TA CLOUD PRINT AND SCAN SECURITY WHITEPAPER

Über TA Cloud Print and Scan

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

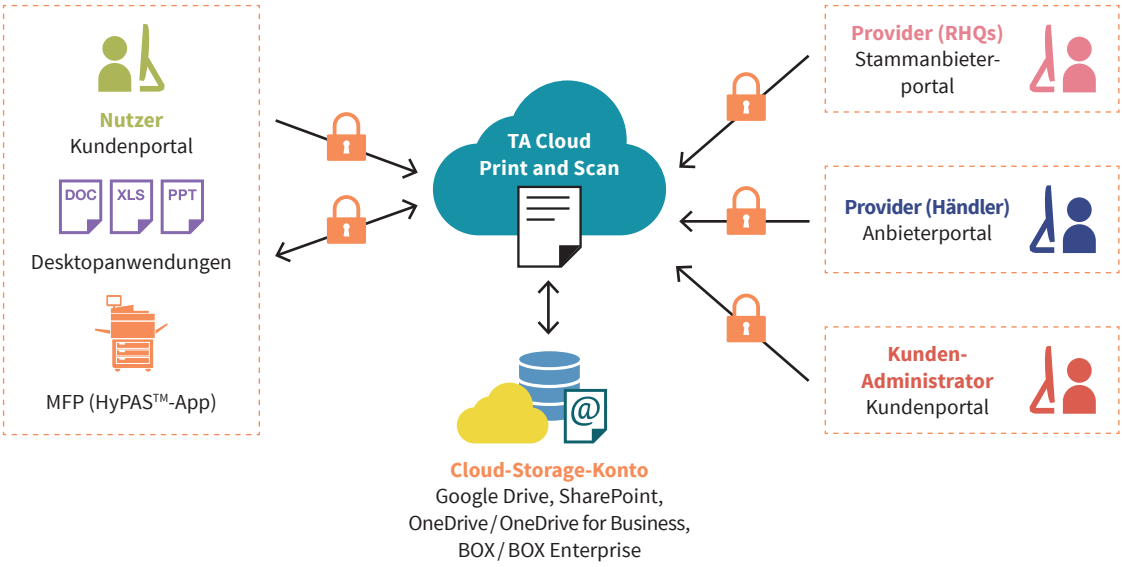
Dieses Whitepaper informiert Händler und Anwender über Sicherheitsmaßnahmen in TACPS. Für Triumph-Adler hat der Schutz der von TACPS verarbeiteten Datenbestände höchste Priorität. Die Datenbestände sind durch die Sicherheitskonfiguration und und die Sicherheitsfunktionen von TACPS streng geschützt.

Viel Freude bei der Lektüre

Ihr Team von TA Triumph-Adler

INHALT

1. Die Komponenten von TA Cloud Print and Scan



(Abb. 1-1) TACPS-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 TACPS-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 TACPS-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 TACPS-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 TACPS-Server her. Kunden können ihre hochgeladenen Druckaufträge über die TACPS-Desktopanwendung freigeben. Mit dieser Anwendung können Kunden ihre Dokumente auch scannen.

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

bsi ISO/IEC 27001 Information Security Management CERTIFIED

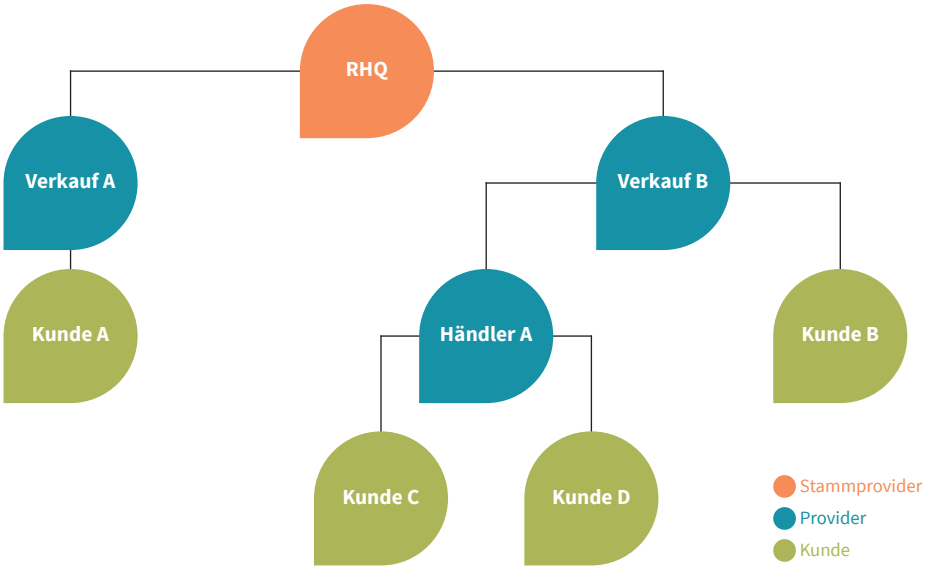
TACPS wurde bei KYOCERA Document Solutions Development America (KDDA) entwickelt, das nach ISO 27001 zertifiziert ist.

2. Mehrinstanzenfähigkeit

TACPS 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 TA Triumph-Adler 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 TACPS-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
Kundenbenutzer	Zugriff nicht möglich	Zugriff nicht möglich	Zugriff möglich Kann nur eigene Protokolldaten sehen	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)
Benutzer, die nicht im TACPS-System sind Benutzer, die vom Administrator als Ziel für Berichte festgelegt wurden	Zugriff nicht möglich	Zugriff nicht möglich	Zugriff möglich Bericht über Anbieterverträge Bericht über Kundenverträge Bericht über die Vertragshistorie	Zugriff nicht möglich

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

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

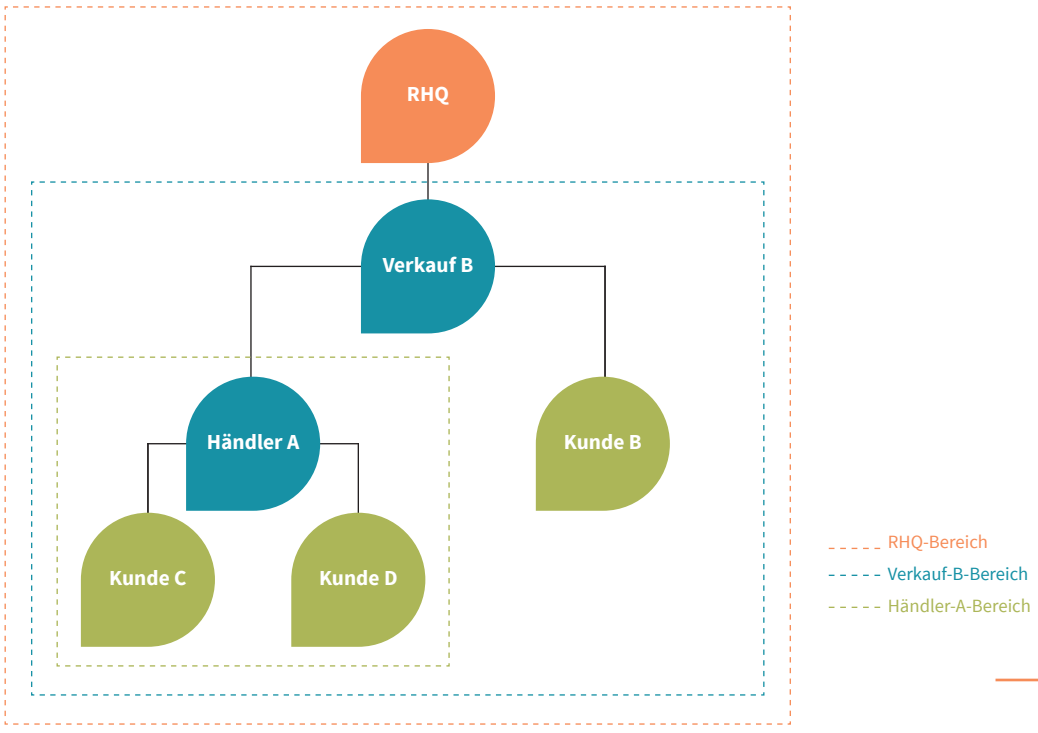
Darüber hinaus können Benutzer 1 und Benutzer 2 vom Kundenportal aus keine weiteren Benutzer in der Organisation Kunde A sehen, nur der Admin (der ein Admin in Kunde A ist) kann Benutzer 1 und Benutzer 2 (und sich selbst, den Admin) als Benutzer in der Organisation Kunde A sehen.

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. Benutzerkennung und -authentifizierung

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

3.1. Kontosperrungsrichtlinie

Die Kontosperrungsrichtlinie schützt TACPS 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.

Anzahl fehlgeschlagener Anmeldeversuche	Drei Versuche
Aufhebung der Sperre	30 Minuten

3.2. Passwortrichtlinie

Der Benutzer muss ein sicheres Passwort verwenden, das der TACPS-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.

Zusätzlich zu den Kennwortrichtlinien wird das Kennwort nicht direkt in der Datenbank gespeichert, sondern nur der Hash-Wert , wodurch verhindert wird, dass das Kennwort des Benutzers im Falle einer Sicherheitslücke ausgelesen wird. Jedes Mal, wenn ein Benutzer seine Anmeldedaten eingibt, wird der Hash-Wert des eingegebenen Passworts mit dem für diesen Benutzer gespeicherten Passwort-Hash-Wert verglichen.

Der Browser verdeckt alle Kennwörter in den Kennworteingabefeldern, um zu verhindern, dass Personen in der Nähe das Kennwort des Benutzers beiläufig vom Bildschirm ablesen können.

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.)

3.3. 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 TACPS-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.

3.4. PIN-Authentifizierung

Um die Anmeldung bei der TACPS 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 TACPS PIN-Authentifizierungsfunktionen, die an verschiedene Situationen angepasst werden können..

- Die Länge des PIN-Codes kann aus 4, 5 oder 6 Ziffern ausgewählt werden.
- Es kann ein beliebiger PIN-Code selbst festgelegt werden.
- Automatische Generierung von Zufalls-PIN-Codes möglich
- Der PIN-Code wird unkenntlich gemacht und als „****“ angezeigt.
- Wenn der Kundenadministrator den PIN-Code für einen Benutzer festlegt, wird der konfigurierte PIN-Code anschließend maskiert. Der eigene PIN-Code des Admins wird jedoch unmaskiert angezeigt.

3.5. ID-Karten-Authentifizierung

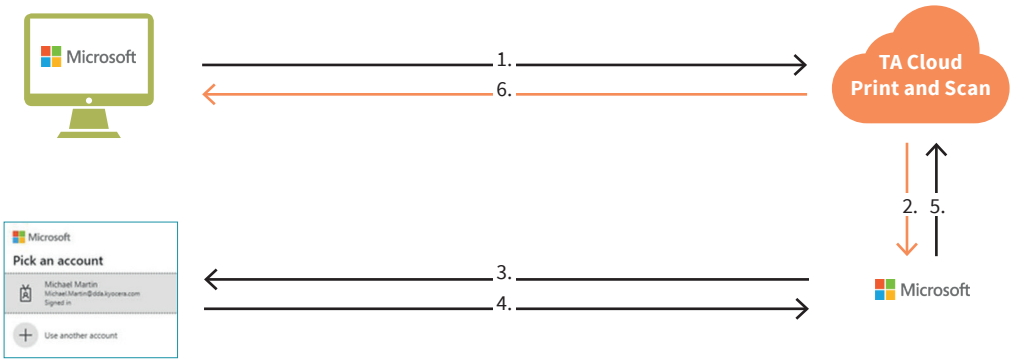
Die Authentifizierung mit ID-Karten wurde als alternative Methode zur Vereinfachung der Anmeldung bei der TACPS-HyPAS™-Anwendung hinzugefügt. Die Registrierung und Verwaltung von ID-Karten wird in der HyPAS™-Anwendung durchgeführt, nachdem sich ein Benutzer dort authentifiziert hat. Die Verwaltung der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

3.6. Authentifizierungs- und Identitätsserver von Drittanbietern

TACPS unterstützt die Authentifizierung von Drittanbietern und ihren entsprechenden Identitätsservern.

3.6.1. 3rd Party Authentifizierung und OAuth2

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



1. Der Benutzer klickt auf "Mit Microsoft anmelden".
2. TACPS 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 TACPS.
6. Die Kontrolle wird an TACPS zurückgegeben und TACPS 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.

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

3.6.2. 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 TACPS anmelden.

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

In diesem Zusammenhang sind einige wichtige Hinweise zu beachten:

- TACPS speichert keine Microsoft Entra ID Anmeldedaten; TACPS folgt dem OAuth2-Authentifizierungsworkflow und leitet zur Überprüfung der Anmeldedaten grundsätzlich zu Microsoft Entra ID weiter
- TACPS verwaltet den Microsoft Entra ID-Benutzer nicht
  - Wenn der entsprechende TACPS-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 TACPS-Benutzer auf TACPS 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 TACPS HyPAS App zu authentifizieren.

3.6.3. 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.

4. Firewall-Konfiguration

Erforderliche Ports:

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

*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 TACPS-Kommunikation zu öffnen.

Sicherheit hat bei TA Triumph-Adler höchste Priorität.

5. Technische Details zum Datenschutz

Dieses Kapitel ist für Personen mit technischen Fachkenntnissen bestimmt.

5.1. Schutz der gespeicherten Daten

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

5.1.1. Zugriffssteuerung

Die Umgebungsressourcen von TACPS 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 TACPS und zu den Anwendungsdaten. Die Benutzer müssen über eine entsprechende RBAC-Autorisierung (rollenbasierte Zugriffssteuerung) verfügen.

5.1.2. Authentifizierung

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

5.1.3. Verschlüsselung

TACPS 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 TACPS-Servers wird diese Verschlüsselung speziell für die Authentifizierung verwendet (Generierung des Hash, wenn ein Benutzer einen Anmeldeversuch unternimmt).

Wie in Kapitel 7 beschrieben, wird TACPS 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 TACPS-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 TACPS streng geschützt.

5.1.4. In TACPS verwendete Informationen

TACPS-Komponente	Informationsbestände (verwendet zum Zweck der Identifikation und Kommunikation innerhalb von TACPS)
TACPS-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 TACPS-Benutzers • Geräteinformationen (Seriennummer, Netzwerkinformationen wie Hostname und IP-Adresse) jedes TACPS-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
TACPS-HyPAS™	• Vom TACPS-Server generierte Authentifizierungs-Token zur Authentifizierung des Geräts oder des angemeldeten TACPS-Benutzers, um Informationen an den TACPS-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)
TACPS-Desktopanwendung	• Proxy-Einstellungen des Netzwerks, mit dem der Desktop verbunden ist; wird verwendet, um die Kommunikation zwischen der TACPS-Desktopanwendung und dem TACPS-Server zu erleichtern • Vom TACPS-Server generierte Authentifizierungs-Token zur Authentifizierung des Geräts oder des angemeldeten TACPS-Benutzers, um Informationen an den TACPS-Server zu senden und von diesem zu empfangen • Dokumente (PDF), die aus Desktopanwendungen über die Druckwarteschlange der TACPS-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 TACPS-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 TACPS-HyPAS™ den Druckauftrag herunterladen kann)
TACPS Chrome-Erweiterung	• Vom CPS-Server generierte Tokens, die das Gerät oder den angemeldeten Benutzer authentifizieren.

5.1.5. Datensicherung

Die Sicherung der TACPS-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.

5.2. Schutz der Kommunikationsdaten

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

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

5.2.1. Benutzerzugriff

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

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

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

Diese Informationen umfassen:

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

5.3. Sichere Kommunikation zwischen dem TACPS-Server und Datenbanken

TACPS 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.

5.4. Direktes Drucken/Scannen aus Box

Wenn ein Kunde seinen Box-Speicher mit TACPS verknüpft, wird beim Drucken oder Scannen (einschließlich Faxweiterleitung) der TACPS-Zwischenspeicher umgangen und direkt aus dem Box-Speicher gedruckt bzw. in den Box-Speicher gescannt, um den Datenschutz und die Sicherheit zu erhöhen.

5.5. Prüfung auf Sicherheitslücken

Um das TACPS-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.

6. Geräteauthentifizierung

Zum Schutz vertraulicher Informationen, die zwischen TACPS und TA Triumph-Adler 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

7. Sicherheitstechnische Details von Amazon AWS

TACPS 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, Netzwerksicherheitsgruppen, Netzwerkzugangs-kontrollliste, Internet-Gateway usw.)
- Speicherung
- Einfacher Benachrichtigungsdienst zur Überwachung von CloudWatch-Anwendungsprotokollen

TACPS wird in den folgenden AWS-Regionen bereitgestellt:

- Tokio (ap-northeast-1)
- 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.

TACPS verwendet MongoDB Atlas, das für die Datenbankspeicherung auf AWS gehostet wird. Der gehostete Datenbank-Cluster befindet sich in der gleichen Region wie die TACPS-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.

8. Über TA Triumph-Adler

TA Triumph-Adler ist Ihr Wegbegleiter ins digitale Büro. Bei uns bekommen Sie alles für den Arbeitsplatz der Zukunft, und das aus einer Hand. Wir entwickeln und liefern ganzheitliche Managed Document Services (MDS), die den Bearbeitungsprozess von Dokumenten im vernetzten und mobilen Büro vollständig abdecken.

Die digitale Transformation lässt sich mit einem verlässlichen Partner an der Seite mutiger angehen und erfolgreicher umsetzen. TA Triumph-Adler ist dieser Partner.

Triumph und Adler sind seit dem 19. Jahrhundert vertraute und klangvolle Namen in den Büros. Früher vor allem für Schreibmaschinen bekannt, sind wir heute präsent mit Druckern und Kopierern. Wir reden allerdings lieber von MFPs, also Multifunktionsprintern, denn längst sind unsere Geräte mit einer Vielzahl von Zusatzoptionen elektronisch aufgerüstet.

Der Umgang mit Dokumenten ist seit gut 120 Jahren unser Kerngeschäft – diese Expertise übertragen wir jetzt in die digitale Ära. Wir sind Ihr Ansprechpartner, wenn es um das elektronische Archivieren, Verwalten und Bearbeiten von Dokumenten geht. Unsere Angebotspalette reicht von der Einsteigerlösung zum Archivieren bis zum individuell ausgestalteten ECM-System. Wenn Sie mehr wollen – fragen Sie uns. Wir liefern!

Damit Sie sich auf Ihr eigentliches Geschäft konzentrieren können.