Schnittstellen Hard- und Software

Inhaltsverzeichnis

1 Druckgeräte-Konfiguration

1.1 Implementierung

Die im Folgenden aufgeführten Besonderheiten und Schnittstellen sind im TK-Umfeld zu berücksichtigen. Jedes zu liefernde Druckgerät und jeder installierte Treiber unterstützt diese Funktionen.

Bei einer notwendigen Anpassung des bei Erstimplementierung (respektive Aktualisierung) verwendeten Treibers unterstützt der AN bei der Auswahl, Konfiguration und Implementierung.

Der AN liefert die entsprechenden Installationspakete inklusive Treiber und Customizing der Einstellungen durch geeignete automatisierte Verfahren (siehe dazu 1.3)

Die TK erstellt die für die Softwareverteilung und Installation erforderlichen MCM (ehemals SCCM) Installationsroutinen. Es dürfen keine Userinteraktionen notwendig sein.

Für die Implementationen ist bei der TK ein entsprechender "Changeprozess" zu durchlaufen. Der AN liefert die vorgenannten Treiber und Einstellungen, unterstützt die TK bei der Installation im Technischen Abnahme Center (TAC) der TK-Unternehmenszentrale, stellt den Ausdruck von ein- und mehrseitiger Dokumenten aus Microsoft Office für jeden Ausgabeschacht sicher. Anschließend laufen TK-seitig die weiteren Abnahmeprozesse. Eventuell erforderliche Anpassungen an der Gerätefirmware (Drucker und MFG), an den Treibern oder Treibereinstellungen sind durch den AN kostenfrei durchzuführen.

1.2 Papier- und Schacht-Einstellungen

Bei den derzeit verwendeten Druckgeräten von Ricoh sind i. d. R. folgende Einstellungen vorgenommen:

Grundanforderung an jedes Drucksystem:	**Papierformat**	**Papiersorte**
Schacht 1 Manuelles Fach	i.d.R. A4	Normal
Schacht 2: TK-Papier m. Logo auf der ersten Seite oben rechts	i.d.R. A4	Briefkopf
Schacht 3: Blanko Papier	i.d.R. A4 außer bei A3 Druckern	Normal
Duplexdruck	-	-
Einseitig oder auch mehrseitig bedruckte Seiten mit Logo müssen richtig gedruckt werden.	-	-

1.3 Treiber und Treibereinstellungen:

Abweichend von den Default Einstellungen nach der Installation des Druckertreibers waren bislang folgende Einstellungen erforderlich und automatisiert einzustellen:

- Schachteinstellungen: Zusatzfach ist einzustellen

- Papierformate sind wie in der Druckerausstattung beschrieben einzustellen
- Duplexeinheit ist einzuschalten
- Duplexdruck ist als Standard einzustellen
- Der Modus für den alternativen Briefkopf (Alternativ Letterheadmode) ist zu aktivieren, damit einseitiges Briefpapier korrekt gedruckt wird
- Standardmäßig ist der S/W-Druck aktiv, Farbdruck kann durch die AW ausgewählt werden

Diese Angaben dienen dem AN als Hinweis zur Abschätzung eventueller Aufwände für die zukünftige Umgebung.

2 Verschlüsselung

Jegliche Kommunikation mit den Druckern und Multifunktionsgeräten hat vollständig verschlüsselt (vorzugsweise via Zertifikat) zu erfolgen. Dazu gehört mindestens:

- Pull-Print (auch KISS24 und SAP)
- Direktdruck (auch KISS24 und SAP)
- Scan-Prozesse
- Zugriff auf die Geräte-Web-Konsole
- Kommunikation zwischen Management-Software und Druckgeräten

3 Anbindung an das TK-Netzwerk

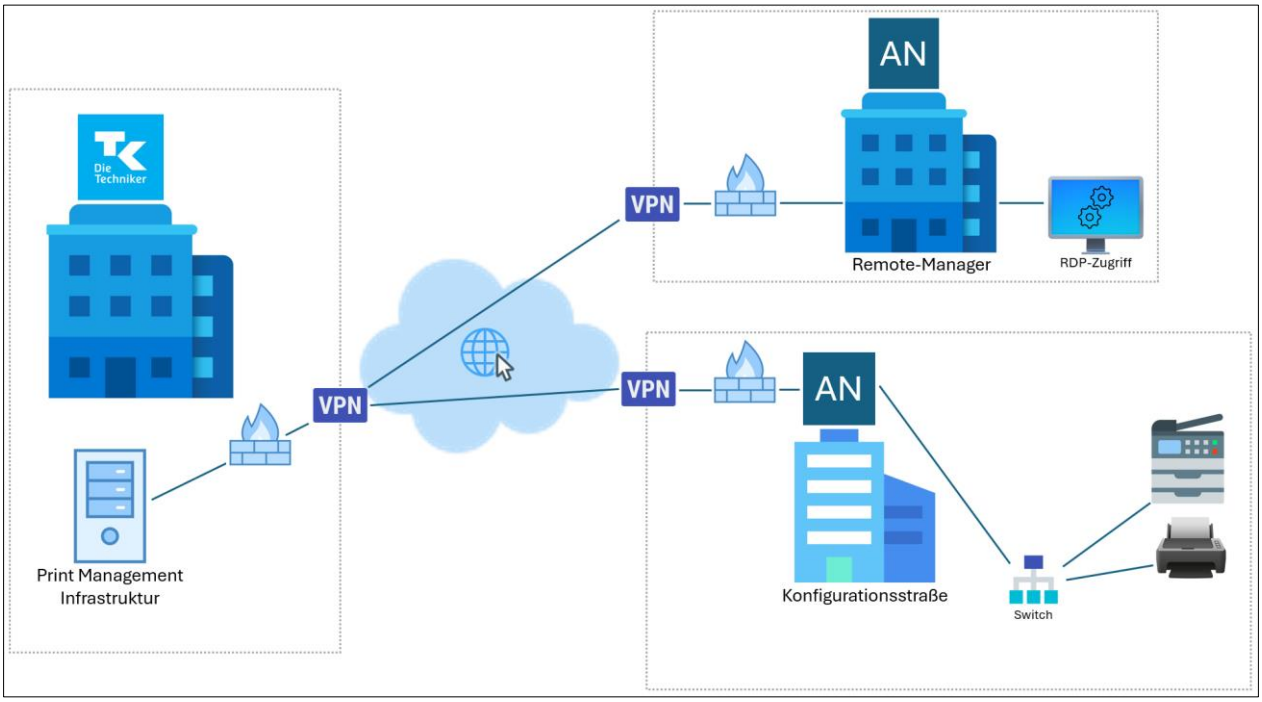


Abbildung 1 - Prinzipielle Anbindung

3.1 Betrieb durch die Remote-Manager

Für die Erbringung der betrieblichen Tätigkeiten durch den AN ist eine VPN-Verbindung zwischen dem AN und der TK erforderlich.

Stand heute ist der AN über einen Site2Site-VPN-Tunnel mit der TK verbunden und verbindet sich über RDP mittels eigener Client-Hardware über einen dedizierten Jumpserver innerhalb der DMZ der TK auf die jeweiligen definierten Netzwerkziele innerhalb der TK. Von dort kann auch die Vor-Konfiguration neuer Geräte, die sich beim AN befinden, durchgeführt werden.

Es bedarf dazu der Bereitstellung eines ausreichend schnellen Internet-Zugangs (mind. 100Mbit, der Upload kann über eine geringere Bandbreite verfügen) und einer festen öffentlichen IPv4 Adresse durch den AN.

Die konkrete Umsetzung wird im Rahmen der projektvorbereitenden Phase zwischen dem AN und der TK festgelegt.

3.2 Konfigurationsstraße

Zur Vorkonfiguration (u.a. Gerätekonfiguration per Template und Zertifikatserlangung) der Drucker und Multifunktionsgeräte wird eine VPN-Anbindung (Site2Site) benötigt.

Die Druckgeräte sind über die VPN-Verbindung mit den notwendigen und abgestimmten Anpassungen zu versorgen.

Es bedarf dazu der Bereitstellung eines ausreichend schnellen Internet-Zugangs (mind. 100Mbit, der Upload kann über eine geringere Bandbreite verfügen) und einer festen öffentlichen IPv4 Adresse durch den AN.

Die konkrete Umsetzung wird im Rahmen der projektvorbereitenden Phase zwischen dem AN und der TK festgelegt.

3.3 Raum für Anbindungstechnik und Konfigurationsserver

3.3.1 Lage der Räumlichkeit

Der Raum für den Einbau der unter Ziff. 3 dargestellte Anbindung und die beim AN zu installierenden Komponenten sollen in einer nicht gefährdeten Lage, z.B. nicht in der Nähe von Hauptzugangsbereichen untergebracht sein. Ferner soll die Positionierung innerhalb des Gebäudes in Bereichen mit möglichst wenig Publikumsverkehr und mit guter Überwachungsmöglichkeit erfolgen. Bei Gebäuden, die besonderen Umweltbedrohungen ausgesetzt sind (z.B. Überflutungsgefahr) ist der Aspekt der Schadensminimierung bei der Raumauswahl zu berücksichtigen.

3.3.2 Einbruchsschutz und Brandschutz

Der Raum soll fensterlos sein. Sind Fenster hier nicht vermeidbar, müssen diese hinreichend einbruchssicher und von außen undurchsichtig sein.

Der Raum ist grundsätzlich im Rahmen der allgemeinen Sicherungsmaßnahmen nach dem Prinzip der Bewegungserkennung zu sichern und muss in das allgemeine Einbruchmeldesystem integriert sein. Für die Räumlichkeiten muss ein angemessener Brandschutz, eine ausreichende Brandfrüherkennung sowie ausreichende Löschtechnik vorhanden sein.

3.3.3 Zutrittskontrolle und -protokollierung

Der Raum muss über eine Zutrittskontrolle verfügen. Hierzu zählen neben technischen auch organisatorische Maßnahmen (z.B. Personenanmeldung). Bei der Umsetzung der Maßnahme müssen die Erfordernisse des Datenschutzes ausreichend berücksichtigt werden. Die Erteilung von Zutrittsberechtigungen muss restriktiv erfolgen, alle zutrittsberechtigten Personen müssen jederzeit ermittelbar sein und ein Entzug einer Zutrittsberechtigung muss kurzfristig und wirksam umsetzbar sein. Kann der Zutritt zum Raum nicht ausreichend eingeschränkt werden, so müssen die IT-Systeme zusätzlich in einem abgeschlossenen Rack verwahrt werden.

Die Schlüssel zu diesem Rack müssen sicher verwahrt werden und dürfen nur berechtigten Personen zugänglich sein. Der Zutritt zum Raum muss mittels einer starken (Zwei-Faktor-) Authentisierung erfolgen. Der Zutritt muss nachvollziehbar protokolliert werden. Die Protokolldaten sind revisionssicher aufzubewahren. Sofern nicht durch andere Vorschriften oder Bestimmungen verschärfend geregelt, gilt für diese Protokolldaten eine Mindestaufbewahrungsfrist von 12 Monaten.

3.4 Bereitgestelltes Equipment

Die TK stellt einen IPSEC-Endpunkt (z.B. Fortigate VPN Device) zum Einbau in ein 19 Zoll Rack zur Verfügung.

Die zu versorgenden Systeme erhalten eine DHCP IPv4 Adresse und sind aus dem TK-Netzwerk heraus über die Management-Umgebung des AN mit den Konfigurationen und Zertifikaten zu versorgen.

Den dafür benötigten Switch hat der AN zu stellen und zu konfigurieren.

Bedingungen:

Gerät	Anforderung	Bemerkung
Anschlüsse	LAN Anschlüsse 100 MBit/Fullduplex, wahlweise auf 1 GBit respektive Automatisch einstellbar.	Die Anzahl der Anschlüsse muss für die Versorgung/Vorkonfiguration der Systeme im Rollout und Incidentfall ausreichend sein.

Der AN sorgt für eine ausreichende Verfügbarkeit der Strom und LAN Anschlüsse.

4 Zertifikatsversorgung

Es kommt ein zertifikatsbasierendes Verfahren auf Basis einer vorhandenen Public-Key-Infrastructure (PKI) mit 4096 bit RSA und SHA-256 Hashalgorithmus zum Einsatz.
Jedes einzelne Gerät, das mit dem TK-Netzwerk verbunden wird, muss für die Autorisierung zwingend über ein individuelles Zertifikat (Gültigkeit 2 Jahre) verfügen, dieses Zertifikat ist alle zwei Jahre zu erneuern. Eine automatisierte Zertifikatserlangung und -aktualisierung wird positiv bewertet (siehe Anlage L1 Fragenkatalog).

Aktuell setzt die TK eine Public Key Infrastructure (PKI) ein, die auf einer Microsoft Certificate Authority mit 4 angebundenen Domänen basiert. Die Server werden mit Windows Server 2022 Standard oder höher betrieben.

Als Schnittstelle für die Zertifikatserlangung von Druckern und Multifunktionsgeräten ist NDES/SCEP von Microsoft im Einsatz.

Darüberhinaus steht planmäßig zum Vertragsbeginn ein Zertifikatspotal von Entrust (Cryptographic Security Platform v1.2) zur Verfügung, hier werden die Protokolle SCEP und ACMEv2 angeboten. Die bisherige NDES/SCEP-Schnittstelle von Microsoft soll damit abgelöst werden.

5 Authentifizierung an den Multifunktionsgeräten

5.1 Kartenleser

Angebotene Kartenleser müssen mindestens die folgenden Technologien unterstützen, um eine Kompatibilität mit denen sich im Einsatz befindlichen Hausausweisen/Chips sicherzustellen.

- Mifare DESfire EV1, EV2 und EV3

- Mifare Classic
- Mifare Plus
- Mifare Ultralight

Der angebotene Kartenleser muss zudem zukünftige mobile Authentifizierungen über NFC Apple Wallet unterstützen.

5.2 Grundlegendes

Die Benutzeridentifizierung erfolgt durch einen Chip/Transponder/Karte oder Aufkleber, im Folgenden *Chip* genannt. Zudem muss die Authentifizierung jederzeit auch durch die Active Directory Anmeldedaten (Username & Passwort) erfolgen können.
Dies setzt voraus, dass die MFG über eine vollwertige Tastatur (mit Layout einer PC-Tastatur) verfügen.

Für die Eintragung der Chip-ID steht bedarfsweise ein Attributsfeld im AD-Benutzerobjekt zur Verfügung.

Die Verknüpfung zwischen User und Chip-ID kann alternativ auch in der Verwaltungssoftware des AN / Herstellers gespeichert werden.

In beiden Fällen muss die Verwaltungssoftware des über eine lesende AD-Anbindung verfügen.

Chips sind der Dienststelle (Dst) vorrätig und werden aktuell an den Ricoh-Bestandsgeräten genutzt.
In einigen Fällen nutzen die TK-Standorte auch eigene Chips. Sofern es technisch funktioniert, ist die Nutzung auch als zulässig.

Zum Leistungsbeginn ist der AN aufgefordert, die Benutzeridentifizierung an den Geräten auch über NFC Apple Wallet bereitzustellen.

5.3 Funktionaler Ablauf der Chip-Zuordnung

1. Chip wird an die TK-Mitarbeitenden ausgehändigt bzw. sind bereits in deren Besitz.
2. TK-Mitarbeiter authentifiziert sich am MFG durch AD-Benutzername und AD-Kennwort.
   Bei X Sekunden (X ist eingestellt) Inaktivität ist eine Reauthentifizierung erforderlich bzw. der Vorgang wird abgebrochen und muss neu gestartet werden.
3. Nach Einlesen der Chip-ID wird diese dem AD-Benutzerobjekt oder Verwaltungssytem die Chip-ID zugeordnet.

5.4 Aufheben / Löschen einzelner Chip-Zuordnungen durch den AN / TK-IT

Der AN muss einzelne Benutzer-/Chip-Zuordnungen auf Basis von übermittelten Tickets aufheben. Das kann notwendig sein, wenn z.B. Mitarbeitende die TK verlassen haben und der Chip anderweitig genutzt werden soll.

Darüberhinaus wird es positiv bewertet (vgl. Anlage XX Wertungsmatrix), wenn der AN eine Möglichkeit bereitstellt, so dass die TK-IT Benutzer-/Chip-Zuordnungen mittels PowerShell-Script über ein Ansible Playbook dokumentiert und geordnet aufheben kann.

5.5 Sperren bekannter Chips

Vor allem in der TK-Unternehmenszentrale kommen bis zu 1.000 Gäste-Hausausweise zum Einsatz, die bedarfsweise an externe Mitarbeitende ausgeben werden.
Diese Hausausweise verfügen über einen kompatiblen Mifare DESfire Chip.

Der AN muss sicherstellen, dass diese Ausweise nicht für die Authentifizierung an den Multifunktionsgeräten genutzt werden dürfen.
Dazu muss der AN Möglichkeiten der Chip-ID-Dokumentation bereitstellen, z.B. ein externer Kartenleser, der an einem Windows-Client genutzt werden kann. Die gesammelten Chip-IDs müsen durch den AN gesperrt oder mit Dummy-Accounts belegt werden.

6 Pull-Print

Bei Pull-Print werden die Druckdateien an einen Pull-Print-Server gesendet und dort verwahrt. Die Benutzer melden sich an einem Drucker/Multifunktionsgerät an und rufen von dort ihre Druckdateien ab.

Druckdateien, die an Pull-Print übergeben wurden, bleiben vom Benutzer abrufbar, bis entweder der Ausdruck der Druckdatei erfolgt ist oder eine von der TK definierte Frist (aktuell 15 Tage) erreicht ist.

Bei der Abholung der Druckdateien sieht der Benutzer die gespeicherten Dateien inkl. Dateiname gelistet.
Der Benutzer hat hier die Möglichkeit die Druckaufträge zu löschen, sie zu drucken und weiterhin zu speichern oder sie lediglich zu drucken.

Der AN muss für Pull-Print verschlüsselte Verbindung konfigurieren, eine unverschlüsselte Verbindung ist nicht zulässig.

Eine verbreitete Arbeitsweise ist, über den Tag viele Druckdateien an Pull-Print zu übertragen und diese später gesammelt abzufordern und auszudrucken. Wenn beim Druck dieser Dateien ein Fehler auftritt, müssen die erfolgreich gedruckten Dateien in Pull-Print nicht mehr abrufbar und die nicht gedruckten Dateien in Pull-Print weiterhin abrufbar sein, auch wenn alle Dateien zusammen zum Druck ausgewählt wurden.

Beispiel:

- Ein Anwender erstellt drei Druckdateien.
- Abends wählt er am Drucker alle drei aus und startet den Druck.
- Druckjob1 wird erfolgreich gedruckt.
- Während des Drucks von Druckjob2 ist der Toner leer / ist das Papier verbraucht.
- Nun muss entweder nach der Behebung des Problems der Druck von Druckjob2 und Druckjob3 fortgesetzt werden, oder Druckjob3 muss weiterhin in Pull-Print abrufbar sein.

- Es ist zu verhindern, dass nicht gedruckte Druckjobs vor Ablauf der Frist aus Pull-Print verschwinden.

7 Direktdruck

Beim Direktdruck werden die Druckdateien ohne vorherige Authentifizerung direkt vom Drucker oder Multifunktionsgerät ausgegeben.

Eine Authentifizierung des Benutzers wie bei Pull-Print erfolgt nicht – der Druck startet unmittelbar.

Der Direktdruck kommt vorrangig bei Einzelplatzdruckern zum Einsatz. Der AN ist angewiesen, für alle in TK-Standorten aktiven Einzelplatzdrucker ein entsprechendes Direktdruck-Druckobjekt bereitzustellen.

Direktdruck-Druckobjekte für Multifunktionsgeräte werden vom AN auf Basis von Tickets bereitgestellt.

Aktuell wird dafür die Druckdatei an den direct printing port 9100 des Druckers gesendet.

Der AN muss für den Direktdruck eine verschlüsselte Verbindung konfigurieren, eine unverschlüsselte Verbindung ist in keinem Druckszenario nicht mehr zulässig.

8 SAP-Druck

8.1 Druckaufbereitung

Der Druckdatenstrom wird zunächst im SAP in einem sogenannten "Gerätetyp" (Englisch: device type) aufbereitet. Auf dem Weg zum Drucker erfolgt eine weitere Aufbereitung durch die jeweiligen Betriebssystemtreiber.

Für jedes in der TK eingesetzte Druckermodell soll der Druckerhersteller einen passenden SAP-Gerätetypen mitliefern oder zusichern, dass das Druckermodell mit einem von der SAP-AG im Standard ausgelieferten SAP-Gerätetypen problemlos betrieben werden kann und diesen nennen.

8.2 SAP: Spool-Auftrag vs. Ausgabeauftrag

Für jede (gewünschte) Ausgabe aus SAP entsteht zunächst ein Spoolauftrag.

Für die tatsächliche Ausgabe kann aus einem Spoolauftrag ein Ausgabeauftrag erzeugt werden.

Ausgabeaufträge aus Spoolaufträgen können sofort automatisch oder nachträglich erzeugt werden.

Spoolaufträge müssen keine und können beliebig viele Ausgabeaufträge haben.

Möglich Arten von Ausgabeaufträgen sind:

- Ausgabe an Drucker
- Ablage im Archiv

- Versand des Outputs per Mail
- Ablage der Rohdaten in einer Datei

8.3 Druckweg

8.3.1 Druck aus Batch

Druck aus Batch soll aus Datenschutzgründen nie direkt auf einem Drucker landen. Für Druck aus Batch ist in allen SAP-Systemen ein Drucker „BatchDummy“ eingerichtet. Dieser Drucker hat keinerlei Verbindung zu einem Ausgabegerät und dient lediglich dazu, dass überhaupt Spoolaufträge (siehe oben) entstehen können.

Wenn Ausgabeaufträge an Drucker erzeugt werden sollen, werden diese von Hand aus den Spoolaufträgen heraus erzeugt.

Ausgabeaufträge an das Archiv werden in der Regel automatisch erzeugt.

8.3.2 Druck aus Dialog

Hier wird der sogenannte lokale Druck (SAP: koppelart G) betrieben. Für jedes Druckermodell ist in den SAP-Systemen ein Drucker hinterlegt, damit die richtige Druckaufbereitung (siehe 8.1) erfolgt. Tatsächlich sind pro Druckermodell zwei Drucker in jedem SAP-System hinterlegt, da in der Definition der Drucker im SAP zwischen simplex- und duplex-Druck unterschieden werden kann.

Die derzeit bei der TK eingesetze Modelle der Firma Ricoh können alle über den gleichen SAP-Gerätetyp (siehe 8.1) angesteuert werden. Somit sind in den SAP-Systemen nur zwei Drucker "TK_lokal-01-beidseitig“ und "TK_lokal-01-einseitig" in jedem SAP-System definiert.

Wenn nicht alle bei der TK eingesetze Modelle über den gleichen SAP-Gerätetyp angesteuert werden könnten, müssten weitere Drucker (TK_lokal-02-beidseitig / TK_lokal-02-einseitig, …) im SAP definiert werden und die Anwender müssten über das Kommentarfeld im SAP entscheiden, auf welchem Hardwaretyp ihr Ausdruck letztendlich landen soll. So war das einmal, als die TK unterschiedliche Drucker der Firma HP eingesetzt hatte.

In den Druckerdefinitionen der lokalen Drucker in den SAP-Systemen ist hinterlegt, dass der jeweilige lokale Standarddrucker der Workstation genutzt wird.

8.3.3 Sonderfälle

Druck von Paletten- und Lieferscheinen.

Hier wird aus SAP-Batch direkt auf (genau) einen Drucker im Lager gedruckt. Hierfür ist dieser Drucker im Linux der SAP-Anwendungsserver mittels cups definiert.

9 Druck aus KISS24

KISS24 ist das zentrale System der TK für die Erstellung und den Versand von Briefen in analoger und digitaler Form. Neben Rollendruck und PDF-Versand per Mail muss es auch den Druck auf Netzwerkdruckern unterstützen.

Anders als beim herkömmlichen Druck auf Netzwerkdruckern werden die Druckdateien bei KISS24 serverseitig gerendert. Eine clientseitig installierte Druckerqueue ist an der Druckjoberstellung nicht beteiligt. Lediglich für die Ermittlung des vom Anwender gewünschten Druckers liest ein Skript auf den Clients die Standard-Drucker-Queue aus. KISS24 überträgt die Druckdatei dann an den auf dem Client als Standard eingestellten Drucker.

9.1 Die Druckdatei

KISS24 rendert Druckdateien in PCL5c. PCL6 wird nicht unterstützt. Eine Druckdatei kann sich aus mehreren einzelnen Dokumenten zusammensetzen, wobei jedes Dokument definiert, ob es auf Logo- oder Blanko-Papier gedruckt werden soll. Gedruckt wird Duplex und in Farbe. Außerdem werden PJL-Befehle verwendet.

9.2 Die Drucker-Ermittlung

Da die Druckdateien auf den KISS24-Servern gerendert werden, muss der vom Anwender angesteuerte Drucker anderweitig ermittelt werden. Dafür liest ein auf den Clients installiertes Tool den Namen der Standard-Druckerqueue aus und macht die Information auf den KISS24-Servern verfügbar. Aus diesem Namen muss der Netzwerkname des Druckers ableitbar sein. Eine Änderung des Queue-Namens durch den Anwender muss unterbunden werden.

9.3 Die Schachtsteuerung

KISS24 kann keine modellspezifische Schachtsteuerung. Für die Ansteuerung des Blanko-Fachs wird ***&l1H***, für Logo ***&l8H*** gesetzt. Wichtig ist außerdem, dass die Dokumente eines Druckjobs in derselben Orientierung im Ausgabefach liegen. Bei der aktuell vorhandenen Druckerflotte wurde das erreicht durch das zusätzliche Setzen von ***&n11WdLetterhead*** an jedem Schachtsteuerungsbefehl. Werden einseitige Druckdateien gedruckt, soll der Druck möglichst schnell erfolgen – ein anfängliches Durchziehen des Papiers, um dann auf die andere Seite zu drucken, ist zu vermeiden.

Der Druckdienst muss sicherstellen, dass mit dieser einheitlichen Schachtsteuerung erzeugte Druckdateien auf allen Druckgeräten korrekt und performant ausgegeben werden.

9.4 Direktdruck

Beim Direktdruck werden die Druckdateien von KISS24 direkt an den Drucker gesendet. Eine Authentifizierung des Benutzers wie bei Pull-Print erfolgt nicht – der Druck startet unmittelbar.

Aktuell wird dafür die Druckdatei an den direct printing port 9100 des Druckers gesendet.

Der Druckdienst muss eine Möglichkeit bieten, Druckdateien zum sofortigen Druck verschlüsselt an jeden beliebigen Drucker zu senden.

9.5 Pull-Print

Bei Pull-Print werden die Druckdateien an einen Pull-Print-Server gesendet und dort verwahrt. Die Benutzer melden sich an einem Drucker an und rufen von dort ihre Druckdateien ab.

Für die Identifikation des Benutzers fügt KISS24 jeder Druckdatei den PJL-Header ‘SET HOSTLOGINNAME=*Benutzer*‘ hinzu.

Aktuell überträgt KISS24 die Druckdateien per LPR an die Pull-Print-Server. Pull-Print wird als Zielkanal identifiziert, indem der Name der auf dem Client installierten Queue mit „Pull-Print“ beginnt.

Der Druckdienst muss eine Möglichkeit zur Erkennung des Pull-Print-Weges an der Druckerqueue auf dem Client bieten. Er muss außerdem eine Schnittstelle zur Übertragung von PCL-Druckdateien an das Pull-Print-System bieten.

Die Schnittstelle soll mit lpr oder http ansprechbar sein um die notwendige Verschlüsselung zu gewährleisten. Die Nutzung von proprietären Protokollen ist unzulässig. Verschlüsselte andere Protokolle, für die es eine Protokollspezifikation gibt und die per TCP angesprochen werden kann, sind zulässig.

9.6 Feedback bei erfolgtem Druck

KISS24 wünscht sich eine Rückmeldung vom Druckdienst, wenn die Ausgabe eines Druckjobs erfolgt ist.

Die Rückmeldung kann über eine der beiden Schnittstellen erfolgen:

- Webhook
- REST

Als Event-Inhalte sind mindestens erforderlich:

- Job-ID (Identifizierung Druckauftrag)
- User (z.B. Anmeldename des TK-Mitarbeitenden)
- Zeitstempel (Uhrzeit und Datum)
- Status (z.B. Druck erfolgreich / fehlerhaft)

Die Umsetzung erfolgt im Dialog zwischen TK und AN im Rahmen der projektvorbereitenden Phase.

10 TKeasy-Druck

Neben den Aufruf von PC-Schriftgut spricht TKeasy an einzelnen Stellen auch direkt am Client verbundene (lokal oder Netzwerk) Drucker an. TKeasy verwendet dabei ausschließlich Schnittstellen, die die Java-API (z.Zt. Oracle JRE 17 Update 15) zur Verfügung stellt.

Die Java-API's selbst bauen i.w. auf die "Java Print Service API" (javax.print) auf. Es werden von TKeasy lediglich die "PrintServices" verwendet, die die Java Print Service API von Haus aus liefert (am Windows-Client zugeordnete Drucker), zusätzliche (ggf. selbst implementierte) Print Services werden hier nicht registriert oder verwendet.

Folgende API's werden im Einzelnen verwendet:

10.1 Ermittlung des PrintServices

Der Anwender hat in TKeasy die Möglichkeit, entweder den von der Plattform definierten Default-PrintService zu verwenden oder einen anderen im System bekannten PrintService als eigenen Default zu benutzen. Der Grund ist, dass über die Java Print Service API nicht in allen Fällen ein Default-PrintService ermittelt werden kann. Die Ursache hierfür ist nicht bekannt.

Ermittlung des Default-PrintServices:

```
/**
 * Liefert den im System definierten Default-PrintService.
 *
 * @return  Default-PrintService oder <code>null</code>, wenn dieser das
 *          benötigte DocFlavor nicht unterstützt.
 */
public PrintService lookupSystemDefaultPrintService() {
       PrintService systemDefaultPrintService
              = PrintServiceLookup.lookupDefaultPrintService();

       if (systemDefaultPrintService != null) {
              for (DocFlavor docFlavor :
                     systemDefaultPrintService.getSupportedDocFlavors()) {
                     if (docFlavor.equals(docFlavor)) {
                            return systemDefaultPrintService;
                     }
              }
       }

       // DocFlavor wird nicht unterstützt oder es gibt gar kein DefaultPrintService.
       return null;
```

```
}
```

Ermittlung eines eigenen Default-PrintService über den Namen (defaultServiceName). Wenn der definierte defaultServiceName nicht gefunden wird, wird der SystemDefaultService (s.o.) verwendet:

```
PrintService[] services = PrintServiceLookup.lookupPrintServices(docFlavor, null);
for (int i = 0; i < services.length; i++) {
	if (services[i].getName().equals(defaultServiceName)) {
		return services[i];
	}
}
```

Folgende DocFlavors werden von TKeasy z.Zt. verwendet. Der PrintService muss diese DocFlavors unterstützen. Inwieweit der Druckertreiber Einfluss auf die unterstützten DocFlavors des zugehörigen Java-PrintService hat, ist nicht bekannt und muss im Zweifel getestet werden:

```
new DocFlavor("application/x-java-jvm-local-objectref", "java.awt.print.Printable");
new DocFlavor("application/x-java-jvm-local-objectref", "java.awt.print.Pageable");
```

Ob künftig noch weitere DocFlavors, z.B. für Report-Druck, verwendet werden, ist nicht ausgeschlossen.

10.2 Verwendung des PrintServices

Der ermittelte PrintService wird auf folgende Arten verwendet:

Aufruf der print()-Methode direkt an einer JTable

Die JTable-Klasse bietet eine direkte Print-Methode. Diese wird unter Mitgabe des PrintServices in bestimmten Situationen direkt aufgerufen. Der Druckdialog wird hier i.d.R. nicht angezeigt.

Verwendung eines PrinterJobs für komplexere Ausdrucke

Für komplexere Ausdrucke (Bit-Images, Tabellen, Texte) wird ein java.awt.print.PrinterJob verwendet. In diesen wird ein selbst implementiertes "java.awt.print.Pageable" gestellt, was die auszudruckenden Daten erstellt:

```
final PrinterJob job = PrinterJob.getPrinterJob();
job.setJobName(task.getTaskName());
job.setPageable(pageable);
job.setPrintService(printService);
```

Es werden zusätzliche Default-PrintAttributes (MediaSize) eingestellt:

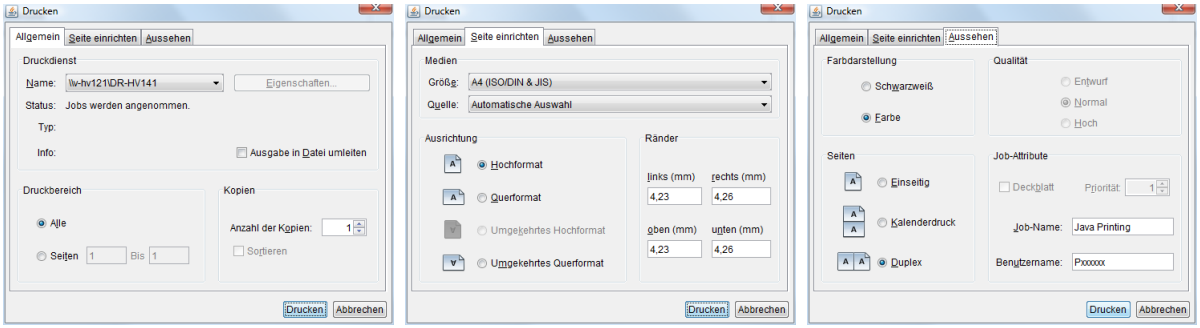
```
// Default-Einstellungen: A4-Portrait.
final PrintRequestAttributeSet printAttributes = new HashPrintRequestAttributeSet();
printAttributes.add(OrientationRequested.PORTRAIT);
MediaSizeName msn = MediaSizeName.ISO_A4;
printAttributes.add(msn);

// Als MediaPrintableArea die MediaSize eingeben, dann werden die physikalischen
// Druckränder des (Default-)Druckers voreingestellt.
final MediaSize a4 = MediaSize.getMediaSizeForName(msn);
printAttributes.add(
        new MediaPrintableArea(
                0,
                0,
                a4.getX(MediaSize.MM),
                a4.getY(MediaSize.MM),
                MediaPrintableArea.MM
        )
);
```

Für den PrinterJob wird der PrintDialog aus der Java Print Service API angezeigt, der an den nativen PrintDialog (Windows) angelehnt ist, aber in der Java-Runtime komplett nachimplementiert ist. Das Aussehen des Dialogs ist von Java vordefiniert, die Anwendung hat keinen Einfluss darauf.

```
printerJob.printDialog(attributes);
```

Für den Anwender stellt sich der Dialog folgendermaßen dar. Die im Dialog angezeigten Optionen hängen davon ab, welche Optionen der PrintService der Print Service API zur Verfügung stellt:



Die letztliche Erzeugung der Druckdaten in Java-Programm erfolgt über die Printable/Pageable-Interfaces mit AWT-Graphics-Objekten. Hier werden zahlreiche Optionen wie auch Farbe, Transparenz u.ä. genutzt.

10.3 Anforderungen an Drucker/Druckertreiber

Verwendete Drucker bzw. die zugehörigen Druckertreiber müssen über Java Print Service API die o.a. DocFlavors unterstützen und auch die erforderlichen Attribute (mit korrekten Werten!) für den PrintDialog liefern. Insbesondere beim PrintDialog werden z.Zt. vereinzelt Abbrüche beobachtet, die darauf zurückzuführen sind, dass der Druckertreiber im Windows nicht kompatibel zur Java Print Service API sind. Was die Inkompatibilität verursachen kann und ob das JRE oder der Druckertreiber "Schuld" ist, ist nicht bekannt. Die Kompatibilität muss in jedem Einzelfall (auch neue Treiberversionen) durch entsprechende Tests sichergestellt werden.

11 Scan-To-Mail

11.1 Mail-Versand von den Multifunktionsgeräten

Die Funktion „Scan-to-Mail“ ermöglicht es, eingescannte Dokumente direkt vom Drucker aus per E-Mail zu versenden – ein Computer ist dafür nicht erforderlich.

Nach der erfolgreichen Konfiguration kann das gewünschte Dokument wie eingescannt werden. Im Anschluss wählt man „E-Mail“ als Ziel aus und startet den Scanvorgang. Nach Abschluss des Scans lässt sich die Empfängeradresse bequem über das Display des Druckers eingeben. Mit einem Klick auf „Senden“ wird das Dokument automatisch per E-Mail verschickt.

Sender ist immer der angemeldete Nutzer, d.h. dessen Name/Mail-Adresse wird dem Empfänger der Mail angezeigt.

11.2 Globales Adressbuch (Exchange)

Authentifizierten Nutzenden steht an den Multifunktionsgeräten das Globale Adressbuch der Exchange-Mail-Infrastruktur zur Verfügung. Die Verbindung muss entsprechend hergestellt werden.

11.3 Konfiguration

Für Scan-toMail stehen die SMTP-Relays der TK zur Verfügung. Jeglicher Mail-Versand erfolgt grundsätzlich erst nach erfolgter Authentifizierung (z.B. Benutzeranmeldung oder Zertifikats-basiert).

Nutzendende haben während des Vorgangs die Auswahlmöglichkeit, ob das gescannte Dokument via PDF oder JPEG versendet werden soll.

11.4 Scan-Profile

An den Multifunktionsgeräten stehen verschiedene Scan-Profile zur Verfügung.

Dazu gehören:

- ScanToMe (Scannen an den eigenen Mail-Account)
- Scan-To (Auswahl über Globales Adressbuch)
- Scan-To (Freitextfeld)
- Kundenberatung (separater Ordner mit rd. 15 verschiedenen TK-internen Mail-Adressen wie z.B. pflege@tk.de)

12 Scan-To-Fax

Das Ferrari-Fax-System (kurz FerFax) wandelt, in Anlehnung an das T.37 Protokoll, E-Mails in Faxe um und sendet diese an einen Empfänger.

12.1 Versenden von FerFaxen

Das FerFax-System nimmt SMTP-Mails aus dem vorhandenen Mail-System an. Das Mail-System selber stellt einen SMTP-Server zur Verfügung zur Annahme von Mails.

Damit der Inhalt umgewandelt werden kann, darf er aus Mail-Body und Anhängen der Art Word-, Excel-, HTML-, Text- oder Bilddatei bestehen. Sowohl Plain-Text als auch HTML-Mails sind möglich. Ist der Betreffzeile das Kürzel #a# vorangestellt, werden nur die Anhänge konvertiert. Ansonsten wird der Body der E-Mail als Anschreiben mit konvertiert und als erste Seite verschickt.

Der Absender der Mail muss eine gültige FerFax Nr, besitzen.
Der Empfänger des Faxes wird durch die Fax Nr. im Anfeld bestimmt.
Es wird die E-Mail an Faxnummer@fax.uc adressiert.

12.2 Rückmeldung des FerFax-Servers

Eine Rückmeldung an Multifunktionsgeräte durch den Fax-Server erfolgt nicht. Die Rückmeldung wird an das Mail-Postfach des jeweiligen Anwenders geschickt.

12.3 Ankommende Faxe

Sind von den Multifunktionsgeräten nicht zu verarbeiten.

12.4 Berechtigung

Am Multifunktionsgerät authentifizierte Benutzer mit Mailadresse im dazugehörigen Actitive Directoryobjekt können Scan-To-Fax nutzen.

13 Automatisierte Tonerversorgung

Der AN hat die automatisierte Tonerversorgung und Tonerentsorgung für alle von ihm zu betreuenden Drucker und Multifunktionsgeräte zeit- und bedarfsgerecht sicherzustellen.

Über eine zentrale, vom AN verwaltete und zur Verfügung gestellte, Appliance (Physik oder virtuell), grundsätzlich im Netzwerk der Techniker Krankenkasse, werden die für die automatisierte Tonerversorgung erforderlichen Informationen von den betreffenden Drucker und Multifunktionsgeräten **eingesammelt**.
Fest definierte und flexible Prozesse gewährleisten die bedarfsgerechte Zubringung des Toners ohne Produktionsunterbrechung zum jeweiligen Drucker oder MFG.

13.1 Adressdatenpflege

Aktuell sind alle Bestands-Drucker und -Multifunktionsgeräte im Ricoh Ansprechpartnerportal „**O**nGoing**F**leet**M**anagement“ enthalten.

Anhand dieser Datenbank werden die Drucker und Multifunktionsgeräte mit Verbrauchs- und Wartungsmaterial versorgt. Änderungen können durch die für das jeweilige Gerät hinterlegten Ansprechpartner oder durch den AN vorgenommen werden.

Der AN hat ein vergleichbares Webportal zur Verfügung zur stellen sowie den Betrieb und die Datenpflege sicherzustellen.
Siehe dazu auch Anlage L1 Fragenkatalog.

Aktuell gibt es Felder für folgende Informationen:

- Hostname
- Seriennummer
- Straße der TK Dienststelle
- Stadt der TK Dienststelle
- Postleitzahl der TK Dienststelle
- Etage
- Raum Nr.
- Abteilung
- Name des Ansprechpartners
- Telefonnummer des Ansprechpartners

- Email Adresse des Ansprechpartners
- Firmenbezeichung
- 3 Felder für zusätzliche Standortinformationen

Die Qualität der Daten kann von zentraler Stelle nicht bewertet werden. Es ist einzelnen mit Abweichungen sowie mit unvollständigen Angaben zu rechnen.

13.2 Überwachung der Verbrauchsmaterialien (z.B. Toner) aller Drucker und Multifunktionsgeräte

Eine direkte Kommunikation der einzelnen Drucker- und Multifunktionsgeräte in das Internet ist nicht vorzusehen.

Kommunikation im TK-Netzwerk:

Die Überwachung der Tonerfüllstände hat automatisiert und bedarfsgerecht durch den AN zu erfolgen. Die Kommunikation mit den Druckern und Multifunktionsgeräten erfolgt über eine vom AN zu stellenden und zu wartende Komponente (physikalische Appliance oder virtuelle Instanz (VMWare)), vorzugsweise über snmp get oder Webservices.

Die Drucker und Multifunktionsgeräte werden über DHCP mit IP-Adressen versorgt und die Adressen können sich ändern, so dass eine DNS Namensauflösung oder andere geeignete Mechanismen verwendet werden sollen um die automatische Abfrage der Informationen sicherzustellen.

Abends oder zum Wochenende werden einige Drucker und Multifunktionsgeräte abgeschaltet und zu Arbeitsbeginn wieder eingeschaltet.

Die Netzwerkkommunikation ist auf ein Minimum zu begrenzen.

Kommunikation von der zentralen Komponente zum AN:

Es hat eine aggregierte verschlüsselte Weitermeldung der Informationen an ein definiertes Zielsystem des AN zu erfolgen. Eine Übermittlung von personenbezogenen Daten ist nicht zulässig.

14 Monitoring

Die TK nutzt für on-premise-Monitoring Grafana Enterprise und betreibt auf allen TK gemanagten Windows- und Linux-Systemen einen Monitoringagent. Dieser sammelt Performancemetriken und Logs ein zur Speicherung in zentralen an Grafana angebundenen Datenbanken. Auf dieser Plattform ist das Monitoring vom AN einzurichten und entsprechende Dashboards zu entwickeln.

Das beinhaltet z.B. das Überwachen relevanter Server-Basis-Gesundheitsdaten (u.a. Festplatten-Platz, RAM- und CPU-Auslastung) sowie spezifische Dienste, Datenbankverbindungen oder Datei-Ordner.

Setzt der AN eine eigene (Cloud-) Managementsoftware ein, welche Observability-Signale der eigenen Komponenten einsammelt, so sollen mind. die Performancemetriken über eine Web-schnittstelle ausgelesen bzw. aktiv versendet werden können.

Als technologische Grundlage kommen hier in Betracht:

- OpenMetrics bzw. Prometheus bzw. InfluxDB Line Protocol HTTPS Endpoint
- Prometheus bzw. InfluxDB 3.x bzw. PostgreSQL kompatible Datenbank
- Versand der Signale via OpenTelemetry bzw. InfluxDB Line Protocol Standard

Darüber hinaus unterstützt der AN aktiv bei der Definition und Verprobung von Alarmierungen (z.B. via Mail oder SMS an den AN) für Schwellwert-Überschreitungen.

Im Rahmen der Einführung der Cloud-Printing-Lösung werden die dazugehörigen Monitoring- und Alarmierungs-Möglichkeiten vom AN dargestellt und in Absprache mit der TK umgesetzt.