

Leistungsbeschreibung Software

Systemvoraussetzungen:

- Server
 - ⇒ Windows Server 2022 und 2025
- Arbeitsplatzcomputer
 - ⇒ Windows 11 Enterprise
 - Intel Core i3 8. Generation und neuer mit mind. 8 GB RAM und mind. 256 GB SSD
- Virtualisierung VMware vSphere ab Version 7+ und neuer
Proxmox VE 8.4.1 und neuer
- Citrix-Zertifizierung XenApp 22.03 LTSR
- Domain integriertes DFS (ohne WINS-Server)
- Datenbanken
 - ⇒ Oracle Standard Edition 2 ab Version 19
 - ⇒ MS SQL-Server Standard Edition ab Version 2019

	Kategorie/Mindestanforderungen
1.	Authentifizierung
1.1	Authentifizierung an Multifunktionsgeräten (MFP) <ul style="list-style-type: none"> - mit Unikatnummer der MIFARE Classic (Mitbenutzung der Karte für Personalzeiterfassung) - und alternativ mit Name und Passwort (z. B. Erstanmeldung und Notfallszenario bei Kartenverlust) gegenüber Active Directory
1.2	Selbstlernfunktion der Kartenzuordnung am Gerät (Zuordnung Karten-Unikatnummer zu Nutzer mittels Active Directory-Anmeldung [Name und Passwort])
1.3	Es muss möglich sein, die folgenden Funktionen erst nach Authentifizierung des Benutzers am Multifunktionssystem zur Verfügung zu stellen: <ul style="list-style-type: none"> - Kopierfunktion - Follow-Me-Druckfunktion - Scanfunktion - Faxfunktion
1.4	Möglichkeit des manuellen Abmeldens (Karte oder Taste am Gerät)
1.5	Automatisches Abmelden nach einstellbarem Zeitintervall
1.6	Bei Netzausfall oder Ausfall des Authentifizierungsservers soll trotzdem ein Kopieren mit Erfassung der Kopien möglich sein (Notfall-Account, PIN oder Abschalten der Lesegeräte).
1.7	Bei MFP's, welche nicht am Netzwerk angeschlossen werden können, muss eine Anmeldung am Gerät per PIN möglich sein (z. B. Schulen).
2.	Druck-, Accounting- und Abrechnungssoftware
2.1	Geräteunabhängiger und vertraulicher Druck auf allen Multifunktionsgeräten (Druckjobs werden auf Server gespeichert und werden vom Nutzer nach Authentifizierung an beliebigem Multifunktionsgerät zur Ausgabe freigegeben)
2.2	Beim AG existieren physisch voneinander getrennte Netzwerke (siehe Leistungsverzeichnis), in denen jeweils für sich die Geräte administriert werden müssen und unabhängige Scan-Server und Follow-Me-Server einzurichten sind.
2.3	In einem der physisch getrennten Netzwerke, dem internen Verwaltungsnetz der Stadtverwaltung, wird eine Virtualisierungsinfrastruktur über zwei Serverräume verwendet. Bei Ausfall eines Serverstandortes muss die gesamte Funktionalität von dem jeweils anderen Standort mit übernommen werden können.

	Kategorie/Mindestanforderungen
2.4	Verteilte Installation der Komponenten auf Datenbank-, Accounting- und Printserver soll möglich sein.
2.5	Loadbalancing/Ausfallsicherheit Printserver: Die Printserver sind ausfallsicher auszulegen. Es wird eine eigenständige (von der Redundanz auf Virtualisierungsinfrastrukturebene unabhängige), weitestgehend automatisierte Ausfallsicherheit, ohne Erfordernis einer Microsoft-Clusterlösung angestrebt. Eine dynamische, lastabhängige Verteilung der Druckaufträge auf mehrere Printserver ist wünschenswert und wird höher bewertet.
2.6	Die Standard-Druckwarteschlange ist fest auf Schwarz/Weiß eingestellt, um versehentliche teure Farbausdrucke zu vermeiden.
2.7	Lauffähigkeit in heterogener Systemumgebung
2.8	Entgegennahme von Druckaufträgen vom Linux-Drucksystem CUPS über die Protokolle IPP oder LPR mit Übernahme der Benutzerkennung aus dem CUPS-Druckauftrag
2.9	Nutzung einer zentralen Datenbank auf vorhandenen Datenbankservern (Microsoft SQL oder Oracle)
2.10	Rollenbasierte Zugriffsrechte der Administratoren und des User-Help-Desk für vorhandene Funktionen innerhalb der Management- und Accounting-Software
2.11	Zentrale Druckkostenabrechnung für alle Leistungsklassen: - Kostenzuordnung und Abrechnung nach Verursacherprinzip - berücksichtigt Seitenklicks (Seitenklicks mit preislicher Unterscheidung von Farbe und s/w) - Abrechnung zusammengefasst nach Kostenstellen
2.12	Möglichkeit der Kostenstellenerfassung auf Nutzer und Geräte
2.13	Konfigurationen in zentraler Oberfläche je Netzwerk administrierbar
2.14	Möglichkeit der zeitgesteuerten Synchronisation mit dem Active Directory (im Netz der Kernverwaltung erfolgt die Pflege der benutzerspezifischen Daten im Active Directory, der Kostenstelle im LDAP)
2.15	Erfasste Kosten sind in Statistiken (Reports) abrufbar.
2.16	Reports sind in den Dateiformaten CSV und XLS (oder PDF) möglich.
2.17	Möglichkeit des individuellen Anpassens von Reports
2.18	Möglichkeit des automatischen Erzeugens von Reports (wöchentlich, monatlich usw.) mit Versand per E-Mail an interne Benutzergruppen
2.19	Möglichkeit einer regelbasierten Druckauftragssteuerung (Druckregeln)
2.20	Übersichtliche Druckauftragsverwaltung am MFP mit wichtigen Informationen zu den Druckaufträgen
2.21	Möglichkeit der Behandlung der Druckjobs am MFP (Anzahl Kopien, Löschen, Speichern, Farbe/ SW Druck)
2.22	Möglichkeit von Mitteilungen an den Benutzer beim Wirken von Druckregeln
2.23	Möglichkeit der Konfiguration verschiedener Preismodelle

	Kategorie/Mindestanforderungen
2.24	Möglichkeit des automatischen Löschsens nicht abgerufener Druckjobs nach einstellbarer Zeitspanne
2.25	Möglichkeit der Steuerung von Zugriffsrechten auf Farbsysteme
3.	Scannen / Scansoftware
3.1	Der AG betreibt die Scanserverlösung Convert2PDF, welche anzubinden ist.
3.2	Möglichkeit der zentralen Konfiguration mehrerer (mindestens 20) Scanziele mit definierten Eigenschaften, die sich zentral auf alle Multifunktionsgeräte innerhalb eines Netzwerkes verteilen lassen.
3.3	Die Scandokumente müssen in zentralen freigegebenen Netzwerkressourcen abgelegt werden können (DFS). Zum Scannen verwendete Protokolle müssen aktuellen Standards entsprechen (nicht SMB v1).
3.4	Beim Scannen in das Homeverzeichnis muss der am Multifunktionsgerät angemeldete Nutzer der Besitzer der im Filesystem erzeugten Datei werden (wegen Quotaregelung). Dies muss ohne separate Anmeldung während des Scanvorgangs realisiert werden.
3.5	Möglichkeit des lokalen Scans für LK2- und LK3-Geräte für bestimmte Außenstellen, ohne Beteiligung eines zentralen Scanservers
3.6.	Die gerätebezogenen Anforderungen der Technische Richtlinie „TR-03138 Ersetzendes Scannen (RESISCAN)“ in der jeweils gültigen aktuellen Fassung müssen erfüllt werden können. Beim Scannen in zentral freigegebene Netzlaufwerke muss es daher möglich sein, zum Scanvorgang erzeugte Metadaten (z.B. Auflösung, Farbe/SW, Seitenzahl, Nutzerkennung, Dokumenten-ID, Vorgangs-ID, ...) in einem maschinenlesbaren Format (vorzugsweise XML) bereitzustellen.
4.	Managementsoftware
4.1	Möglichkeit der Überwachung, Verwaltung und Konfiguration der Geräte über eine zentrale, mehrbenutzerfähige Oberfläche je Netzwerk (Flottenmanagement)
4.2	Möglichkeit des Zugriffs je Netzwerk auf die Weboberfläche der Geräte aus zentraler Oberfläche heraus
4.3	Übersichtliche Anzeige von Verbrauchsmaterial, Fehlermeldungen und Gerätezuständen
4.4	Möglichkeit der Konfiguration von automatischen Meldungen (Fehler, Verbrauchsmaterial, Zählerstände) an interne Benutzergruppen
4.5	Möglichkeit der Konfigurierbarkeit von automatischen Meldungen (Fehler, Verbrauchsmaterial, Zählerstände) an externen Support
4.6	Kommunikation der Meldungen an externen Support muss über einen zentralen Absender (Managementserver) erfolgen.
4.7	Möglichkeit zur zentralen Verteilung von Firmware-Updates
5.	IT- Sicherheit/ Datenschutz/ Dokumentation
5.1	Fernzugriffe wie Webinterface (https), FTP (File Transport Programme) oder Telnet müssen für Administratoren einzuschränken und deaktivierbar sein.
5.2	Wenn eine Datenspeicherung auf der Festplatte des MFP erfolgt, muss diese verschlüsselt sein.
5.3	Nicht verarbeitete Druckaufträge müssen automatisch nach definierten Zeiten zu löschen sein.

	Kategorie/Mindestanforderungen
5.4	Druck- und Scanaufträge müssen nach der Bearbeitung automatisch entfernt werden (es sei denn Nutzer wählt explizit, dass sie gespeichert werden sollen).
5.5	Die Daten auf der integrierten Festplatte der MFP müssen sicher zu löschen sein (nach einem zertifizierten Verfahren mit einem Bitmuster überschreiben).
5.6	Die Verwaltung der MFP muss über verschlüsselte Protokolle erfolgen. Wenn SNMP verwendet wird: dann SNMPv3
5.7	Sicherheitspatches für zentrale Software müssen innerhalb eines Monats nach Veröffentlichung zur Verfügung gestellt werden.
5.8	Sicherheitspatches der Firmware müssen innerhalb eines Monats nach Veröffentlichung zur Verfügung gestellt werden und zentral zu verteilen sein
5.9	Alle Geräte müssen zur Netzwerkauthentifizierung den Standard IEEE 802.1X EAP TLS mit Zertifikat unterstützen.
5.10	Auf den Servern, mit denen die Software betrieben wird, kann der Auftraggeber eigenständig die jeweils aktuellen Microsoft Sicherheitspatches installieren
5.11	Alle angebotenen Softwarelösungen müssen im Kernnetz der Stadtverwaltung lauffähig sein. Alle angebotenen Leistungen (speziell MPS) sind ohne einen direkten Netzwerkzugriff von außen auf das Netz der Stadtverwaltung zu gewährleisten
5.12	Der Zugriff auf die Konfiguration von Druckern und Multifunktionsgeräten muss beschränkt werden. Änderungen dürfen nur durch Administratoren erfolgen.
5.13	Alle nicht benötigten Funktionen und Schnittstellen sind zu deaktivieren.
5.14	Aktivitäten auf Druckern und Multifunktionsgeräten müssen protokolliert werden. Der Zugriff auf die Protokolle muss auf berechtigte Personen einschränkbar sein.
5.15	Bei Rückgabe oder Austausch von Druckern und Multifunktionsgeräten müssen auf ihnen befindlichen Information sicher gelöscht werden. Das ist zu dokumentieren.
5.16	Geräteinterne Festplatten sind zu verschlüsseln, wenn die Geräte außerhalb von geschlossenen Arbeitsräumen betrieben werden.
5.17	Unbeaufsichtigt durchgeführte Fernwartungen sind geeignet zu protokollieren. Die Protokolle sind dem Auftraggeber regelmäßig zur Verfügung zu stellen.