IF IT WORX, IT'S UTAX

UTAX CLOUD PRINT AND SCAN SECURITY WHITEPAPER

UTAX // SECURITY-WHITEPAPER / UTAX CLOUD PRINT AND SCAN

utax.de

Über UTAX Cloud Print and Scan

UTAX Cloud Print and Scan (UCPS) ist eine cloudbasierte Druck- und Scanlösung für Büros, mit der Administratoren auf einfache Weise Benutzer verwalten, UTAX Multifunktionsdrucker (MFPs) registrieren und Druckaktivitäten für ihre eigenen Organisationen verfolgen können.

Dieses Whitepaper informiert Händler und Anwender über Sicherheitsmaßnahmen in UCPS. Für UTAX hat der Schutz der von UCPS verarbeiteten Datenbestände höchste Priorität. Die Datenbestände sind durch die Sicherheitskonfiguration und und die Sicherheitsfunktionen von UCPS streng geschützt.

Viel Freude bei der Lektüre

Ihr UTAX-Team

WICHTIGER HINWEIS

In Umgebungen, in denen sich mehrere Benutzer einen PC teilen, konnte es vorkommen, dass andere Benutzer Ihren Druckauftrag sehen, drucken oder löschen konnten, wenn Ihr Desktop-Client eine alte Version (v1.3.1 oder niedriger) hatte. Es wird dringend empfohlen, auf Version 1.3.2 oder höher zu aktualisieren, wodurch die oben genannten Probleme behoben werden. Der UCPS-Desktop-Client kann nicht als gemeinsamer Druckertreiber verwendet werden.

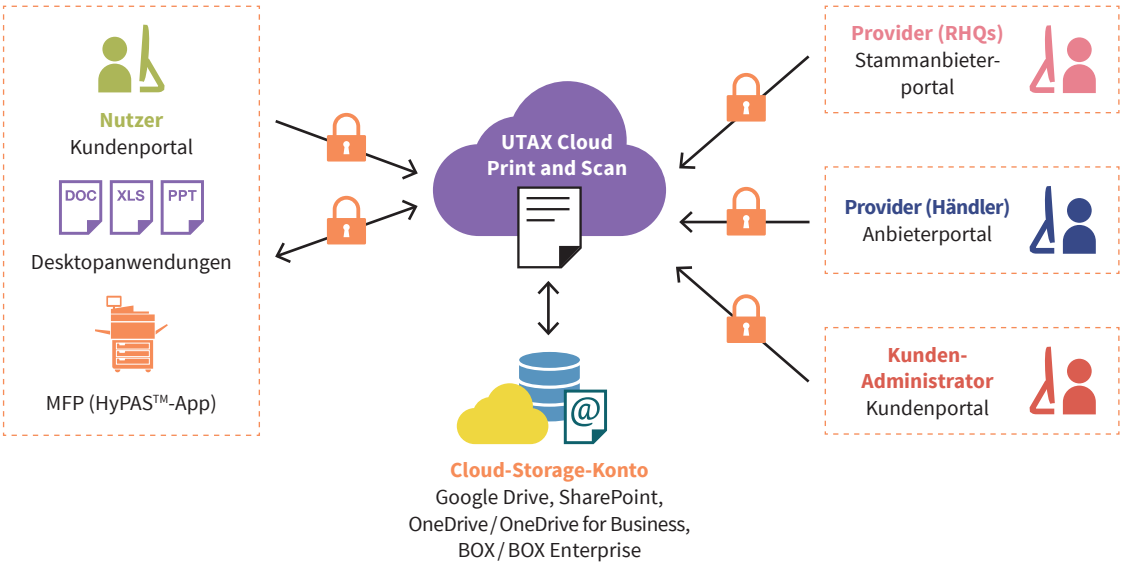
INHALT

INHALT

1. Die Komponenten von UTAX Cloud Print and Scan

UTAX Cloud Print and Scan (UCPS) ist eine cloud-basierte Druck- und Scanlösung für Unternehmen mit der Administratoren auf einfache Weise Benutzer verwalten, UTAX-Multifunktionsdrucker (MFPs) registrieren und Druckaktivitäten für ihr eigenes Unternehmen verfolgen können.

Dieses Whitepaper informiert Händler und Anwender über die Sicherheitsmaßnahmen in UCPS. Die Priorität von UTAX liegt auf dem sicheren Schutz der Informationen, die von UCPS verarbeitet werden. Diese Informationen werden durch die Konfiguration und die Sicherheitsfunktionen von UCPS strengstens geschützt.



(Abb. 1-1) UCPS-Komponenten

Stammanbieterportal: Der Stammanbieter (RHQ) kann mithilfe eines Webbrowsers auf das Stammanbieterportal zugreifen. Mit diesem Portal können die RHQs die URL-Links der Endbenutzer-Lizenzvereinbarung (EULA), der Datenschutzerklärung und des UCPS-Desktopanwendungspakets für ihre Region verwalten. Dieses Portal verfügt auch über eine Organisationsstruktur für RHQs, die die Hierarchie aller Organisationen in ihrer Region anzeigt.

Anbieterportal: Der Anbieter (RHQ, SC, Händler) kann mithilfe eines Webbrowsers auf das Anbieterportal zugreifen. Er kann für untergeordnete Anbieter oder für seine Kunden Organisationen hinzufügen, bearbeiten oder löschen.

Kundenportal: Der Kundenadministrator oder Kundenbenutzer kann mithilfe eines Webbrowsers auf das Kundenportal zugreifen. Der Kundenadministrator kann Benutzerkonten für seine eigene Organisation hinzufügen und Einstellungen in Bezug auf Drucklimits und Druckrichtlinien konfigurieren. Kundenbenutzer können ihren Druckstatus kontrollieren und gescannte Dokumente herunterladen.

Desktopanwendung: Die Desktopanwendung stellt eine Verbindung zum UCPS-Server her. Kunden können ihre Druckaufträge hochladen. Abhängig von der Konfiguration der Warteschlange (in der Cloud oder lokal) werden die Druckaufträge entweder auf dem Desktop oder auf dem UCPS-Server gespeichert.

Für die Non-HyPAS™-Modelle bietet der Desktop Client Direktdruck, ein monatliches Druckkontingent und die Nutzungsberichte.

Chrome-Erweiterung: Die Chrome-Erweiterung wird speziell für Chromebook-Benutzer bereitgestellt, damit sie ihre Druckaufträge von jeder Anwendung, die die Druckfunktion unterstützen, hochladen können. Die Chrome-Erweiterung wird im Chrome Web Store angeboten und kann von dort heruntergela-den werden.

HyPAS™-Anwendung (MFP-Client): Die HyPAS™-Anwendung stellt eine Verbindung zum UCPS-Server her. Kunden können ihre hochgeladenen Druckaufträge über die UCPS-Desktopanwendung freigeben. Mit dieser Anwendung können Kunden ihre Dokumente auch scannen.

Cloud-Speicher: Als Cloud-Speicher für Drittanbieter unterstützt UCPS auch Integrationen in Google Drive, BOX, OneDrive and SharePoint Online. Durch die Verknüpfung Ihres Cloud-Speicher-Kontos mit Ihrem UCPS-Konto können Sie aus Ihrem Cloud-Speicher drucken und gescannte Daten an diesen senden.

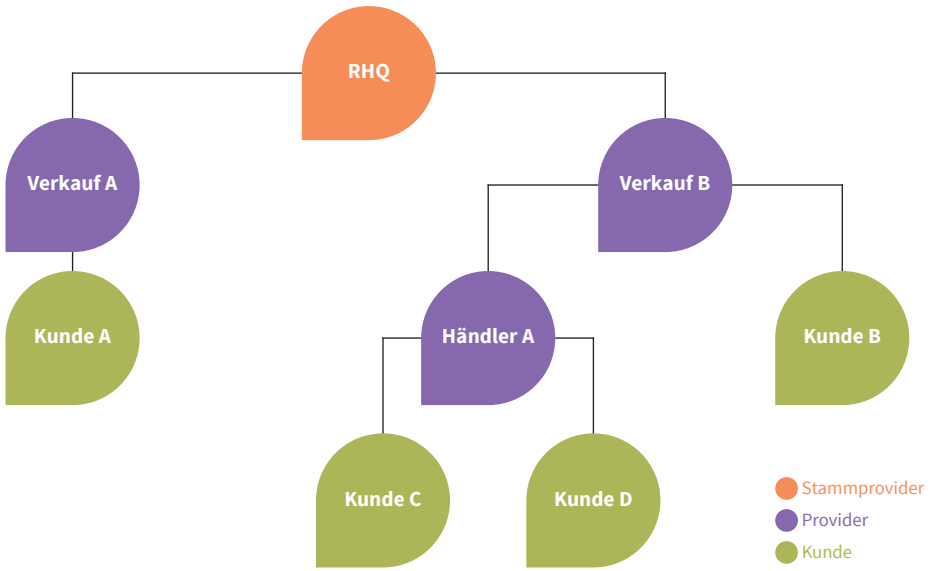
UCPS wurde von Kyocera Document Solutions (KDC) und Kyocera Document Solutions Development America (KDDA) entwickelt, die nach ISO 27001 zertifiziert sind.

2. Mehrinstanzenfähigkeit

UCPS nutzt die Mehrinstanzenfähigkeit, um mehrere Vertriebsgesellschaften, Händler und Kundenorganisationen unterzubringen. Jede Vertriebsgesellschaft, jeder Händler und jeder Kunde wird als eine Organisation behandelt. Die Zugriffssteuerung erfolgt über eine hierarchische Baumstruktur (Abb. 2-1).

Organisationen werden in zwei Typen klassifiziert: Anbieterorganisationen und Kundenorganisationen. Eine Anbieterorganisation ist auf die Verwaltung einer oder mehrerer Kundenorganisationen ausgerichtet. Anbieterorganisationen verfügen über Prüf- und Berichtsfunktionen, während Kundenorganisationen Funktionen bereitstellen, die direkt mit Bürofunktionen wie Drucken und Scannen zusammenhängen.

Die hierarchische Struktur ist der bei UTAX üblichen Vertriebshierarchie nachempfunden. Ein RHQ (regionaler Hauptsitz) ist die übergeordnete Organisation (Stammanbieter-Organisation) mit Vertriebsgesellschaften, die dem RHQ als Anbieterorganisationen untergeordnet sind. Kunden der Vertriebsgesellschaften wären demnach die Kundenorganisationen und Blattknoten in der hierarchischen Baumstruktur.



(Abb. 2-1) Hierarchische Struktur von UCPS-Organisationen

Außer der übergeordneten Organisation ist es keiner Organisation möglich, die Daten einer anderen Organisation einzusehen. Die Daten in den Kundenorganisationen bestehen üblicherweise aus Informationen über den Benutzer, Auftragsdaten des Benutzers (z. B. Druck- und Scanaufträge, Informationen über Aufträge), den mit der Kundenorganisation verknüpften Geräten sowie Protokollen (Aufträge / gedruckte Seiten, gescannte Seiten). Die Daten sind bereichsbezogen und der Zugriff auf Daten ist begrenzt (Tabelle 2-1).

Benutzertyp	Benutzer der Kundenorganisation	Geräte der Kundenorganisation	Report (Aufträge / gedruckte/ gescannte Seiten)	Auftragsdaten des Kunden (Dokumente drucken und scannen)
Anbieter-Administrator	Zugriff nicht möglich	Zugriff möglich	Zugriff nicht möglich	Zugriff nicht möglich
Anbieter-Support	Zugriff nicht möglich	Zugriff möglich	Zugriff nicht möglich	Zugriff nicht möglich
Kunden-Administrator	Zugriff möglich	Zugriff möglich	Zugriff möglich Benutzerbericht, Benutzergruppen-bericht Gerätebericht	Zugriff möglich Kann nur eigene Auftragsdaten sehen
Printer Manager	Zugriff möglich (Nur Druckkontigente)	Zugriff nicht möglich	Zugriff nicht möglich	Zugriff möglich (Kann nur eigene Auftragsdaten sehen)
Kundenbenutzer	Zugriff nicht möglich	Zugriff nicht möglich	Zugriff möglich Kann nur eigene Protokolldaten sehen	Zugriff möglich Kann nur eigene Auftragsdaten sehen
Gastbenutzer	Zugriff nicht möglich	Zugriff nicht möglich	Zugriff nicht möglich	Zugriff möglich (Kann nur eigene Auftragsdaten sehen)
Benutzer, die nicht im UCPS System sind	Zugriff nicht möglich	Zugriff nicht möglich	Zugriff nicht möglich	Zugriff nicht möglich

(Tabelle 2-1) Zugriff auf Organisations- und Benutzerdaten je nach Benutzertyp

Wenn dem Administrator des Kunden Zugriff auf die externe API gewährt wird, kann über die API auf die Liste der Benutzer in der Kundenorganisation und das Auftragsprotokoll der Kundenorganisation (einschließlich Geräteinformationen, Ausführungs-ID, Ausführungszeit, Auftragstyp und Seitenzahl) zugegriffen werden.

Wenn zum Beispiel Benutzer 1 und Benutzer 2 beide Benutzer in der Organisation Kunde A sind, kann Benutzer 1 nur seine eigenen Druck- und Scanaufträge sehen und nicht die des Benutzers 2 (siehe Abb. 2-2).

(Abb. 2-2) Zugriff auf Benutzerdaten für eine Kundenorganisation

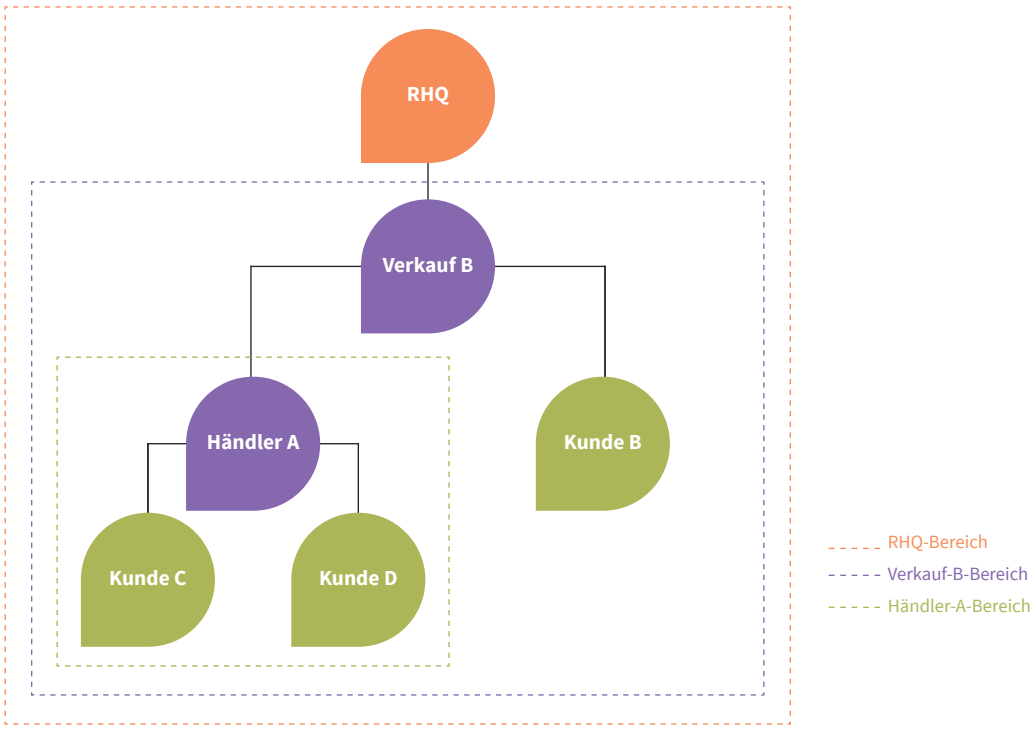
Darüber hinaus können Benutzer 1 und Benutzer 2 vom Kundenportal aus keine weiteren Benutzer in der Organisation Kunde A sehen, nur der Admin (der ein Admin in Kunde A ist) kann Benutzer 1 und Benutzer 2 (und sich selbst, den Admin) als Benutzer in der Organisation Kunde A sehen.

Schließlich kann der Admin keine Druck- oder Scanaufträge anderer Benutzer sehen, aber der Admin kann sehen, welche Geräte für die Organisation Kunde A registriert wurden und mit ihr verknüpft sind.

Geltungsbereiche gibt es auch zwischen Root-Provider-, Provider- und Kundenorganisationen. Auf Organisationsebene werden lizenzbezogene Informationen (z. B. wie viele Geräte eine Kundenorganisation registrieren darf) verfolgt und ausgetauscht, um die Abrechnung zu erleichtern (Abb. 2-3).

Die Sichtbarkeit dieser Daten gilt von unten nach oben für die übergeordneten Organisationen. Das heißt, dass ein RHQ die aggregierten Daten der Kunden B, C und D sehen, aber nicht zwischen diesen Organisationen unterscheiden kann. Dies liegt daran, dass die Namen der Organisationen in den Berichten zu den Providerverträgen anonymisiert sind. In ähnlicher Weise kann der Vertrieb B die aggregierten Daten von Kunde C und Kunde D sehen, ist aber nicht in der Lage, zwischen ihnen zu unterscheiden.

Es ist erwähnenswert, dass übergeordnete Organisationen die von ihnen erstellten Organisationen identifizieren können, da sie diese untergeordneten Organisationen selbst erstellt und den Organisationsnamen beim Erstellen der Organisation festgelegt haben. Das bedeutet, dass Vertrieb B die Daten von Kunde B separat sehen und diese Daten als getrennt von den aggregierten Daten von Kunde C und Kunde D identifizieren kann. Ebenso kann Händler A die Daten von Kunde C und Kunde D sehen und unterscheiden.



(Abb. 2-3) Zugriff auf lizenzbezogene Informationen für jede Organisation

3. Kommunikationssicherheit zwischen den Modulen

Transport Layer Security (TSL) ist eine Standard-Sicherheitstechnologie zum Aufbau einer verschlüsselten Verbindung zwischen einem Server und einem Client. In CPS wird TLS verwendet, um sensible Informationen zu sichern und zu schützen, die zwischen CPS und einem Browser, Gerät, Desktop-Client, Mobilgerät oder einer Datenbank ausgetauscht.

Zu diesen Informationen gehören:

- CPS-Benutzeranmeldedaten und Passwörter
- Benutzerdaten
- Auftragsinformationen (Druckauftrag, Scanauftrag usw.)
- Dokument
- Messdaten zur Dokumentenzahl (Anzahl der gedruckten Seiten, Anzahl der gescannten Seiten, Kontingent usw.)

Dadurch wird sichergestellt, dass Dritte im Netzwerk die Nutzdaten während der Übertragung nicht entschlüsseln oder manipulieren.

3.1. Sicherheit zwischen der HyPAS-Anwendung und dem CPS-Server

Die folgende Tabelle listet die TLS-Versionen auf, die verfügbar sind, wenn eine HyPAS-Anwendung auf einem von CPS unterstützten Modell installiert ist. Modelle, für die mehrere Versionen aufgeführt sind, verwenden je nach Firmware-Version des Geräts unterschiedliche TLS-Versionen. Wenn die neueste Firmware-Version installiert ist, wird die sicherste Version verwendet.

3.1.1. DIN-A3-Multifunktionssysteme

Produktreihe	System	Unterstützte TLS-Version
Athena	9515ci 8515ci 7515ci 10565i 9565i 8565i 7565i	1.3
Iris	6006ci 5006ci 4006ci 3206ci 2506ci	1.2/1.0
Iris2	6007ci 5007ci 4007ci 3207ci 2507ci 6057i 5057i	1.3/1.2
Iris2020	7008ci 6008ci 5008ci 4008ci 3508ci 2508ci 7058i 6058i 5058i	1.3
IRIS2024	7009ci 6009ci 5009ci 4009ci 3509ci 2509ci 7059i 6059i 5059i	1.3
HANABI2	P-C3080i MFP P-C2480i MFP	1.2
MATSURI2	P-3240i MFP P-2540i MFP	1.2
MATSURI3	P-3241i MFP	1.3
Mercury4	8507ci 7507ci	1.2
Tomcat3	4062i 3262i	1.2
Tomcat4	4063i 3263i	1.3
Zeus4	9057i 8057i 7057i	1.2

3.1.2. DIN-A4-Multifunktionssysteme

Projektname	TA/UTAX Marke	Unterstützte TLS-Version
Libra	P-4026iw MFP	1.2/1.0
Libra2	P-4027iw MFP	1.3
Mebius E-Model HyPAS MFP	P-C3062i MFP P-C3066i MFP P-C3562i MFP P-C3566i MFP	1.2
TASKalfa Mebius-E Plus	357ci	1.2
Perseus2	352ci 402ci 502ci	1.3/1.2
	302ci	1.2
Polaris E-Model	P-6036i MFP P-5536i MFP P-4531i MFP P-4536i MFP	1.2
Polaris E-Model Plus	P-6038i MFP P-6038if MFP	1.2
Polaris Next HyPAS	P-4532i MFP P-6039i MFP P-5539i MFP P-4539i MFP	1.3
Virgo	P-C3563i MFP P-C3567i MFP P-C4063i MFP P-C4067i MFP 358ci 458ci	1.3

3.1.3. DIN-A4-Drucksysteme

Projektname	TA/UTAX Marke	Unterstützte TLS-Version
Virgo	P458ci	1.3

4. Benutzerkennung und -authentifizierung

Beim Zugriff auf UCPS muss sich der Benutzer mit einem aktivierten Konto anmelden. Unautorisierte Benutzer können nicht auf UCPS zugreifen. Für die Anmeldung werden die folgenden Sicherheitsfunktionen unterstützt.

4.1. Kontosperrungsrichtlinie

Die Kontosperrungsrichtlinie schützt UCPS vor Passwortentschlüsselungsangriffen. Nach einer vorher festgelegten Anzahl von fehlgeschlagenen Anmeldeversuchen wird das Benutzerkonto für einen definierten Zeitraum gesperrt.

Wie in der nachstehenden Tabelle gezeigt, wird das Benutzerkonto nach drei fehlgeschlagenen Anmeldeversuchen gesperrt. Nach 30 Minuten wird die Sperre aufgehoben. Diese Einstellung gilt auch für den Fall, dass die Authentifizierung mit einem Einmalpasswort (OTP) während der Multi-Faktor-Authentifizierung (MFA) fehlschlägt.

Anzahl fehlgeschlagener Anmeldeversuche	Drei Versuche
Aufhebung der Sperre	30 Minuten

4.2. Passwortrichtlinie

Der Benutzer muss ein sicheres Passwort verwenden, das der UCPS-Passwortrichtlinie entspricht. Es werden nur Passwörter zugelassen, die dieser Richtlinie entsprechen. Diese Richtlinie verhindert, dass Benutzer einfache Passwörter einrichten, und schützt vor unbefugtem Zugriff durch Dritte.

Alle Passwörter in UCPS werden mit einem Hash gespeichert und über ein Netzwerk übertragene Passwörter können bei der Übertragung verschlüsselt werden. Der Browser blendet auch alle Passwörter aus.

Die nachstehende Tabelle zeigt, wie Passwortlänge und Komplexität definiert sind:

Passwortlänge	Zwischen 8 und 64 Zeichen
Passwortkomplexität	Enthält mindestens ein Zeichen aus jeder Kategorie: • Zahlen zwischen 0 und 9 • Großbuchstaben* • Kleinbuchstaben* • Sonderzeichen (!"#$%&'()*+,-./:;<=>?@[]^_`{|}~)

*Nur Zeichen des englischen Alphabets (keine Unicode-Zeichen wie Umlaute, japanische Kanji/Hiragana/Katakana usw.)

4.3. Richtlinie für Benutzernamen

Die Richtlinie für Benutzernamen dient zur Überprüfung, ob der Wert ein gültiger Benutzername ist. Dadurch werden Sonderzeichen verhindert, die für SQL-Injection-Schwachstellen verwendet werden könnten.

Länge des Benutzernamens	Zwischen 4 und 64 Zeichen
Unzulässige Zeichen	Symbols \ / : , ; * ? " < > | [ ] { } $ % ` & ( ) + =

4.4. Richtlinie für Vor- und Nachname

Es gibt eine Richtlinie für die Felder „Vorname“ und „Nachname“, um bestimmte Sonderzeichen zu verhindern, die für SQL-Injection-Schwachstellen verwendet werden könnten. Die Validierungsfunktion überprüft, ob der Wert ein gültiger Personenname ist, um eine zusätzliche Barriere gegen Angriffe wie Skript-Injection zu schaffen.

Länge des Benutzernamens	Zwischen 1 und 255 Zeichen
Unzulässige Zeichen	Symbols \ / : , ; * ? " < > | [ ] { } $ % ` & ( ) + =

4.5. Automatischer Logout

Um zu verhindern, dass ein Benutzer sein Gerät nicht mehr benutzt, aber weiter angemeldet ist, wurde eine Funktion implementiert, die den Benutzer automatisch abmeldet, wenn eine angemeldete Sitzung eine bestimmte Zeit inaktiv ist.

Diese automatische Abmeldung gilt für alle Clients, die auf den UCPS-Server zugreifen: MFP/HyPAS™, Desktop-Client und Webbrowser.

Für den Desktop-Client wurde die Dauer der automatischen Abmeldung anpassbar gemacht, um den spezifischen Bedürfnissen der RHQs gerecht zu werden.

4.6. PIN-Authentifizierung

Um die Anmeldung bei der UCPS HyPAS™-Anwendung zu vereinfachen, unterstützt die Lösung die PIN-Authentifizierung. Im Allgemeinen ist die PIN-Authentifizierung für die Verbesserung des Bedienkomforts praktisch, aber sie beeinträchtigt die Sicherheitsstärke. Da jede Umgebung unterschiedliche Sicherheitsstandards erfordert, unterstützt UCPS PIN-Authentifizierungsfunktionen, die an verschiedene Situationen angepasst werden können..

Wählbare PIN-Code-Länge	4–12 Zeichen
Benutzerdefinierte PIN-Code-Einstellung	Unterstützt
Administrator-Einstellung beliebiger PIN-Codes für jeden Benutzer	Unterstützt
Ausblendung konfigurierter PIN-Codes (****)	• Wenn ein Administrator den PIN-Code eines Benutzers einsieht, wird dieser ausgeblendet angezeigt. • Der eigene PIN-Code des Benutzers wird ohne Verschlüsselung angezeigt.

4.7. ID-Karten-Authentifizierung

Die Authentifizierung mit ID-Karten wurde als alternative Methode zur Vereinfachung der Anmeldung bei der UCPS-HyPAS™-Anwendung hinzugefügt. Die Registrierung und Verwaltung von ID-Karten wird in der HyPAS™-Anwendung durchgeführt, nachdem sich ein Benutzer dort authentifiziert hat. Die Verwaltung der ID-Karten (z. B. das Löschen einer zuvor registrierten Karte) erfolgt über die UCPS-Webanwendung. Die Registrierung von ID-Karten kann auch in der HyPAS™-Anwendung durchgeführt werden, sobald sich der Benutzer in der HyPAS™-Anwendung authentifiziert hat.

4.8. Multi-Faktor-Authentifizierung

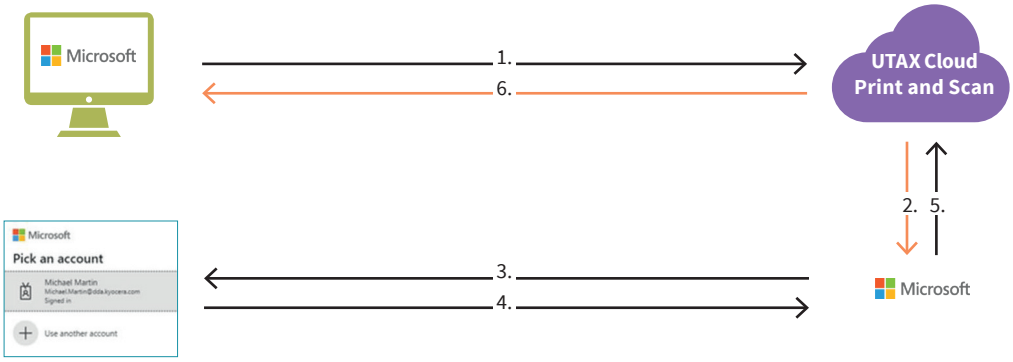
UCPS unterstützt die E-Mail-basierte Multi-Faktor-Authentifizierung (MFA). Es sendet einen einmaligen Passcode an die registrierte E-Mail-Adresse des Benutzers und verlangt die entsprechende Eingabe. Dadurch wird das Risiko eines unbefugten Zugriffs erheblich reduziert, selbst wenn das Passwort kompromittiert wurde. Dieser OAuth2-Authentifizierungsablauf ist für andere Drittanbieter (z. B. unterstützte Speicherdienste wie OneDrive, Google Drive, Box und SharePoint) identisch. Wenn die Authentifizierung für die Verknüpfung mit diesen Drittanbietern initiiert wird, wird eine separate Webseite geladen und die Authentifizierung auf den von diesen Drittanbietern kontrollierten Seiten durchgeführt. UCPS hat niemals Zugriff auf die für die Drittanbieterdienste eingegebenen Benutzeranmeldedaten.

4.9. Authentifizierungs- und Identitätsserver von Drittanbietern

UCPS unterstützt die Authentifizierung von Drittanbietern und ihren entsprechenden Identitätsservern.

4.9.1. 3rd Party Authentifizierung und OAuth2

UCPS bietet die Möglichkeit, Speicher von Drittanbietern zu verbinden und sich mit Azure AD-Anmeldeinformationen anstelle von UCPS-Anmeldeinformationen zu authentifizieren. UCPS folgt dem Industriestandard für OAuth2-Authentifizierungen.



1. Der Benutzer klickt auf "Mit Microsoft anmelden".
2. UCPS ruft Microsoft-APIs auf, um die OAuth2-Authentifizierung mit den Azure AD-Anmeldeinformationen durchzuführen.
3. Der Benutzer wird zu einer Anmeldeseite weitergeleitet, die von Microsoft gesteuert wird. Da es sich um eine Seite handelt, die von Microsoft verwaltet wird, werden alle zusätzlichen Authentifizierungsfunktionen, die Microsoft unterstützt, ebenfalls von dieser Seite unterstützt. (z. B. 2FA/MFA)
4. Der Benutzer folgt den Aufforderungen zur Authentifizierung. (z. B. Eingabe des Benutzernamens/der E-Mail-Adresse und des Passworts, Durchführung von 2FA/MFA)
5. Microsoft sendet das Ergebnis der Authentifizierung (ob erfolgreich oder nicht) an UCPS.
6. Die Kontrolle wird an UCPS zurückgegeben und UCPS ruft die entsprechende Seite auf. (z. B. wenn die Authentifizierung bei Microsoft erfolgreich)

Dieser OAuth2-Authentifizierungsablauf gilt auch für andere Drittanbieter (z. B. für unterstützte Speicheranbieter wie OneDrive, Google Drive, Box und SharePoint). Wenn die Authentifizierung initiiert wird, um eine Verbindung zu diesen Drittanbietern herzustellen, wird eine separate Webseite geladen und die Authentifizierung wird auf den Seiten durchgeführt, die von diesen Drittanbietern verwaltet werden.

UCPS hat niemals Zugriff auf die Benutzeranmeldeinformationen, die bei den Diensten der Drittanbietern eingegeben wurden.

4.9.2. Microsoft Entra ID

Microsoft Entra ID (früher bekannt als Azure Active Directory / Azure AD) wird von der Anwendung unterstützt. Sobald der Administrator eine Organisation für die Verwendung einer Microsoft Entra ID konfiguriert hat, können sich Benutzer, die in dieser Entra ID Instanz existieren, mit dessen Zugangsdaten in UCPS anmelden.

Wenn sich ein Benutzer erfolgreich in der Webanwendung oder dem Desktop-Client mit seinen Microsoft Entra ID anmeldet, wird ein UCPS-Benutzer erstellt, der Informationen aus seiner Microsoft Entra ID-Identität (E-Mail, Gruppeninformationen) enthält. Dieser UCPS-Benutzer ist eine separate Identität in der Anwendung.

In diesem Zusammenhang sind einige wichtige Hinweise zu beachten:

- UCPS speichert keine Microsoft Entra ID Anmeldedaten; UCPS folgt dem OAuth2-Authentifizierungsworkflow und leitet zur Überprüfung der Anmeldedaten grundsätzlich zu Microsoft Entra ID weiter
- UCPS verwaltet den Microsoft Entra ID-Benutzer nicht
  - Wenn der entsprechende UCPS-Benutzer gelöscht wird, wird der Microsoft Entra ID-Benutzer nicht gelöscht und existiert weiterhin in Microsoft Entra ID
  - Wenn der Microsoft Entra ID-Benutzer gelöscht wird, bleibt der UCPS-Benutzer auf UCPS bestehen, kann sich aber nicht mehr mit Microsoft Entra ID-Anmeldeinformationen authentifizieren, da der Entra ID-Benutzer nicht mehr vorhanden ist.

Wenn Microsoft Entra ID für die Organisation eingerichtet ist, kann sich ein Benutzer nicht mehr mit seinen Microsoft Entra ID-Zugangsdaten bei der HyPAS App anmelden. ID-Karte und PIN-Anmeldung sind für den Benutzer weiterhin verfügbar, um sich in der UCPS HyPAS App zu authentifizieren.

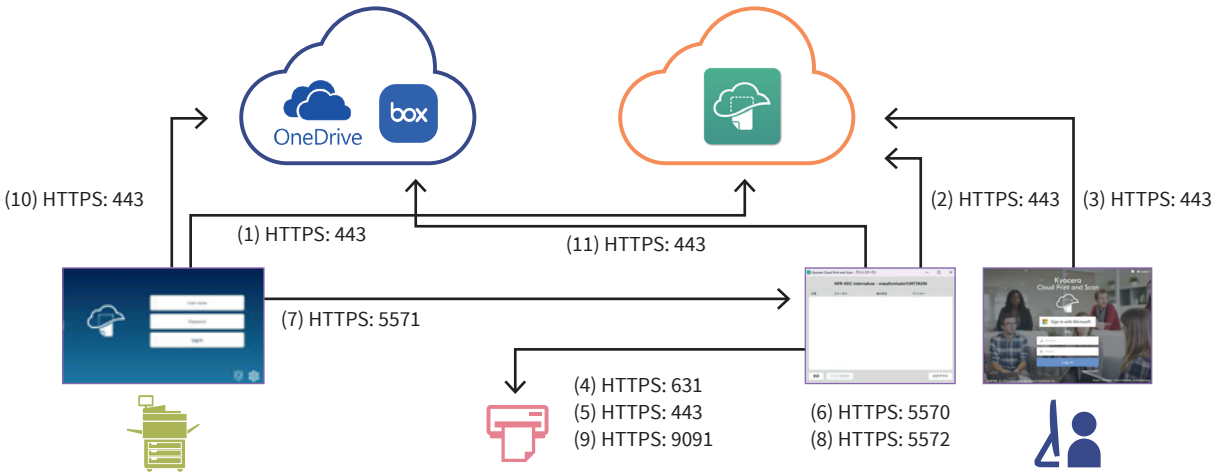
4.9.3. Google Workspace

Google Workspace wird von der Webanwendung unterstützt. Die im Abschnitt Microsoft Entra ID beschriebenen Fälle werden auch für Google Workspace unterstützt.

Zusätzlich zu diesen Fällen unterstützt Google Workspace auch Folgendes:
Import von Nutzern aus dem Google Workspace; dieser Vorgang wird manuell vom Webportal initiiert.

5. Anschlüsse und Kommunikations-anforderungen

Die von UCPS verwendeten Ports sind wie folgt. Die Nummern in der Abbildung (z. B. (1), (2), …) entsprechen den Verbindungsinformationen in der folgenden Tabelle.



Erforderliche Ports:

Quelle	Ziel	Protokoll	Port	Service
MFP / HyPAS™	UCPS-Server	TCP	443	HTTPS: Anmelden sowie Auftragsprotokoll und Scandaten an UCPS senden*
UCPS-Desktop-Client	UCPS-Server	TCP	443	HTTPS: Anmelden und Auftragsliste an UCPS senden
Webbrowser	UCPS-Server	TCP	443	HTTPS: Zugriff auf die Benutzeroberfläche
UCPS-Desktop-Client	Drucker/MFP	TCP	631	HTTPS: IPP-Druck (für Nicht-HyPAS™-Modelle)
UCPS-Desktop-Client	Drucker/MFP	TCP	443	HTTPS: Sicheres IPP-Drucken (für Nicht-HyPAS™-Modelle)
UCPS Desktop Client	UCPS-Desktop-Client	TCP	5570	HTTP: nur für interne / lokale Kommunikation verwendet
MFP / HyPAS™	UCPS-Desktop-Client	TCP	5571	HTTPS: Auftragsliste und Auftragsdaten abrufen
UCPS-Desktop-Client	UCPS-Desktop-Client	TCP	5572	HTTP: Nur für die interne/lokale Kommunikation (für Nicht-HyPAS™-Modelle)
UCPS-Desktop-Client	Drucker/MFP	TCP	9091	HTTPS: Abrufen von Druckerinformationen (für Nicht-HyPAS™-Modelle)
UCPS HyPAS™-Anwendung	Cloud-Speicher von Drittanbietern	TCP	443	HTTPS: Druckdaten abrufen, Scandaten senden und Faxweiterleitung
UCPS-Desktop Client	Cloud-Speicher von Drittanbietern	TCP	443	HTTPS: Druckdaten senden (unterstützt nur das Senden an OneDrive)

*Druckaufträge werden vom MFP / HyPAS™-Anwendung initiiert, so dass für Port 443 keine speziellen Firewall-Regeln für eingehende Aufträge erforderlich sind. Bitte wenden Sie sich an Ihre zuständige IT-Abteilung, um die Ports für die UCPS-Kommunikation zu öffnen.

6. Datenschutz

6.1. Schutz der gespeicherten Daten

Die Informationsbestände von UCPS müssen geschützt werden und dürfen nicht durchgelassen werden oder verloren gehen. UCPS implementiert Sicherheitsschutzmaßnahmen für gespeicherte Informationsbestände und eine Unterstützung zur Datenwiederherstellung mithilfe der unten beschriebenen Funktionen.

6.1.1. Zugriffssteuerung

Die Umgebungsressourcen von UCPS werden nur auf Personen beschränkt, die Wartungs- und Überwachungsaufgaben in dieser Umgebung ausüben. Nur Personen mit ordnungsgemäßer Zugriffssteuerung haben Zugang zu den Ressourcen der AWS-Umgebung von UCPS und zu den Anwendungsdaten. Die Benutzer müssen über eine entsprechende RBAC-Autorisierung (rollenbasierte Zugriffssteuerung) verfügen.

6.1.2. Authentifizierung

Die Datenbank von UCPS erfordert eine Benutzerauthentifizierung, um Zugriff auf die Daten aus der Datenbank zu erhalten. Die Authentifizierungsdaten werden während der Einrichtung konfiguriert.

6.1.3. Verschlüsselung

UCPS verwendet den höchsten Verschlüsselungsstandard, der vom Play Framework (2.6.6) und der verwendeten Silhouette-Bibliothek (5.0.0) unterstützt wird: SHA-256 Bit. Innerhalb des UCPS-Servers wird diese Verschlüsselung speziell für die Authentifizierung verwendet (Generierung des Hash, wenn ein Benutzer einen Anmeldeversuch unternimmt).

Wie in Kapitel 7 beschrieben, wird UCPS auf der Amazon AWS-Plattform gehostet und für die Datenbank wird MongoDB verwendet.

AWS bietet Verschlüsselung auf mehreren Ebenen, um Ihre Daten zu sichern, einschließlich Verschlüsselung im Ruhezustand, Verschlüsselung während der Ausführung und Schlüsselverwaltung (mit AWS Key Management), wodurch AWS verschiedene Verschlüsselungsmodelle unterstützt.

Festplatten, die von AWS-VMs verwendet werden, sind durch Festplattenverschlüsselung geschützt. Dies schützt sowohl die Betriebssystemfestplatte als auch die Datenfestplatten mit vollständiger Volumenverschlüsselung. Die Festplatten werden mit dem 256-Bit Advanced Encryption Standard (AES) verschlüsselt und die Verschlüsselung ist für den Benutzer transparent.

Daten im Ruhezustand in der UCPS-Datenbank werden über die von MongoDB Atlas in der Enterprise-Version bereitgestellte Verschlüsselung verschlüsselt. MongoDB verwendet standardmäßig den 256-Bit Advanced Encryption Standard im Modus Cipher Block Chaining (AES256-CBC), wobei andere Verschlüsselungsoptionen verfügbar sind. Der von MongoDB verwendete Verschlüsselungsschlüssel kann vom Schlüsselverwaltungsdienst des Cloud-Anbieters übernommen werden, wobei MongoDB den Schlüssel automatisch alle 90 Tage rotiert. Der Verschlüsselungsprozess ist für den Benutzer transparent.

Daten, die über AWS-33-Speicher gespeichert werden, werden standardmäßig verschlüsselt. Die S3-Verschlüsselung kann AWS-verwaltete Schlüssel oder Kunden-Masterschlüssel verwenden, die im Schlüsselverwaltungsservice gespeichert sind.

Daten werden bei der Übertragung ebenfalls verschlüsselt.

Datenbestände sind durch Sicherheitskonfiguration und Sicherheitsfunktionen von UCPS streng geschützt.

6.1.4. In UCPS verwendete Informationen

UCPS-Komponente	Informationsbestände (verwendet zum Zweck der Identifikation und Kommunikation innerhalb von UCPS)
UCPS-Server	• Organisationsinformationen (URLs der einzelnen Organisationsportale, E-Mail-Adressen der Admins der einzelnen Organisationen, Organisationstyp, Lizenzinformationen, Datenaufbewahrungsfristen) • Benutzerinformationen (Vor- und Nachname, Benutzername, E-Mail-Adresse, Authentifizierungs-Hashes, Authentifizierungs-Token von verknüpften Cloud-Speicher-Konten) jedes UCPS-Benutzers • Geräteinformationen (Seriennummer, Netzwerkinformationen wie Hostname und IP-Adresse) jedes UCPS-Geräts, die für die Geräteregistrierung und Berichterstellung verwendet werden • Geräteprotokollierungsinformationen (Anzahl der Scans, andere Gerätevorgänge) zum Zweck der Erstellung von Nutzungsberichten (zur Unterstützung der Abrechnung) und zur Wartung/Fehlersuche • Informationen zu Druck- und Scanaufträgen • Druckaufträge (bei Cloud-Warteschlangen) und Scanaufträge • Nutzungsberichte (für Abrechnungszwecke) nach Benutzer, Benutzergruppe, Gerät, Anbieter und Kundenorganisationen
UCPS-HyPAS™	• Vom UCPS-Server generierte Authentifizierungs-Token zur Authentifizierung des Geräts oder des angemeldeten UCPS-Benutzers, um Informationen an den UCPS-Server zu senden und von diesem zu empfangen • Dokumente (PDF/JPG), die vom Gerät gedruckt oder gescannt werden sollen • Metriken (gedruckte und gescannte Aufträge und Seiten)
UCPS-Desktopanwendung	• Proxy-Einstellungen des Netzwerks, mit dem der Desktop verbunden ist; wird verwendet, um die Kommunikation zwischen der UCPS-Desktopanwendung und dem UCPS-Server zu erleichtern • Vom UCPS-Server generierte Authentifizierungs-Token zur Authentifizierung des Geräts oder des angemeldeten UCPS-Benutzers, um Informationen an den UCPS-Server zu senden und von diesem zu empfangen • Dokumente (PDF), die aus Desktopanwendungen über die Druckwarteschlange der UCPS-Desktopanwendung gedruckt werden. Bei einer lokalen Warteschlange werden die PDF-Druckaufträge lokal auf dem Desktop gespeichert, während sie bei Verwendung der Cloud-Warteschlange auf den UCPS-Server hochgeladen werden. • Dokumente (PDF), die lokal gespeichert sind, befinden sich in den folgenden Ordnern: - (Windows) C:\Users\<username>\AppData\Local\KCP - (Mac) /Users/Shared/Library/Cloud Print and Scan • Informationen über Druckaufträge (Name des Dokuments, Anzahl der Seiten, Speicherort, von dem UCPS-HyPAS™ den Druckauftrag herunterladen kann)
UCPS Chrome-Erweiterung	• Vom CPS-Server generierte Tokens, die das Gerät oder den angemeldeten Benutzer authentifizieren.

6.1.5. Datensicherung

Die Sicherung der UCPS-Datenbank auf AWS wird durch MongoDB Atlas erleichtert. MongoDB Atlas bietet eine konfigurierbare Cloud-Sicherung, die von MongoDB verwaltet wird. Der aktuelle Sicherungsplan ist auf zweimal täglich eingestellt und wird sieben Tage lang aufbewahrt. Die Wiederherstellung der Datenbank wird ebenfalls durch MongoDB Atlas ermöglicht.

Die Einsatzbereiche für UCPS und die Datenbank- Sicherungsregionen sind wie folgt:

Geografische Region	AWS-Region
Asien-Pazifik	ap-northeast-1(Tokio)
Asien-Pazifik (AU)	ap-southeast-2(Sydney)
Europa (EU)	eu-central-1(Frankfurt)
Vereinigte Staaten (US)	us-east-1(North Virginia)

6.2. Schutz der Kommunikationsdaten

UCPS schützt Kommunikationsdaten bezüglich des Benutzerzugriffs zur Verwendung von UCPS bzw. der Datenkommunikation zur Übertragung von Daten zwischen UCPS und den Geräten.

Zum Schutz der UCPS-Kommunikationsdaten gegen Masquerading, Abgreifen oder Modifizierung werden die Daten verschlüsselt und die UCPS-Komponenten müssen sich gegenseitig authentifizieren.

6.2.1. Benutzerzugriff

Wenn ein Benutzer über eine Anwendung (Webanwendung über einen Browser, Desktopanwendung oder HyPAS™-Anwendung) auf UCPS zugreift, wird ein authentifizierter Kommunikationskanal aufgebaut. UCPS-Benutzer können unabhängig von der Benutzerrolle über die Client-Oberfläche des Webbrowsers auf das UCPS-Webportal zugreifen.

Jeder Zugriff auf das UCPS-Webportal erfordert die Identifizierung und Authentifizierung des Benutzers. Erst bei erfolgreicher Identifizierung und Authentifizierung kann der Benutzer entsprechend seiner Rolle auf das UCPS-Webportal zugreifen. Das UCPS-Webportal schützt die Kommunikationsdaten mittels HTTPS.

6.2.2. HTTPS-Protokoll

HTTPS beruht auf zugrunde liegenden sicheren Protokollen (TLS), die den gesamten Datenverkehr zwischen Browser und Server verschlüsseln. TLS erfordert ein Zertifikat mit einem privaten Schlüssel, einem öffentlichen Schlüssel, Domäneninformationen und einer Kette von Signaturen von Zertifizierungsstellen.

In UCPS wird TLS verwendet, um sensible Informationen, die zwischen dem UCPS-Server und einem Browser, einem Gerät oder einer Datenbank ausgetauscht werden, zu sichern und zu schützen.

Diese Informationen umfassen:

- UCPS-Benutzeranmeldeinformationen und Passwörter
- Informationen zur Geräteauthentifizierung
- Benutzerdaten
- Auftragsinformationen (Druck- und Scanaufträge, gedruckte Seiten, verwendete Farbeinstellungen usw.)

Die UCPS-Umgebung kann vom Umgebungsadministrator auch so konfiguriert werden, dass ein selbst signiertes Zertifikat verwendet wird. Es müssen Schritte befolgt werden, um entweder ein selbst signiertes Zertifikat innerhalb der Umgebung zu erstellen oder ein selbst signiertes Zertifikat in die Umgebung hochzuladen.

Zertifikate über Cert Manager haben eine Lebensdauer von 90 Tagen und werden automatisch erneuert, wenn sie abgelaufen sind. Selbst signiertes Zertifikate müssen vom Umgebungsadministrator verwaltet werden.

6.3. Sichere Kommunikation zwischen dem UCPS-Server und Datenbanken

UCPS auf AWS stellt die Netzwerkverbindung zur Datenbank über TLS-verschlüsselten Netzwerkverkehr her. Der Datenbankzugriff ist auf Verbindungen beschränkt, die von der IP-Zugriffsliste von Atlas mit den richtigen Anmeldeinformationen für die Datenbank stammen.

6.4. Direktes Drucken und Scannen aus Box- und OneDrive-Speichern

UCPS bietet Funktionen, die den Datenschutz und die Sicherheit von Benutzerdaten verbessern. Derzeit werden nur die Speicherdienste Box und OneDrive unterstützt. Wenn ein Benutzer diese Speicherdienste jedoch mit UCPS verknüpft, werden alle Druck- und Scanvorgänge (einschließlich Faxweiterleitung) durch direkte Interaktion mit den jeweiligen Speicherdiensten abgewickelt. Zu keinem Zeitpunkt wird dabei der temporäre Speicher von UCPS verwendet.

6.5. Prüfung auf Sicherheitslücken

Um das UCPS-System bezüglich Sicherheitsmaßnahmen auf dem neuesten Stand zu halten, wird der folgende Zeitplan für die Bewertung der Sicherheitslücken eingehalten:

- Durchführung einer internen Bewertung der Sicherheitslücken zum Zeitpunkt der Softwarefreigabe
- Regelmäßige Prüfung der Schwachstellen in Abhängigkeit von den Vorschriften zur Serververwaltung.
- Falls sich die Konfiguration des öffentlichen Servers wesentlich ändert, z. B. bei einem Upgrade, ist eine Schwachstellenbewertung vorzunehmen.

7. Geräteauthentifizierung

Zum Schutz vertraulicher Informationen, die zwischen UCPS und UTAX Geräten übertragen werden, wird die Sicherheit durch HTTP über TLS erzwungen. Standardmäßig ist das TLS-Protokoll für die Gerätekommunikation aktiviert.

Dabei können die folgenden Optionen eingestellt werden:

- Einfache Anmeldung
- Anmeldung mit ID-Karte
- PIN-Anmeldung

8. Sicherheitstechnische Details von Amazon AWS

UCPS wird auf der Amazon AWS-Plattform gehostet. AWS erfüllt die breite Palette international anerkannter Informationssicherheitskontrollen und branchenspezifischer Konformitätsstandards wie ISO 27001, HIPAA, FedRAMP, SOC 1 und SOC 2 (siehe die detaillierte Liste der konformen Standards im AWS Security Whitepaper).

Die Hosting-Umgebung ist so konzipiert, dass die von AWS bereitgestellten Dienste und Sicherheitsfunktionen genutzt werden, um unsere Anwendung zu sichern und zu überwachen.

Zu den verschiedenen Funktionen, die genutzt werden, gehören:

- Verschiedene AWS-Anmelde-informationen für Anmeldung/Zugriff
- Sicherheitsprotokolle
- Instanzisolierung
- Firewalls/API-Zugriff
- Sichere HTTPS-Zugriffspunkte
- Netzwerksicherheit (VPC-Isolierung, Netz-werksicherheitsgruppen, Netzwerkzugangs-kontrollliste, Internet-Gateway usw.)
- Speicherung
- Einfacher Benachrichtigungsdienst zur Überwachung von CloudWatch-Anwendungsprotokollen

UCPS wird in den folgenden AWS-Regionen bereitgestellt:

- Tokio (ap-northeast-1)
- Sydney (ap-southeast-2)
- Frankfurt (eu-central-1)
- North Virginia (us-east-1)

Siehe Introduction to AWS Security und AWS Security Documentation für weitere Details zur globalen Infrastruktur und dienstspezifischen Sicherheit.

UCPS verwendet MongoDB Atlas, das für die Datenbankspeicherung auf AWS gehostet wird. Der gehostete Datenbank-Cluster befindet sich in der gleichen Region wie die UCPS-Instanz. Dieser Datenbank-Cluster ist als 3-Knoten-Replikatgruppe konfiguriert. MongoDB Atlas setzt jeden Knoten automatisch in Verfügbarkeitszonen innerhalb der Region ein, um Redundanz und Hochverfügbarkeit zu gewährleisten.

Siehe MongoDB Atlas AWS Reference document für Details zur Erstellung und Bereitstellung von Datenbank-Clustern auf AWS.

9. Über UTAX

UTAX ist als Partner leistungsstarker Fachhändler der Wegbereiter für digitale Prozesse. Büro-kommunikationslösungen und IT-Prozesse auf der Höhe der Zeit sind unsere Expertise: Mit der Erfahrung aus mehr als 60 Jahren bieten wir alles, was das Dokumentenmanagement und Projekt-geschäft leichter macht.

Als eingetragene Marke der TA Triumph-Adler GmbH wird UTAX in Deutschland über ein Netz aus über 200 autorisierten Vertragshändlern vertrieben. International agieren wir in über 40 Ländern der EMEA-Region.

Dabei setzen wir auf absolutes Vertrauen als Basis einer langfristig erfolgreichen Partnerschaft. Wir sind immer erreichbar und kümmern uns um die Bedürfnisse unserer Partner wie um unsere eigenen. Denn ihr Erfolg ist auch unser Erfolg.

Damit Sie sich auf Ihr eigentliches Geschäft konzentrieren können.

IF IT WORX, IT'S UTAX