EMIL® Plattform Factsheet zu Architektur, Technik und Datenschutz

Das Wichtigste vorweg – wo liegen die Daten?

Die Daten werden im Rechenzentrum des Betreibers, also der jeweiligen Klinik bzw. Praxis gespeichert. Ein Zugriff von außen ist nicht erforderlich und ist so wie so in der Regel über Firewalls abgesichert. Dies ist aus Datenschutzgründen die optimale Lösung, um die Datenschutzregeln des Betreibers umzusetzen und meist auch eine Grundvoraussetzung für die Herstellung von Schnittstellen zu Kliniksystemen, Labors und Praxiscomputersystemen.

Architektur

Das System ist ein Client-Server-System, die Daten liegen ausschließlich auf dem Server und die Arbeitsplätze haben nur verschlüsselt per HTTPS Zugriff auf den Server.

Das System ist bewusst keine Web-Anwendung, sondern als Windows Rich Client ausgelegt. Gründe dafür sind unter anderem Restriktionen der Web-Technik und die immer noch hohe Vielfalt an Browserumgebungen, was die Realisierung komplexer und systemnaher Funktionen wie z.B. eine Scanneranbindung erschwert bzw. sogar verhindern kann.

Das System arbeitet serverseitig mit einem Applikationsserver, in den ein wartungs- und lizenzkostenfreier angepasster Firebird SQL Datenbankserver gekapselt eingebunden ist. Eine Verwendung anderer Datenbankplattformen ist nicht möglich, da sehr viel Businesslogik in der Datenbank verankert ist. Dokumente und Bilder werden zur Entlastung der Datenbank in Dateiform gespeichert aber ebenfalls nur durch den Applikationsserver über HTTPS ausgeliefert, sodass kein filebasierter Zugriff auf den Server erforderlich ist.

Technik und Betriebsumgebungen

Ein Serverbetrieb in virtualisierter Umgebung ist problemlos möglich, Systemvoraussetzung für die Serverseite ist ein 64 Bit Betriebssystem (Windows, Linux). 8 GB Ram und 250 GB Plattenplatz sind für den Start ausreichend. Der Plattenplatzbedarf wird im Wesentlichen von der Menge Dokumente, Scans und Bilder bestimmt, die in der Plus-Version angelegt werden können. Clients können sowohl nativ auf PCs installiert als auch von einer Share geladen werden. Sie erfordern keine zusätzlichen Laufzeitumgebungen (kein .NET, kein Java, keine Datenbanktreiber oder Ähnliches) auf dem Clientrechner und installieren auch keine Dateien außerhalb des Clientordners.

Mit dem Zusatzprodukt Crossover können die Clients im nahezu kompletten Funktionsumfang auch auf Linux und OSX ausgeführt werden.Ein Betrieb über Terminalserver bzw. Citrix ist auch möglich, erfordert aber unter Umständen zusätzliche Maßnahmen bei der Aktualisierung (siehe kommender Punkt).

Aktualisierung

Die Aktualisierung des Systems erfolgt auf Grund der Frequenz inhaltlicher Änderungen, KV Stammdaten und Anforderungen mindestens quartalsweise. Dabei können Server und Clients über ein sehr komfortables System quasi auf Knopfdruck im laufenden Betrieb aktualisiert werden. Dieses System wird seit 20 Jahren von ITC Kunden sehr geschätzt, da besonders im klinischen Umfeld auf Grund der Arbeitszeiten das Finden entsprechender Freiräume für Betriebsunterbrechung eine große Herausforderung sein kann.

Diese Technik lädt ein Aktualisierungspaket – wahlweise online vom ITC Server oder aus Datei – und führt damit automatisiert zunächst ein Update des Servers durch: Dieser erzeugt eine Kopie der laufenden Instanz (ohne Daten), aktualisiert diese und schaltet dann auf diese um. Da Client und Server asynchron arbeiten, merken die Anwender von diesem Wechsel nichts. Die Clients können nahtlos weiterarbeiten und erhalten neue Features auf Clientseite beim nächsten Start der Software, da der Client sich automatisch beim Start selbst aktualisiert.

Dieser Prozess kann in Umgebungen, in denen z.B. mit festen Softwarepaketen gearbeitet wird, teilweise nicht komplett zum Einsatz kommen, so dass dort möglicherweise andere Aktualisierungsprocederes etabliert werden müssen. Dies ist dann im Einzelfall mit der jeweiligen IT Abteilung zu besprechen und zu konzipieren.

Datensicherheit, Benutzerverwaltung und verschlüsselte Kommunikation

ITC hat sich für die verschlüsselte HTTPS Kommunikation zwischen Client und Server entschieden, um auch in internen Klinik- und Praxisnetzen maximale Datensicherheit zu gewährleisten. Ein filebasierter Zugriff auf den Server des Systems ist für Clients nicht erforderlich. Die Low-Level Authentifizierung auf Netzwerkebene erfolgt über den Industriestandard JsonWebToken.

Für den Zugriff über den Client ist eine Benutzeranmeldung erforderlich, es gibt ein rollenbasiertes Berechtigungssystem mit einer feinkörnigen Rechtevergabe. Eine Abbildung über Active-Directory ist nicht auf Grund der komplexen Rechtestruktur, die in der Plus-Version bis auf Einzelfeldebene herunter reicht, nicht möglich. Eine LDAP Authentifizierung ist für 2021 geplant.

Schnittstellen

Die Plattform verfügt über eine Vielzahl Schnittstellen, darunter serverseitig HL7/HCM für Administrative und Befunddaten sowie MDM für die Rückgabe von PDF Befunden für das Klinikumfeld, server- bzw. clientseitig GDT/BDT/LDT für das Praxisumfeld. Im Bereich der Rheumatologie können die gängigen Tablet-Questionaire-Systeme angebunden werden.

Weitergabe exportierter Daten

Daten, die im Rahmen von Studien oder Versorgungsverträgen weitergegeben werden (z.B. DMPs oder Rheuma Kerndokumentation), werden mit public Key Verfahren (KVCrypt oder GPG) im System vor der Weitergabe verschlüsselt, wobei das System natürlich nur über den öffentlichen Schlüssel des Empfängers verfügt.