Patientenaufruf

Technische Dokumentation



Version 1.0 · Stand März 2026

© xJRx98 Software · Jonas Ruhland · München
info@xjrx98software.de · www.xjrx98software.de

Inhaltsverzeichnis

1 Systemarchitektur 3
1.1 Netzwerktopologie 3
1.2 Kommunikationsprotokoll 3
2 Verbindungsaufbau und Transportverschlüsselung 4
2.1 TLS-Zertifikat (WSS) 4
2.2 Verbindungsmanagement 4
3 Lizenzierungssystem 5
3.1 Aufbau der Lizenz 5
3.2 Lizenzprüfung 5
3.3 Lizenzanforderung – RSA-Verschlüsselung 5
4 Datensicherheit 6
4.1 Transportverschlüsselung 6
4.2 Statistikdaten – Verschlüsselung im Ruhezustand 6
4.3 Datensparsamkeit 6
4.4 Admin-Passwort 7
5 Datenschutz (DSGVO-Hinweise) 8
5.1 Welche Daten werden verarbeitet? 8
5.2 Auftragsverarbeitung 8
5.3 Empfehlungen für den sicheren Betrieb 8
6 Statistik und Datenexport 9
6.1 Aufbau der Statistik 9
6.2 Export-Auslöser 9
6.3 Dateistruktur 9
7 Konfigurationsdateien und Datenspeicherorte 10
7.1 Übersicht 10
7.2 Konfiguration der Server-IP 10
8 Systemvoraussetzungen und Installation 11
8.1 Systemvoraussetzungen 11
8.2 Firewall-Hinweis 11
8.3 Mehrere Aufruf-Instanzen 11
9 Fehlerbehandlung und Diagnose 12
9.1 Häufige technische Probleme 12
10 Support & Kontakt 13

1 Systemarchitektur

Das Patientenaufruf-System besteht aus zwei eigenständigen Programmen, die über das lokale Praxisnetzwerk per WebSocket-Protokoll kommunizieren. Es ist kein Internet-Zugang und kein externer Server erforderlich – die gesamte Kommunikation findet innerhalb des geschlossenen Netzwerks statt.

Komponente	Funktion
Ausgabe.exe (Server)	Läuft auf dem Ausgabe-PC. Betreibt gleichzeitig den WebSocket-Server (Port 8765) und das Vollbild-Anzeigemuster.
Aufruf.exe (Client)	Läuft auf allen Eingabe-PCs (Rezeption, Behandlungszimmer). Verbindet sich als WebSocket-Client mit dem Server.

1.1 Netzwerktopologie

Ausgabe.exe übernimmt die Serverrolle: Sie lauscht auf Port **8765** (TCP/WSS) und nimmt Verbindungen von beliebig vielen Aufruf-Instanzen entgegen. Alle verbundenen Clients werden dabei synchron gehalten – Verlaufsdaten, Designeinstellungen und Anzeigedauern werden bei jeder neuen Verbindung automatisch übertragen.

- Protokoll: WebSocket über TLS (WSS) – gesicherte Verbindung im lokalen Netz
- Standard-Port: 8765 (TCP)
- Netzwerkzugang: nur im lokalen LAN/WLAN erforderlich, keine Internetverbindung nötig
- Mehrere Clients gleichzeitig: unbegrenzt viele Aufruf-Instanzen können sich verbinden

1.2 Kommunikationsprotokoll

Die Kommunikation erfolgt ausschließlich über strukturierte JSON-Nachrichten. Jede Nachricht enthält ein Feld "typ", das die Art der Nachricht beschreibt. Der Server empfängt Nachrichten von Clients und verteilt relevante Aktualisierungen an alle verbundenen Clients (Broadcast).

Nachrichtentyp	Bedeutung
aufruf	Client sendet einen neuen Patientenaufruf (Name + Raum).
verlauf	Server sendet die letzten 5 Aufrufe an neu verbundene Clients.
schrift_groesse	Admin ändert Schriftgröße – wird sofort an alle Clients gebroadcastet.
design	Admin ändert Farben oder Hintergrundbild – Broadcast an alle Clients.
anzeige_dauer	Admin ändert die Anzeigedauer – Broadcast, wird serverseitig gespeichert.
statistik_abfrage	Client fordert aktuelle Statistikdaten vom Server an.
passwort_hash_sync	Admin-Passwort-Hash wird mit dem Server synchronisiert (für Statistik-Export).

2 Verbindungsaufbau und Transportverschlüsselung

2.1 TLS-Zertifikat (WSS)

Die WebSocket-Verbindung zwischen Client und Server wird durch TLS (Transport Layer Security) abgesichert. Ausgabe.exe lädt beim Start ein X.509-Zertifikat (server.crt) und den zugehörigen privaten Schlüssel (server.key). Minimum-TLS-Version ist TLS 1.2.

> *Das Zertifikat ist ein selbstsigniertes Zertifikat, das mit der Lizenz ausgeliefert wird. Der Client (Aufruf.exe) enthält das zugehörige öffentliche Zertifikat und vertraut diesem explizit – eine Validierung über eine öffentliche CA ist bewusst nicht vorgesehen, da die Kommunikation ausschließlich im internen Netz stattfindet.*

Der Client erstellt einen SSL-Kontext mit dem Serverzertifikat und erzwingt eine Zertifikatsprüfung. Nur ein Server, der das zur Lizenz gehörende Zertifikat besitzt, kann eine Verbindung aufbauen. Dies verhindert Man-in-the-Middle-Angriffe auch im lokalen Netz.

2.2 Verbindungsmanagement

Aufruf.exe versucht beim Start automatisch, eine Verbindung zur gespeicherten Server-IP aufzubauen. Bei Verbindungsverlust wird alle 10 Sekunden ein Wiederverbindungsversuch gestartet. Der Verbindungsstatus wird durch einen farbigen Punkt im Hauptfenster angezeigt (grün = verbunden, rot/orange = getrennt).

- Verbindungs-Timeout: 10 Sekunden pro Versuch
- Keep-Alive: WebSocket Ping alle 20 Sekunden, Timeout nach 10 Sekunden
- Maximale Nachrichtengröße: 10 MB (relevant für Hintergrundbilder)
- Mindestabstand zwischen zwei Aufrufen: 5 Sekunden (serverseitig erzwungen, verhindert gleichzeitige Anzeige)

3 Lizenzierungssystem

3.1 Aufbau der Lizenz

Jede Lizenz ist eindeutig an ein bestimmtes Gerät gebunden. Sie enthält die Geräte-IDs des lizenzierten PCs, Kundendaten, Gültigkeitszeitraum, die hinterlegte E-Mail-Adresse für Passwortrücksetzmechanismen sowie das TLS-Zertifikat für die Netzwerkkommunikation. Die Lizenzdatei trägt die Endung .lic.

Lizenzfeld	Beschreibung
Kundenname	Name der Praxis / des Lizenznehmers.
E-Mail-Adresse	Für den Passwort-Einmalcode. Wird niemals extern übermittelt.
ID1	Hardwaregebundene ID (aus CPU-ID + MAC-Adresse berechnet, 12 Zeichen, hex).
ID2	Beim ersten Programmstart zufällig generierte ID, lokal gespeichert (12 Zeichen, hex).
Gültig ab / bis	Aktivierungsdatum und Ablaufdatum der Lizenz.
Lizenzierte PCs	Anzahl der gleichzeitig nutzbaren Aufruf-Installationen.
TLS-Zertifikat	Das server.crt für die verschlüsselte Netzwerkkommunikation.

3.2 Lizenzprüfung

Beim Programmstart liest Aufruf.exe die Lizenzdatei und prüft: Ablaufdatum, Übereinstimmung der Geräte-IDs mit der aktuellen Hardware sowie die Integrität der Lizenzdatei. Eine manipulierte oder abgelaufene Lizenz wird abgewiesen. Ohne gültige Lizenz startet das Programm nicht.

ID1 wird reproduzierbar aus CPU-ID und MAC-Adresse berechnet. ID2 ist eine einmalig zufällig generierte ID, die lokal gespeichert wird. Beide IDs zusammen stellen eine eindeutige Gerätebindung sicher, die auch einen Hardware-Wechsel erkennt.

3.3 Lizenzanforderung – RSA-Verschlüsselung

Wenn ein Nutzer über Aufruf.exe eine Testlizenz anfordert, werden Name, E-Mail-Adresse sowie ID1 und ID2 mit einem fest eingebetteten öffentlichen RSA-Schlüssel (2048 Bit, PKCS1-OAEP-Padding) verschlüsselt. Der verschlüsselte Datensatz wird anschließend an xJRx98 Software übermittelt. Auf diese Weise verlassen ausschließlich verschlüsselte Daten das Gerät – eine Entschlüsselung ist nur mit dem privaten Schlüssel bei xJRx98 Software möglich.

- Algorithmus: RSA-2048 mit OAEP-Padding
- Übertragenes Datenformat: Base64-codierter Chiffretext
- Inhalt der verschlüsselten Nachricht: Name, E-Mail, ID1, ID2

4 Datensicherheit

4.1 Transportverschlüsselung

Alle Daten, die zwischen Aufruf.exe und Ausgabe.exe übertragen werden, sind durch TLS gesichert. Dies gilt sowohl für Patientenaufrufe als auch für Konfigurationsnachrichten und Statistikdaten. Im lokalen Netz ohne TLS (bei fehlendem Zertifikat) würde das System auf unverschlüsseltes WebSocket (ws://) zurückfallen – dies wird in der Konsole explizit gemeldet und sollte im Produktionsbetrieb vermieden werden.

> ⚠ *Stellen Sie sicher, dass server.crt und server.key vorhanden sind. Nur so ist die Verbindung TLS-verschlüsselt (wss://). Das Fehlen der Zertifikatsdateien führt zu einer unverschlüsselten ws://-Verbindung.*

4.2 Statistikdaten – Verschlüsselung im Ruhezustand

Statistikdaten (Aufrufe pro Stunde und Raum) werden nicht im Klartext gespeichert. Der Export erfolgt als AES-256-GCM-verschlüsselte XML-Datei (.xml.enc). Der Schlüssel wird mittels PBKDF2-HMAC-SHA256 aus dem Admin-Passwort-Hash abgeleitet. Pro Datei werden ein zufälliger Salt (16 Byte) und ein zufälliger Nonce (12 Byte) neu generiert, sodass identische Inhalte nie denselben Chiffretext erzeugen.

Parameter	Wert
Verschlüsselungsalgorithmus	AES-256-GCM (authentifizierte Verschlüsselung)
Schlüsselableitung	PBKDF2-HMAC-SHA256, 100.000 Iterationen
Salt	16 Byte zufällig pro Datei
Nonce	12 Byte zufällig pro Datei
Dateiformat	salt (16 B) || nonce (12 B) || ciphertext
Speicherort	Dokumente/Patientenaufruf/Statistik/

Die Statistikdaten werden täglich um 23:59 Uhr automatisch exportiert und aus dem Arbeitsspeicher gelöscht. Ein Export erfolgt außerdem beim Beenden des Programms sowie wenn der letzte Client die Verbindung trennt. Vorhandene Dateien für denselben Zeitraum werden zusammengeführt (Merge), nicht überschrieben.

4.3 Datensparsamkeit

Das System speichert ausschließlich anonymisierte statistische Daten. Es werden lediglich Uhrzeit (Stunde) und Raum protokolliert – keine Patientennamen, keine Diagnosen, keine personenbezogenen Informationen. Die Aufrufe selbst werden nur temporär im Arbeitsspeicher gehalten und nach 15 Minuten (900 Sekunden) automatisch aus dem Verlaufsspeicher entfernt.

- Keine persistente Speicherung von Patientennamen
- Keine Übertragung von Daten ins Internet
- Verlaufseinträge: max. 5 Einträge, Ablauf nach 15 Minuten

- Statistik: ausschließlich Stunde + Raum (keine Namen)

4.4 Admin-Passwort

Das Admin-Passwort wird nie im Klartext gespeichert. Beim Setzen eines neuen Passworts wird ein kryptografischer Hash erzeugt und serverseitig in der server_config.json abgelegt. Der gleiche Hash wird für die Schlüsselableitung der Statistik-Verschlüsselung verwendet. Eine Passwort-Zurücksetzung ist über einen zeitlich begrenzten 8-stelligen Einmalcode möglich, der an die in der Lizenz hinterlegte E-Mail-Adresse gesendet wird. Der Code ist 15 Minuten gültig.

5 Datenschutz (DSGVO-Hinweise)

Das Patientenaufruf-System wurde mit dem Ziel entwickelt, den Umgang mit personenbezogenen Daten auf das absolut notwendige Minimum zu beschränken. Im Folgenden eine Übersicht der relevanten Aspekte für den Betrieb in einer Arztpraxis.

5.1 Welche Daten werden verarbeitet?

Im laufenden Betrieb werden Patientennamen temporär im Arbeitsspeicher gehalten und auf dem Ausgabebildschirm angezeigt. Eine dauerhafte Speicherung von Namen findet nicht statt.

Datum	Speicherort / Dauer
Patientenname (Aufruf)	Nur im RAM, max. 15 Minuten, danach automatisch gelöscht
Uhrzeit des Aufrufs	In anonymisierter Statistik (nur Stunde, kein Name)
Genutzter Raum	In anonymisierter Statistik
Geräte-IDs (ID1, ID2)	Lokal auf dem Gerät, nur für Lizenzprüfung
Name + E-Mail (Lizenzantrag)	RSA-verschlüsselt übertragen, nur bei xJRx98 Software gespeichert

5.2 Auftragsverarbeitung

Beim Betrieb des Systems in einer Arztpraxis werden Patientennamen (wenn auch nur kurzzeitig) verarbeitet. xJRx98 Software hat keinen Zugriff auf diese Daten – weder direkt noch indirekt. Die Verarbeitung findet ausschließlich auf den Geräten der Praxis statt. Dennoch empfehlen wir, die Nutzung im Rahmen Ihres Datenschutzkonzepts zu dokumentieren.

> *xJRx98 Software verarbeitet im Betrieb des Systems keine personenbezogenen Daten Ihrer Patienten. Eine Auftragsverarbeitungsvereinbarung (AVV) ist daher in der Regel nicht erforderlich – wir empfehlen jedoch, dies mit Ihrem Datenschutzbeauftragten abzustimmen.*

5.3 Empfehlungen für den sicheren Betrieb

- Stellen Sie sicher, dass der Ausgabebildschirm nur im Wartezimmer sichtbar ist und nicht von der Straße oder öffentlichen Bereichen eingesehen werden kann.
- Ändern Sie das Standard-Admin-Passwort ("admin") nach der Ersteinrichtung.
- Speichern Sie die Lizenzdatei und Statistikdateien nicht auf freigegebenen Netzlaufwerken ohne Zugriffsbeschränkung.
- Löschen Sie bei Geräteaustausch oder Ausscheiden des Geräts die Statistikdateien unter Dokumente/Patientenaufruf/Statistik/ gemäß Ihrer Löschkonzeptdokumentation.
- Erteilen Sie nur berechtigtem Personal Zugang zum Admin-Bereich.

6 Statistik und Datenexport

6.1 Aufbau der Statistik

Der Server erfasst zu jedem Aufruf die Stunde (z. B. 09, 10) und den Raum. Patientennamen werden nicht gespeichert. Die Daten werden als hierarchische XML-Struktur organisiert: pro Tag werden Aufrufe pro Stunde sowie die Auslastung je Raum und Stunde festgehalten.

6.2 Export-Auslöser

Die Statistikdaten werden zu folgenden Zeitpunkten aus dem Arbeitsspeicher in die verschlüsselte XML-Datei geschrieben:

- Täglich automatisch um 23:59 Uhr
- Beim geordneten Beenden von Ausgabe.exe
- Wenn der letzte Client die Verbindung trennt
- Auf Anfrage im Admin-Bereich (manuell)

Nach dem Export werden die Statistikdaten aus dem RAM gelöscht. Beim nächsten Export derselben Zeitperiode werden vorhandene Dateien nicht überschrieben, sondern zusammengeführt.

6.3 Dateistruktur

Die exportierten Dateien werden unter folgendem Pfad gespeichert:

```
Windows: C:\Users\[Benutzername]\Documents\Patientenaufruf\Statistik\
```

Dateiname: [frühestes-Datum].xml.enc (z. B. 2026-03-01.xml.enc)

> ⚠ *Löschen Sie die .xml.enc-Dateien nicht. Sie sind verschlüsselt und können nur mit dem Programm Aufruf.exe entschlüsselt und angezeigt werden.*

7 Konfigurationsdateien und Datenspeicherorte

7.1 Übersicht

Alle Konfigurationsdaten werden lokal auf den Geräten gespeichert. Es gibt keine Cloud-Synchronisation und keinen zentralen Server.

Datei / Ordner	Inhalt und Speicherort
config.json	Aufruf.exe: gespeicherte Server-IP, Räume-Liste. Speicherort: AppData\Local\Patientenaufruf\
lizenz.lic	Lizenzdatei mit Geräte-IDs, Gültigkeitsdaten, Kundendaten, TLS-Zertifikat. Speicherort: AppData\Local\Patientenaufruf\
server_config.json	Ausgabe.exe: Admin-Passwort-Hash, Anzeigedauer. Speicherort: AppData\Local\Patientenaufruf\
server.crt / server.key	TLS-Zertifikat und privater Schlüssel (nur Ausgabe-PC). Speicherort: neben Ausgabe.exe oder eingebettet in der EXE.
[datum].xml.enc	Verschlüsselte Statistikdateien. Speicherort: Dokumente\Patientenaufruf\Statistik\

7.2 Konfiguration der Server-IP

Die IP-Adresse des Ausgabe-PCs wird in der config.json des jeweiligen Aufruf-PCs gespeichert. Bei Änderung (z. B. nach Neustart des Ausgabe-PCs) muss die neue IP in den Einstellungen eingetragen werden. Eine feste IP-Adresse für den Ausgabe-PC (DHCP-Reservierung im Router oder statische IP direkt am Gerät) ist empfehlenswert, um diesen Schritt zu vermeiden.

8 Systemvoraussetzungen und Installation

8.1 Systemvoraussetzungen

	Ausgabe.exe (Server)	Aufruf.exe (Client)
Betriebssystem	Windows 10 / 11 (64-bit)	Windows 10 / 11 (64-bit)
Netzwerk	LAN oder WLAN, feste IP empfohlen	LAN oder WLAN, Zugriff auf Ausgabe-PC
Port	TCP 8765 eingehend (Firewall)	TCP 8765 ausgehend
Bildschirm	1080p oder größer empfohlen (Vollbild)	Beliebige Auflösung
Ton	Optional: Soundausgabe für Benachrichtigungston	—

8.2 Firewall-Hinweis

Beim ersten Start fragt Windows möglicherweise, ob Ausgabe.exe Netzwerkzugriff erhalten darf. Dieser Zugriff muss für das lokale Netzwerk (privates Netzwerk) erlaubt werden. Ohne diese Freigabe können Aufruf-Instanzen keine Verbindung aufbauen.

> *Empfohlene Firewall-Regel: Eingehende TCP-Verbindung auf Port 8765, nur aus dem lokalen Subnetz (z. B. 192.168.0.0/16). Fragen Sie im Zweifelsfall Ihre IT.*

8.3 Mehrere Aufruf-Instanzen

Es können beliebig viele Aufruf.exe-Instanzen gleichzeitig betrieben werden – z. B. eine pro Behandlungszimmer. Alle Instanzen verbinden sich mit derselben Ausgabe.exe. Der Aufrufverlauf der letzten 5 Aufrufe ist für alle Instanzen sichtbar und wird bei jeder neuen Verbindung automatisch übertragen.

9 Fehlerbehandlung und Diagnose

9.1 Häufige technische Probleme

Problem	Ursache / Lösung
Aufruf-Button grau	Keine WebSocket-Verbindung. Ausgabe.exe prüfen, IP-Adresse in den Einstellungen kontrollieren.
Roter Status-Punkt	Verbindung getrennt. Aufruf.exe versucht alle 10 Sekunden erneut. Alternativ: Einstellungen > Verbinden.
Name erscheint verzögert	Mindestabstand von 5 Sekunden zwischen zwei Aufrufen (serverseitig). Normal und gewollt.
Lizenz wird als ungültig abgewiesen	Lizenz ist an ein anderes Gerät gebunden oder Hardware wurde getauscht. Kontakt: info@xjrx98software.de
Statistik kann nicht exportiert werden	Admin-Passwort nicht gesetzt oder server_config.json fehlt. Im Admin-Bereich Passwort setzen.
TLS-Warnung in der Konsole	server.crt oder server.key fehlen neben Ausgabe.exe. Verbindung läuft unverschlüsselt.

10 Support & Kontakt

Bei technischen Fragen, Lizenzproblemen oder Anpassungswünschen stehe ich Ihnen gerne zur Verfügung.

Kontaktweg	Details
E-Mail (allgemein)	info@xjrx98software.de
E-Mail (Lizenzen)	info@xjrx98software.de – Betreff: Lizenz + Kundennamen
Website	www.xjrx98software.de

© 2026 xJRx98 Software · Jonas Ruhland · München · Alle Rechte vorbehalten.