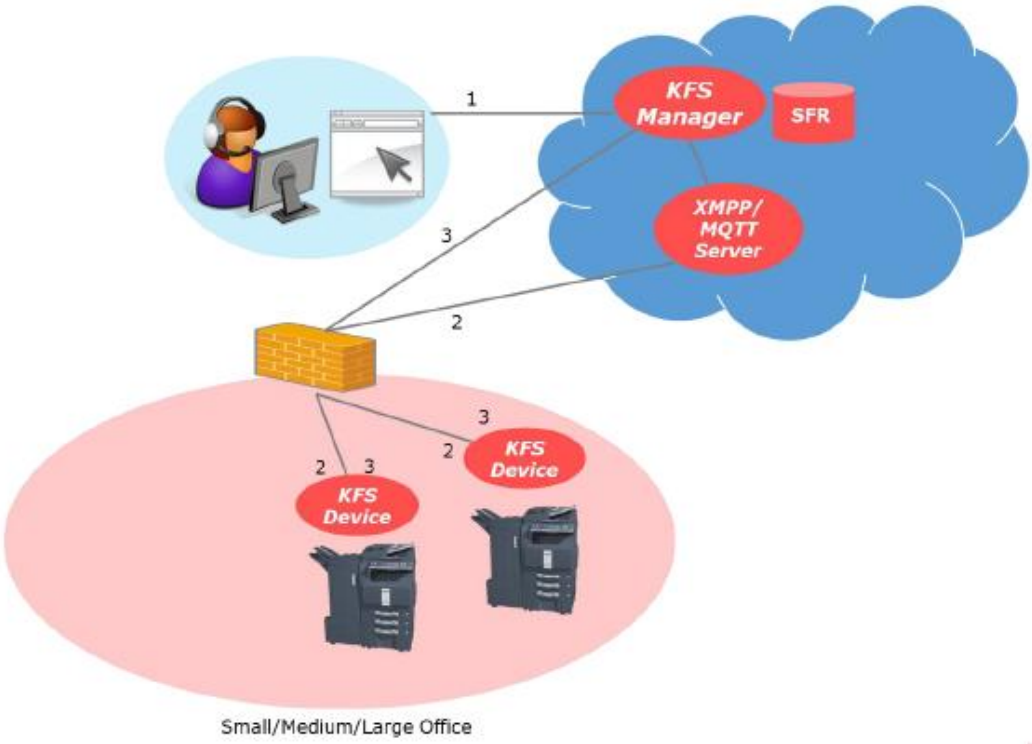

Abbildung 10: Kommunikationsfluss beim Abrufen von Remote-Snapshot-Daten

Wie in Abbildung 10 dargestellt, wird für die UTAX FM -Funktion zum Abrufen der Snapshots von Remotegeräten eine sichere Verbindung genutzt:

1. Ein Benutzer von UTAX FM fordert mit der Web-UI von UTAX FM bzw. der UI der mobilen Anwendung über HTTPS Snapshot-Daten eines Geräts an.
2. UTAX FM stellt über das sichere XMPP/MQTT-Protokoll eine Verbindung mit UTAX FM Gateway/ UTAX FM Device her und sendet den Snapshot-Befehl.
3. UTAX FM Gateway/ UTAX FM Device ruft Snapshot-Daten von einem bestimmten verwalteten Gerät ab und sendet diese Daten via HTTPS an UTAX FM.

Kommunikation von Remote HyPAS Management

UTAX FM erlaubt ein Remote-HyPAS-Management, inklusive Remote-Installation, -Deinstallation, -Aktivierung und -Deaktivierung der HyPAS-Anwendung in UTAX FM Device.

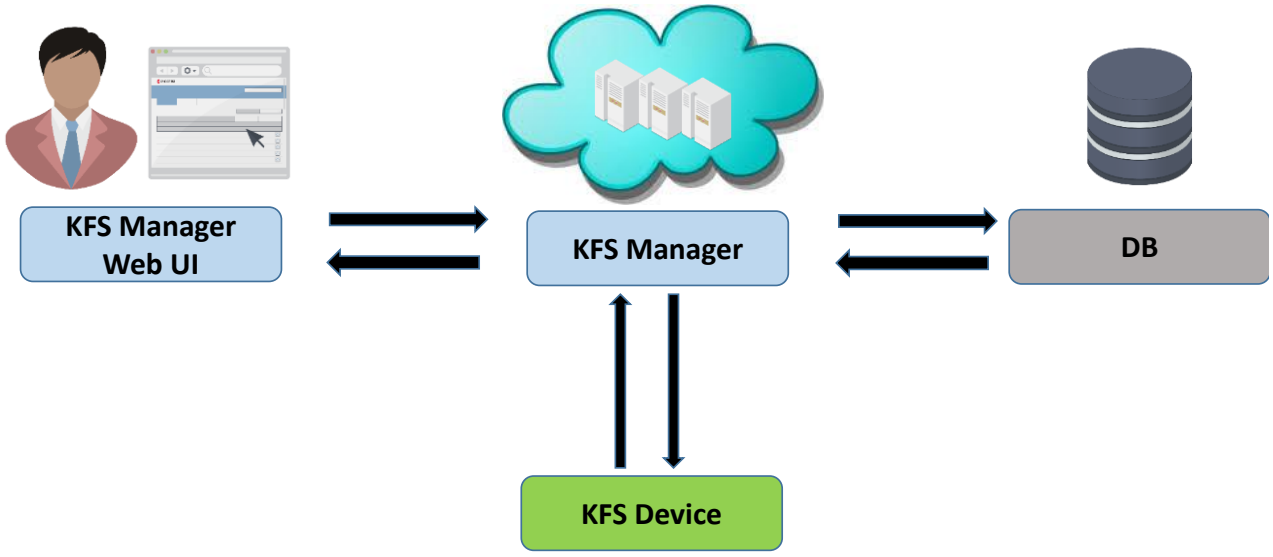

Abbildung 11: Kommunikationsfluss von Remote HyPAS Management

Wie in Abbildung 11 dargestellt, wird beim Remote-HyPAS-Management durch folgende Schritte für eine sichere Verbindung gesorgt:

1. Ein Benutzer von UTAX FM fordert über die Web-UI von UTAX FM via HTTPS eine Liste von HyPAS-Anwendungen an.
2. UTAX FM stellt über das sichere XMPP/MQTT-Protokoll eine Verbindung mit UTAX FM Device her und sendet UTAX FM Device eine Liste von HyPAS-Anwendungen zum Installieren/Deinstallieren/Aktivieren/Deaktivieren der HyPAS-Anwendungen. Der am HyPAS-Aktivierungsverfahren beteiligte Lizenzschlüssel wird ebenfalls sicher über XMPP/MQTT übertragen und vor der sicheren Speicherung in Azure DB mit AES verschlüsselt.

3. UTAX FM Device lädt das verschlüsselte HyPAS-Anwendungspaket über HTTPS von UTAX FM herunter (wenn die Anwendung installiert werden soll).
4. UTAX FM kann dieses Verfahren nach dem Empfang einer Meldung von UTAX FM Device beenden, sobald die Aktion abgeschlossen ist.

Kommunikation von Remote-Bedienfeldern

UTAX FM bietet eine Funktion für Remote-Bedienfelder, die nicht nur die aktuelle Darstellung des Bedienfelds eines verwalteten Geräts in UTAX FM anzeigen, sondern das Bedienfeld auch über UTAX FM verwalten kann. Mit dieser Funktion lässt sich das Bedienfeld eines Geräts bedienen, wenn im Bedienfeld des Zielgeräts die Bestätigungsmeldung angezeigt wird und der Benutzer im Voraus zugestimmt hat. Es ist möglich, den Benutzerkreis, der dem Administrator die Zustimmung geben kann, zu beschränken.

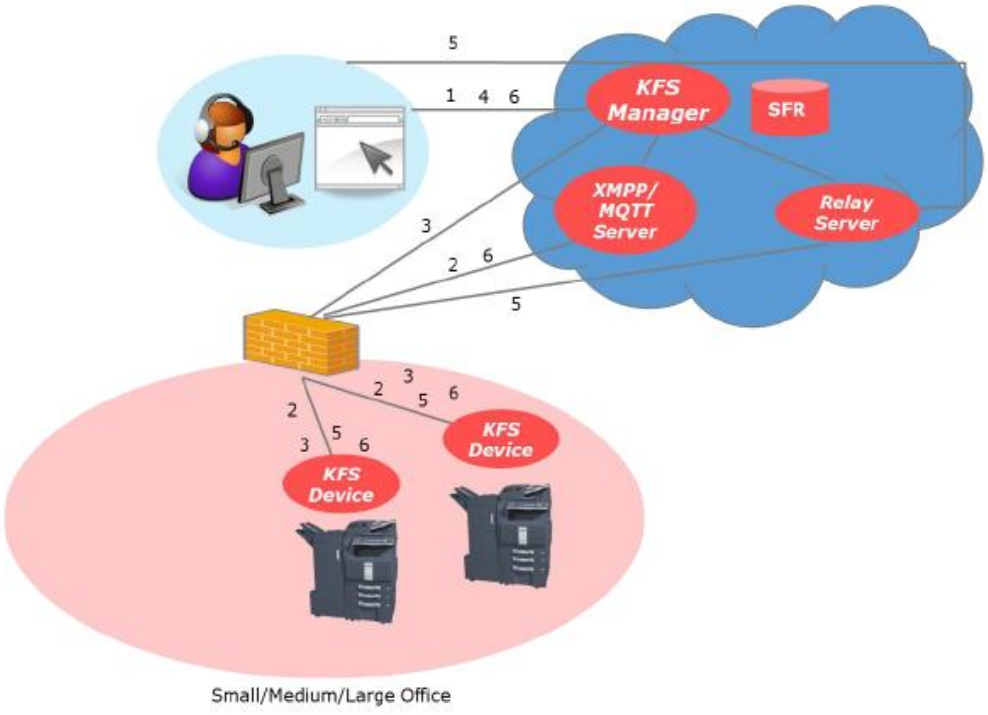

Abbildung 12: Kommunikationsfluss eines Remote-Bedienfelds

Wie in Abbildung 12 dargestellt, wird bei Remote-Bedienfeldern durch folgende Schritte für eine sichere Verbindung gesorgt:

1. Ein Benutzer von UTAX FM fordert mit der Web-UI von UTAX FM via HTTPS ein Remote-Bedienfeld an.

2. UTAX FM stellt über das sichere XMPP/MQTT-Protokoll eine Verbindung mit UTAX FM Device her und sendet eine Remote-Bedienfeldanfrage an UTAX FM Device.
3. UTAX FM Device ruft die Daten des Relay-Servers für UTAX FM über HTTPS ab und stellt eine Verbindung mit UTAX FM her, um das Remote-Bedienfeld zu erhalten.
4. Der Webbrowser des Benutzers ruft die Daten des Relay-Servers für UTAX FM über HTTPS ab und stellt eine Verbindung mit UTAX FM her, um das Remote-Bedienfeld zu erhalten.
5. Bilddaten und Betriebsbefehle werden zwischen dem Gerät und Webbrowser in beide Richtungen übertragen und ermöglichen somit eine Remotebedienung des Bedienfelds.
6. Mit UTAX FM lässt sich dieser Prozess beenden, indem über einen sicheren XMPP/MQTT-Kommunikationskanal ein Befehl zum Stoppen an UTAX FM Device gesendet wird.

5. KYOCERA’s Maßnahmen zum Schutz von UTAX FM

KYOCERA hat noch vor allen anderen MFP- und Druckerherstellern am 17. November 2017 eine ISMS-Zertifizierung für Cloudsicherheit (*[13]) erhalten. Seitdem wird die Zertifizierung nach einem Auditprozess, der die Einhaltung der Auditstandards bestätigt, kontinuierlich erneuert. Da Clouddienste heute in immer mehr Branchen Anwendung finden, werden mit Blick auf die neuesten internationalen Standards für Datenschutz und den Umgang mit personenbezogenen Daten strengere Sicherheitskontrollen und eine präzisere Verwaltung benötigt. In bestimmten Sektoren, in denen Clouddienste eingeführt werden (besonders in medizinischen Einrichtungen und Bildungseinrichtungen sowie in Unternehmen und Behörden, in denen wichtige Informationen verarbeitet werden), ist die Einhaltung von Sicherheitsstandards vorgeschrieben. Daher steigt der Bedarf nach objektiven Standards, die die Kontrollsysteme der einzelnen Anbieter von Clouddiensten zertifizieren.

KYOCERA setzt darauf, dass die Sicherheit von Daten, die im Rahmen der Dokumentenworkflows von Kunden erzeugt werden, rundum gewährleistet wird. KYOCERA hat im Rahmen seiner Bemühungen, Kunden sichere und flexible Clouddienste bereitzustellen, noch vor anderen Unternehmen in der Branche eine ISMS-Zertifizierung für Cloudsicherheit erhalten. Das Unternehmen wird die Qualität seiner Lösungsservices für Dokumente weiter verbessern und somit einen Beitrag zum Wachstum der Kundengeschäfte leisten.

Außerdem verfolgt KYOCERA ununterbrochen die aktuellsten Sicherheitstrends und Informationen über Schwachstellen. KYOCERA extrahiert und analysiert Sicherheitsanforderungen, die auf Sicherheitsanfragen von Kunden basieren, und nutzt diese in der aktualisierten Version von UTAX FM. KYOCERA entwickelt UTAX FM anhand der folgenden Entwicklungsrichtlinie: „Open Web Application Security Project (OWASP)“. KYOCERA sucht sorgfältig nach möglichen Sicherheitsrisiken, um für UTAX FM maximale Sicherheit zu erreichen. Vor der Veröffentlichung von UTAX FM-Produkten werden Sicherheitsdiagnosetests nicht nur bei KYOCERA, sondern auch von einem unabhängigen Anbieter durchgeführt.

Tabelle 18: Übersicht über die ISMS-Akkreditierung

Organisation	Kyocera Document Solutions Inc.	
Schema	Information Security Management System Zertifizierung (ISMS) (ISO/IEC 27001:2022 / JIS Q 27001:2023	ISMS Cloud Security Zertifizierung (ISO/IEC 27017:2015 / JIP ISMS517-1.0)
Datum der Verlängerung	22.10.2025	
Umfang der Akkreditierung	- Softwareentwicklungsabteilungen des Geschäftsbereichs Druckprodukte sowie des Geschäftsbereichs Produktion und Industriedruck Anforderungsanalyse, Entwicklung, Betrieb und Wartung von Firmware in MFPs/Druckern und Anpassung an Kundenanforderungen - Abteilungen für die Entwicklung und den Betrieb von Business-Lösungssoftware Anforderungsanalyse, Entwicklung, Betrieb und Wartung von Business-Lösungsprodukten und Anpassung an Kundenanforderungen	- Software-Forschungs- und Entwicklungsabteilungen, Unternehmensforschungs- und Entwicklungsabteilung (akkreditiert nur für Abteilungen, die UTAX FM entwickeln und betreiben) - ISMS Cloud Security Management System in der Systementwicklung, im Betrieb und in der Wartung als Cloud-Dienstleister, der UTAX FM anbietet und Microsoft Azure als Cloud-Dienstnutzer einsetzt
Zertifizierungsregistrierungsnummer	IS 735190	IS 735190 / CLOUD 735193
Prüfende Organisation	BSI Group Japan K.K.BSI Group Japan K.K. .	

(*13) Abkürzung für „Information Security Management System“, ein System für Unternehmen zur Kontrolle von Sicherheitsrisiken für Informationsressourcen.

6. Sicherheit: technische Details

In diesem Abschnitt werden Maßnahmen gegen Sicherheitsbedrohungen und zum Schutz der Hosting-Umgebung beschrieben.

6.1. Schutz vor Sicherheitsbedrohungen

UTAX FM verlässt sich auf der Infrastrukturebene beim Schutz seiner Clouddienste und virtuellen Maschinen vor böswilligen Angriffen (z. B. DDoS- und DNS-Angriffen) auf Microsoft Azure. Der Schutz von Azure vor DDoS-Angriffen erfolgt durch eine kontinuierliche Überwachung und wird mithilfe von Penetrationstests kontinuierlich verbessert. Er dient dazu, nicht nur externe Angriffe, sondern auch Angriffe anderer Azure-Mandanten abzuwehren. Darüber hinaus bietet Azure ein internes DNS zum Schutz interner VM-Namen. VM-Namen werden innerhalb eines Clouddiensts in Form privater IP-Adressen aufgelöst, während über Clouddienste hinweg für Vertraulichkeit gesorgt wird (auch innerhalb des gleichen Abonnements). Genauere technische Informationen dazu finden Sie im Microsoft Azure Network Security White Paper

Auf der Anwendungsebene wird UTAX FM von einer dritten Partei kontinuierlich auf typische Sicherheitslücken von Webanwendungen (wie Rechteausweitung, Directory Traversal, Code Injection, Cross-Site Scripting usw.) untersucht. Wenn bei diesen Tests schwere Probleme ermittelt bzw. von anderen Quellen gemeldet werden, werden diese Probleme umgehend behoben, damit die entsprechende Anwendung sicher bleibt.

Speziell zum Schutz vor dem Knacken von Kennwörtern reagiert UTAX FM auf eine fehlgeschlagene Authentifizierungsanfrage mit einer Verzögerung.

Die Validierung von Sicherheitsrisiken (einschließlich externer) wird in Originalmodulen von KYOCERA, der Infrastruktur (Azure) und allen Betriebssystemen ausgeführt. Mit Blick auf die Infrastruktur (Azure) überprüft KYOCERA die von Microsoft monatlich herausgegebenen Informationen zu Sicherheitslücken. Für Sicherheitsrisiken in Betriebssystemen prüfen wir die Revisionsverläufe einmal alle sechs Monate.

6.2. Hosting-Umgebung

UTAX FM wird auf der Microsoft Azure-Plattform gehostet. Microsoft erfüllt eine umfassende Palette an international anerkannten Kontrollen für Informationssicherheit sowie branchenspezifische Compliance-Standards wie ISO 27001, HIPAA, FedRAMP, SOC 1 und SOC2 sowie länderspezifische Standards wie Australia CCSL (IRAP), UK G-Cloud, Singapore MTCS und Japan ISMAP. Zudem war Microsoft der erste Anbieter, der den einheitlichen internationalen Verhaltenskodex zum Datenschutz für Clouddienste (ISO/IEC 27018) umgesetzt hat. Darüber hinaus bietet Microsoft Vertragsklauseln nach EU-Standard an, die vertragliche Garantien hinsichtlich der Übertragung personenbezogener Daten außerhalb des Europäischen Wirtschaftsraums (EWR) enthalten.

Die Azure-Plattform umfasst verschiedene Sicherheitsebenen. Bei eingehendem Verkehr aus dem Internet sorgt der DDoS-Schutz von Azure für die Erkennung großer Angriffe auf Azure. Der Verkehr erreicht die speziell für Kundenumgebungen (z. B. UTAX FM) konfigurierten Endpunkte. Die Endpunkte übersetzen öffentlich verfügbare IP-Adressen und Ports in interne Adressen und Ports im Azure Virtual Network. Das Azure Virtual Network sorgt für eine komplette Isolierung von allen anderen Netzwerken sowie dafür, dass Daten ausschließlich über vom Kunden konfigurierte Pfade und Methoden übertragen werden. Diese Pfade und Methoden stellen die nächste Sicherheitsebene dar, in der Datenverkehr mithilfe von Zugriffssteuerungslisten (ACLs) kontrolliert wird.

7. Health Insurance Portable & Accountability Act (HIPAA)

HIPAA-Vorschriften beinhalten Sicherheitsstandards für den Schutz elektronischer Gesundheitsdaten. Der UTAX FM erfüllt die HIPAA-Standards, da UTAX FM keine Patientendaten erfasst, speichert oder überträgt, mit der sich eine Person oder Gruppe von Patienten identifizieren ließe. Zugriff auf UTAX FM wird durch die Benutzerrolle sowie den mit der Gruppe des Benutzers verknüpften Zugangscode streng kontrolliert. Benutzer müssen sich mit einem registrierten Benutzernamen anmelden. Außerdem gilt eine strenge Kennwortrichtlinie. Nicht autorisierte Benutzer können unter keinen Umständen auf UTAX FM zugreifen. Zugriff auf das System wird erfasst und kann für Prüfzwecke analysiert werden. Mit diesen Prüfprotokollen lässt sich untersuchen, ob UTAX FM sicher ist. Mit UTAX FM übertragene Daten werden verschlüsselt. Außerdem authentifizieren sich UTAX FM -Komponenten gegenseitig. UTAX FM sendet Gerätedaten auf sichere Weise und ausschließlich zum Zweck der Geräteverwaltung oder -wartung und übermittelt keinerlei Patientendaten. Vor dem Einsatz von Remote-Diensten von UTAX FM bittet Sie UTAX um Ihre Zustimmung.

8. Server Zertifikat

Einer der Hauptgründe, warum Webserver das von der CA ausgestellte Server-Zertifikat einsetzen, ist die Absicherung des Zertifizierungsgegenstandes und die Verhinderung von "Spoofing" der Server Domäne. Auf der Clientseite wird Spoofing erkannt, indem die Richtigkeit von Zieldomain und eingestellter Domain durch Überprüfung der Zertifikatsgültigkeiten bestätigt wird. Auf der anderen Seite verwenden das UTAX FM Gerät und der UTAX FM das Server-Zertifikat zur Verschlüsselung des Kommunikationspfades. Dies hat den Hintergrund, dass die Zertifizierung zwischen UTAX FM Gerät und UTAX FM mit Hilfe der einzigartigen Methode des XMPP/MQTT durchgeführt wird. Selbst wenn der Angreifer den Server in irgendeiner Weise überlistet, kann dieser durch einen speziellen Algorithmus der Zertifizierungsmethode keine Verbindung zum Server herstellen. Darüber hinaus führt das UTAX FM Remoteteam, um die durchgehende Sicherheit zu gewährleisten, mit Hilfe des Schwachstellendiagnosetools regelmäßig manuelle Auswertungen durch.

9. Anhang

Konsultieren Sie Abbildung 5 (UTAX FM -Komponenten und Datenströme).

9.1. Über die Intranet-Firewall

- TCP-Port 443 (HTTPS) muss geöffnet sein, um ausgehenden Datenverkehr zuzulassen. Dieser Port dient UTAX FM Device und UTAX FM Gateway zur Verbindungsherstellung mit UTAX FM.
- Wenn Ihre Firewall ausgehenden Datenverkehr anhand einer Ziel-Whitelist beschränkt, müssen Sie in UTAX FM die Hostnamen der Webserver hinzufügen.
  - ➢ Die Namen der Webserver hängen davon ab, in welchem Azure-Rechenzentrum UTAX FM gehostet wird. Diese Daten stellt Ihnen die UTAX-Hauptniederlassung in Ihrer Region bereit.

  Für eine einfache Whitelist-Verwaltung der Kunden-Firewall weisen XMPP/MQTT-Server-Endpunkte eine einheitliche Form auf. So lässt sich die IP-Adresse aus dem vorhandenen XMPP/MQTT-Server extrahieren und als Endpunkt des XMPP/MQTT-Servers bereitstellen. Die XMPP/MQTT-Server werden also nicht benötigt und können aus der Whitelist entfernt werden.
  Wenn der Kunde den XMPP/MQTT-Server mit dem Hostnamen für die Whitelist definiert, muss wegen der Vereinheitlichung der XMPP/MQTT-Server-Endpunkte ein neuer Hostname hinzugefügt werden.
  - ➢ Zur Verwendung des Remote-Bedienfelds muss die IP-Adresse des Relay-Servers des Remote-Bedienfelds zur Firewall-Whitelist des Kunden hinzugefügt werden.

9.2. Über das System, das UTAX FM Gateway (NetGateway) hostet

- TCP-Port 443 (HTTPS) muss geöffnet sein, um ausgehenden Datenverkehr zuzulassen. Dieser Port dient NetGateway zur Verbindungsherstellung mit UTAX FM. Mit Port 443 wird über HTTPS eine sichere Verbindung zur Startseite des Systems hergestellt.
- TCP-Port 9797 (HTTPS) muss geöffnet sein, um eingehenden Datenverkehr zuzulassen. Das ist erforderlich, wenn Sie eine Verbindung zur Webseite von NetGateway herstellen möchten. Wenn dieser Port bereits bei der Installation von NetGateway verwendet wurde, kann der Benutzer einen anderen Port angeben.
- TCP-Port 80 (HTTP) muss geöffnet sein, um ausgehenden Datenverkehr zuzulassen. Dieser Port dient NetGateway zur Verbindungsherstellung mit der Startseite des Systems.
- TCP-Port 9090 (HTTP) und/oder TCP-Port 9091 (HTTPS) müssen geöffnet sein, um ausgehenden Datenverkehr zuzulassen. Dieser Port dient NetGateway zur Datenanforderung von dem System.

- TCP-Port 9100 sollte geöffnet werden, um ausgehenden Datenverkehr zu ermöglichen, wenn Sie die Funktion zum Senden von Dateien über Raw Port Printing (RAW) verwenden möchten.
- Die TCP-Ports 800 - 899 sollten für den eingehenden Datenverkehr geöffnet werden. Nur einer dieser Ports wird beim Firmware-Upgrade des Geräts verwendet.
- Der UDP-Port 161 muss geöffnet werden, um ausgehenden Datenverkehr zu den Geräten zu ermöglichen. Dieser Port wird verwendet, um Gerätestatus und -eigenschaften über SNMP zu erfassen.
- Bei der Installation von NetGateway wird in der Windows-Firewall automatisch der TCP-Port 8081 (HTTPS) geöffnet, um eingehenden Datenverkehr von Geräten zuzulassen. Wenn dieser Port bereits bei der Installation von NetGateway verwendet wurde, kann der Benutzer einen anderen Port angeben. Dies ist notwendig, wenn Sie die Funktion von NetGateway nutzen möchten, um den ausgehenden Netzwerkverkehr von UTAX FM Device als einen einzigen Kommunikationspunkt zu konsolidieren. Die so erstellte eingehende Regel wird gelöscht, wenn NetGateway deinstalliert wird.
- TCP-Port 9696 (HTTPS) wird für die Kommunikation zwischen Diensten innerhalb des NetGateways verwendet, muss aber nicht geöffnet werden. Wenn dieser Port bereits bei der Installation des NetGateways verwendet wurde, kann der Benutzer einen anderen Port angeben.

9.3. Über das System, das den lokalen Agenten hostet

- Der TCP-Port 9000 muss geöffnet sein, um eingehenden Datenverkehr für die Kommunikation zwischen UTAX FM Gateway und Local Agent zuzulassen. Dieser Port wird verwendet, um Geräteinformationen von über USB angeschlossenen Geräten zu erfassen.
- TCP-Port 445 muss für eingehenden Datenverkehr geöffnet sein, wenn Sie die Funktion von UTAX FM Gateway für Windows zur Installation oder Aktualisierung des lokalen Agenten verwenden möchten. Der Port dient der Übertragung von Dateien über SMB, die für die Installation oder Aktualisierung des lokalen Agenten benötigt werden.
- Windows-Verwaltungsinstrumentation (WMI) muss aktiviert sein, wenn Sie die Funktion von UTAX FM Gateway für Windows zur Installation oder Aktualisierung des lokalen Agenten nutzen möchten.
    - ➢ Wenn eine Aktivierung von WMI nicht mit der Sicherheitsrichtlinie Ihres Standorts übereinstimmt, sollten Sie die Funktion deaktiviert lassen. In dem Fall müssen Sie den lokalen Agenten manuell installieren (und nicht mit UTAX FM Gateway für Windows).