Smart Remote Services

Ihre intelligente Verbindung zu digitalen Services

siemens-healthineers.ch/srs

SIEMENS
Healthineers

Inhalt

„Durch den über die Fernwartungsinfrastruktur SRS geleisteten Support erhalten wir schnelle Unterstützung bei Problemen und klare Antworten auf unsere Fragen [...]. Die mit der Fernwartung betrauten syngo-Experten (Remote-Support-Techniker) haben Fernzugriff auf unseren Server und arbeiten ausgesprochen effizient. Bei jedem Anliegen können Sie direkt auf unsere Workstations zugreifen und die Bedienung übernehmen, um uns Schritt-für-Schritt-Anweisungen zu geben. So fühlen wir uns niemals uns selbst überlassen."

Nullam Jeremy Brächet
MRT-Techniker, IRM Lyon Nord, Lyon, Frankreich.

Smart Remote Services (SRS)

Ihre intelligente Verbindung zu digitalen Services

Hohe Systemverfügbarkeit, sichere Diagnosen und Effizienz im klinischen Alltag sind Grundvoraussetzung, um Ihren Leistungsanforderungen gerecht zu werden. Gleichzeitig ist es von höchster Wichtigkeit, zum Schutz Ihrer Systeme und Patientendaten dafür zu sorgen, dass Ihre Geräte auf dem neuesten Stand der Technik bleiben. Angesichts dieser Anforderungen verfolgen wir konsequent ein Ziel: Sie proaktiv zu unterstützen, um langfristig Ihren Erfolg zu sichern. Smart Remote Services (SRS) ist ein schnelles, sicheres und leistungsstarkes Datenübertragungssystem, das Ihre medizinischen Systeme mit unseren Expert*innen verbindet, die Sie mit proaktiven und interaktiven Services in Ihrem Arbeitsalltag unterstützen und Abläufe spürbar beschleunigen.
Durch die SRS-Anbindung haben Sie Zugang zu unseren umfassenden Remote Services und können:

- **Ihre diagnostische Genauigkeit und klinischen Ergebnisse verbessern**
  dank kontextspezifischer Interaktion und schneller Echtzeit-Applikationsunterstützung per Fernzugriff
- **Leistung und Funktionen Ihrer Geräte optimieren**
  dank regelmässiger Remote-Software-Updates, die Ihr System problemlos auf den neuesten Stand bringen
- **Ihre Systemverfügbarkeit erhöhen**
  dank Echtzeit-Fernüberwachung und proaktiver Planung von Wartungseingriffen

Dieses Sicherheitskonzept beschreibt, welche Massnahmen Siemens Healthineers zur sicheren Übertragung von Gerätedaten und zum Schutz von Patientendaten bei der Erbringung von Smart Remote Services an Ihren medizinischen Geräten im Rahmen der technischen Unterstützung und klinischen Anwendung ergreift. Das Konzept findet bei sämtlichen Produkten Anwendung, für die Smart Remote Services angeboten werden.

Um medizintechnische Geräte und Softwaresysteme sicher aus der Ferne überwachen zu können, setzt Siemens Healthineers als einer der ersten Hersteller in der Medizintechnik ein international anerkanntes Informationssicherheits-Managementsystem ein. Dieses System wurde in Deutschland vom TÜV Süd nach der international gültigen Norm ISO/IEC 27001:2022 zertifiziert.
Das Zertifikat ISO/IEC 27001:2022 mit der zugehörigen Erklärung zur Anwendbarkeit (Liste der Kontrollen) ist für alle Kunden gültig und allen Kunden zugänglich, mit Ausnahme der Kunden aus der VR China. Für China liegt eine unabhängige Zertifizierung gemäss CPCS Level 3 vor.

1 Sicherheitsmassnahmen für unseren Remote-Service-Prozess

Smart Remote Services ist unser Gateway, über das wir aus der Ferne auf Ihre Supportanfragen für reaktive und interaktive Dienstleistungen reagieren (technische Fernunterstützung und Remote-Anwendungssupport) und Ihnen datengestützte proaktive Dienstleistungen bieten. Aufgrund der durch Smart Remote Services gebotenen Service-Vielfalt verfolgen wir verschiedene Ansätze zum Schutz Ihres Unternehmens, wenn diese Services von Mitarbeitenden von Siemens Healthineers oder von autorisierten Geschäftspartnern erbracht werden.

a Technische Fernunterstützung

Bei der Behandlung von Vorfällen folgen wir einem Dreistufenansatz, der Smart Remote Services als direkten Kanal nutzt, um aus der Ferne Fehler zu beheben und Experten-Support für unsere Produkte zu bieten.

Unsere Servicemitarbeitenden im Customer Care Center reagieren auf Ihre Supportanfrage und sorgen per Fernzugriff auf Ihr System für eine frühzeitige Fehleranalyse und -behebung. Darüber hinaus leisten unsere Remote Services-Spezialist*innen per Fernzugriff Second-Level-Support und für IT-Systeme, wie PACS oder fortschrittliche Nachverarbeitungssysteme, auch First-Level-Support.

Bei unseren mit der Applikationssoftware *syngo*®[1] ausgestatteten Produkten werden die Patient*innen daten vor ihrer Übertragung in das mit der Fehlerbehebung betraute Customer Care Center ausgeblendet. Bei den jüngsten Software-Versionen[2] kann zudem festgelegt werden, welche Anwender*innen auf welche Daten des Geräts Zugriff haben sollen (siehe Abschnitt 2). Die Entscheidung, ob Sie einem einem Service Engineer oder Ihren eigenen Mitarbeitenden Zugang zu den Daten gewähren, liegt somit in Ihren Händen.

Für nicht mit *syngo* ausgestattete Produkte gibt es keinen technisch implementierten Kontrollmechanismus für den Datenzugriff. In diesen Fällen nehmen wir zur Gewährleistung von Datensicherheit und Datenschutz unsere organisatorischen Massnahmen und unsere SRS-Infrastruktur zu Hilfe (siehe Abschnitt 4).

b Remote-Applikationsunterstützung

Bei Fragen zu Applikationen können unsere Applikationsspezialist*innen des Customer Care Centers bzw. Remote Services Centers Ihre Mitarbeitenden via SRS unterstützen, indem sie aus der Ferne das Display Ihrer Systeme einsehen und die Anwender per Desktop-Management-Software anleiten.

Hierzu müssen Sie zunächst den Fernzugriff explizit freigeben. Zudem können Sie während der Online-Support-Sitzung den Zugriff beliebig verfolgen und zu jedem Zeitpunkt beenden.

Die meisten In-vitro-Produkte bieten eine zusätzliche Sicherheitsstufe: Wird eine Remotesitzung erkannt, so werden alle geschützten Gesundheitsinformationen (PHI) verborgen, um das Risiko zu verringern, dass solche PHI ausserhalb Ihrer Einrichtung sichtbar werden könnten. Weitere Einzelheiten sind dem Security White Paper für das jeweilige medizinische Gerät zu entnehmen.

c Proaktives Monitoring

Einige proaktive Services erfordern, dass Ihr Gerät regelmässig einen vordefinierten Datensatz an unser Remote Service Center sendet. Hierbei handelt es sich um Systemlogs, statistische Daten und Systemzuverlässigkeits-daten, wie die Anzahl der durchgeführten Scans und Restarts.

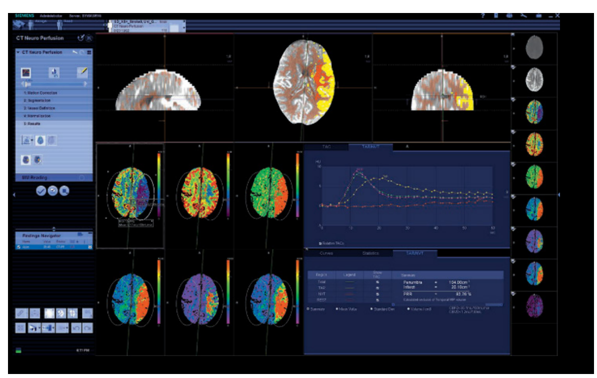


Abbildung 1: Benutzeroberfläche von *syngo* mit anonymisierten Patientendaten

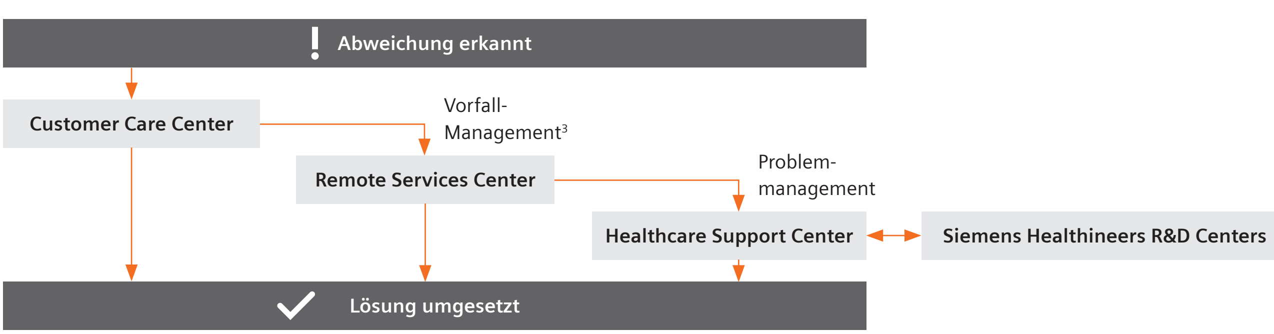


Abb. 2: Siemens Healthineers Eskalationsprozess zur Bearbeitung von Service-Calls

[1] *syngo® ist ein eingetragenes Warenzeichen der Siemens Healthineers AG*

[2] *Informationen bezüglich der auf Ihrem Gerät installierten Software-Version erhalten Sie von Ihrem Siemens Healthineers Ansprechpartner*

[3] *Je nach Produktreihe wird das Vorfall-Management direkt von unserem Remote Services Center übernommen*

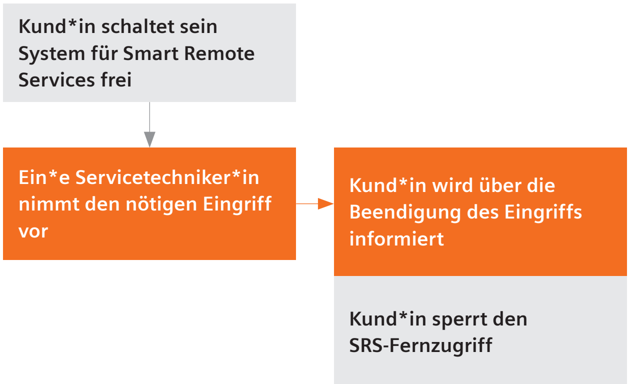
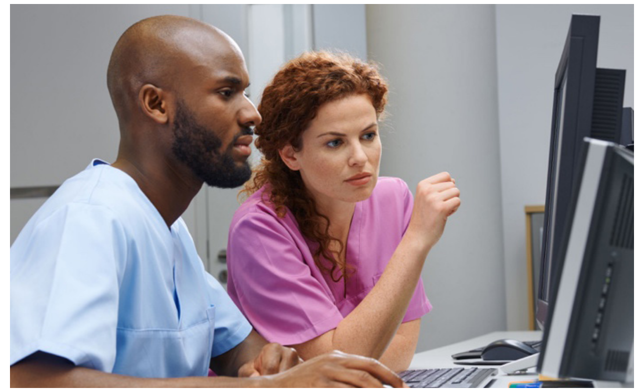


Abb. 3: Ablauf eines SRS-Eingriffs im Modus "kein Zugang"



2 SRS-Sicherheitsmassnahmen für unsere Applikationssoftware

a SRS-Sicherheitsmassnahmen für Applikationssoftware

Unsere mit der Applikationssoftware[4] *syngo* ausgestatteten Produkte können zum Schutz Ihrer Daten während des gesamten Ferneingriffs nachstehende Funktionen nutzen.

Sitzungssteuerung
Sie bestimmen, welche Zugriffsebene einem System, auf dem unsere *syngo*-Applikationssoftware läuft, gewährt wird. Jede Applikationsunterstützungssitzung erfordert ein einmaliges Sitzungspasswort. Mit diesem erteilen Sie unseren Spezialist*innen von Fall zu Fall das Zugriffsrecht auf Ihren Bildschirm. Sobald das Problem behoben ist, endet die Verbindung. Der Zugriff auf Ihre Systeme ohne Ihre ausdrückliche Zugriffsberechtigung ist nicht möglich.

Beim Aufbau einer Fernverbindung haben Sie die Wahl zwischen vier Zugriffsarten:

- **Kein Zugang**
  Bei dieser Einstellung gewähren Sie nur für den jeweiligen genehmigten Eingriff den Zugriff auf Ihr System. Untersuchungen von Patient*innen mit dem System sind weiterhin möglich.
- **Begrenzter / eingeschränkter Zugang**
  Der autorisierte Service Engineer hat für einen vordefinierten Zeitraum begrenzten Zugriff auf einen Teil der Servicefunktionen ohne Beeinträchtigung der laufenden Untersuchungen.
- **Permanenter begrenzter Zugang**
  Der autorisierte Service Engineer hat Zugriff auf einen Teil der Servicefunktionen ohne Beeinträchtigung der laufenden Untersuchungen. Dieser Zugriff ist nicht zeitlich begrenzt.
- **Uneingeschränkter Zugang**
  In diesem Modus haben unsere Service Engineers uneingeschränkten Zugang zu Ihren Servicefunktionen. Während der Durchführung von Remote Services sind keine Untersuchungen von Patient*innen möglich.

Durch die Wahl einer Zugriffsart legen Sie fest, in welchem Umfang und wie lange Sie uns Servicezugriff auf Ihr System gewähren. Sie haben jederzeit die Kontrolle über die Sitzung, indem Sie beliebig Zugriffsrechte gewähren bzw. unterbinden.

Die meisten unserer Kund*innen entscheiden sich für den permanenten begrenzten Zugang. Natürlich haben Sie jederzeit die Möglichkeit, den Zugriff zu ändern. Abb. 3 zeigt den Ablauf im Modus "kein Zugang".

Hinweis: Die oben beschriebene Sitzungssteuerung ist nicht auf serverbasierte IT-Systeme, wie PACS oder fortschrittliche Nachverarbeitungssysteme, anwendbar. Der Fernzugriff auf solche Systeme erfordert keine direkte Interaktion mit den Endanwender*innen, da diese Systeme nicht zwingend einen bestimmten Arbeitsplatz beanspruchen.

[4] *Umfasst i.d.R. unsere diagnostischen Bildgebungsmodalitäten und schliesst serverbasierte Systeme wie syngo.via und syngo.plaza aus*

Zugriffskontrolle
Voraussetzung für jeden Fernwartungseingriff ist, dass Sie zuvor ausdrücklich den SRS-Zugriff auf Ihr System gewährt haben[5]. Einstellungen von Messparametern sind nur im Rahmen der Applikationsunterstützung und mit der von Ihnen erteilten Zugriffsberechtigung möglich. Nach Ablauf einer festgelegten Leerlaufzeit wird die SRS-Sitzung Ihres Systems automatisch beendet.

Passwortgeschützter Zugriff
Nach genehmigtem Zugriff auf Ihr System muss sich der*die Service Engineer bzw. Applikationsspezialist*in zunächst mit einem zeitabhängigen Passwort authentifizieren, bevor er*sie sich auf dem System einwählen kann.

Für IT-Systeme, die unter Ihrer IT-Domain erreichbar sind, können die System-Passwortrichtlinien und Sicherheitsmassnahmen Ihrer Umgebung angepasst werden, solange sie nicht die Funktionstüchtigkeit des Systems beeinträchtigen.

Vier-Augen-Prinzip
Während jeder Remote-Sitzung zeigt Ihr Systembildschirm (in der rechten unteren Ecke) an, dass momentan Remote-Serviceleistungen erbracht werden. Zeitgleich erläutern unsere Service Engineers bzw. Applikationsspezialist*innen in einem Telefonanruf, welche Massnahmen durchgeführt werden. Wenn Sie entscheiden, die Sitzung zu beenden, werden umgehend alle laufenden Service-Programme kontrolliert geschlossen, ohne den weiteren sicheren Betrieb des Systems zu gefährden.

E-Mail-Benachrichtigung bei Fernverbindungen
Auf Ihren Wunsch können wir einen E-Mail-Service einrichten, der die Verbindungsdetails jeder Fernverbindung zu einer E-Mail-Adresse Ihrer Wahl bereitstellt. Diese E-Mail kann nach jeder Sitzung durch eine zweite Benachrichtigung mit weiteren Angaben zu den vorgenommenen Eingriffen ergänzt werden. Versendet werden diese E-Mails nicht von den medizinischen Systemen selbst, sondern von der DMZ des SRS-Servers (siehe Kapitel 4).

b SRS-Sicherheitsmassnahmen für unsere Labordiagnostik-Systeme und Software

Unsere Labordiagnostikgeräte sind durch die folgenden drei Elemente für die Fernüberwachung und den Support durch Smart Remote Services geeignet:

- Proprietäres Softwareprotokoll auf dem Gerät zur Erleichterung der Kommunikation mit dem Atellica Connectivity Manager (ACM)
- Der ACM stellt über eine sichere, verschlüsselte Internetverbindung (IBC) eine Verbindung zur Smart Remote Services Infrastruktur her. Informationen zur IBC finden Sie in Abschnitt 3 des vorliegenden Dokuments unter "Sicherheitsmassnahmen bzgl. der Internet-Based Connectivity".

[5] *Die beschriebene Funktionalität ist auf serverbasierten Systemen, wie syngo.via Server oder und syngo.plaza Server, nicht verfügbar.*

- Smart Remote Services bietet die fortlaufende Fernüberwachung der angebundenen Siemens Healthineers Geräte und bei Bedarf auch Desktop-Fernunterstützung.

Zugriffskontrolle
Der Fernzugriff ist auf autorisierte Servicemitarbeitende beschränkt und erfordert entsprechende Authentifizierungsdaten.

Sowohl auf dem System als auch auf dem ACM sind Service-Benutzerkonten vorhanden, die zur Verwaltung der Funktionen des Produkts unbedingt erforderlich sind. Bei aufkommenden Problemen sind die autorisierten Service Engineers ggf. gehalten, auf den Desktop des Geräts zuzugreifen. Die Service Engineers loggen sich zur Fernunterstützung in die Smart Remote Services Infrastruktur ein und fordern für das Gerät bzw. Produkt eine Online-Verbindung an. Sämtliche Interaktionen zwischen den Service Engineers und den angebundenen Geräten der Kliniken und Labore erfolgen über die SRS-Anwendung und werden vom ACM verwaltet, der verhindert, dass Ihre Geräte direkt mit dem externen Netzwerk in Berührung kommen. Alle Anwender- und Systeminteraktionen von Siemens Healthineers werden für Auditzwecke aufgezeichnet.

Sitzungskontrolle
Sie können den Umfang des für den*die Remote-Anwender*in verfügbaren Zugriffs über die grafische Benutzeroberfläche des ACM definieren. Die grafische Benutzeroberfläche von ACM bietet dann diese Kontrollmöglichkeiten für alle angeschlossenen Geräte. Sie haben uneingeschränkte Kontrolle über Datei-Uploads, Downloads sowie den Fernzugriff auf den Desktop zu Ihren Geräten. Sie haben das Recht, den Zugang zu Fernzugriffssitzungen, Software-Updates und Anwendungen zu gewähren bzw. zu verweigern.

Bei Computerproblemen können Sie nur von autorisierten Service Engineers eine Fernzugriffssitzung anfordern. Es gibt zusätzliche Service-Benutzerkonten, die zur effektiven Verwaltung der Funktionen des Produkts unbedingt erforderlich sind. Diese dürfen nicht entfernt oder verändert werden.

SRS-Remote-Desktop-Sitzungen werden ad hoc initiiert und stehen in der Regel im Zusammenhang mit der Untersuchung von Geräteproblemen. Die in der SRS-Anwendung eingeloggten autorisierten Service Engineers können den Fernzugriff auf ein Gerät oder auf ACM anfordern. Die am Gerät eingegangene Anfrage muss vom Kunden vor ihrem Verfall, sprich innerhalb von 30 Sekunden akzeptiert werden. Wird der Zugriff gewährt, sind alle Fernwartungsaktivitäten auf dem Monitor des Geräts einsehbar. Die Smart Remote Services Infrastruktur zeichnet die Fernverbindungen und Dateiübertragungen auf. In jedem Fall muss Ihr lokaler User die Sitzung per Fernzugriff auf den Desktop akzeptieren, damit der Remotebenutzer fortfahren kann.

Netzwerk-Steuerung
SRS unterstützt:

- die statische IP-Adressierung und DHCP-Zuweisung
- NTLM-Authentifizierung bei Verwendung eines ISA-Servers als Proxy-Kommunikationskanal über Standard- und Authentifizierungs-Proxyserver, je nach Bedarf

Datenübertragung
Die gesamte Kommunikation zwischen der Smart Remote Services-Infrastruktur und dem lokalen ACM ist standardmässig verschlüsselt. Die Kommunikation zwischen dem lokalen ACM und den Geräten kann bei einigen Geräten verschlüsselt werden. Spezifische Einzelheiten entnehmen Sie bitte dem Security White Paper Ihres medizinischen Geräts von Siemens Healthineers.

Die Fernüberwachung erfolgt durch die Übertragung von Daten vom Gerät an die Smart Remote Services Infrastruktur über den ACM. Je nach Gerät und betroffenem Datensatz kann die Übertragung an die Smart Remote Services Infrastruktur entweder durch das Gerät selbst oder durch das in der SRS-Anwendung angemeldete Servicepersonal initiiert werden.

3 Sicherheitsmassnahmen für Daten auf dem Übermittlungsweg

Für den sicheren Datentransport zwischen Ihrer Umgebung und der Smart Remote Services Infrastruktur verwenden wir eine gesicherte und verschlüsselte Verbindung. Wenn Sie darüber hinaus den gesamten Netzwerkverkehr durch Ihre eigene Firewall leiten, sichern Sie sich die volle Kontrolle über Ihre Kommunikation.

Die In-vitro-Medizingeräte bieten Internet-Based Connectivity (IBC) Technologie, um eine virtuelle private Verbindung (VPN) herzustellen. Die In-vivo-Medizingeräte unterstützen zusätzlich zu IBC die Verbindungs-technologien IPSec und WebSocket/TLS zum Aufbau der VPN-Verbindung.

Je nach dem jeweiligen Medizingerät können die genutzten Dienste lokal oder in der cloudbasierten Implementierung von SRS genutzt werden.

a Sicherheitsmassnahmen für IPSec-Verbindungen

Unsere Smarte Remote Services nutzen für die Verbindung beider Umgebungen eine hochmoderne IPSec-Lösung.

Falls Sie keinen VPN-Endpunkt haben, kann Ihnen Siemens Healthineers ein VPN-Endpunkt-Gerät zur Nutzung von Smart Remote Service zur Verfügung stellen. Wir überwachen regelmässig Sicherheitshinweise und aktualisieren die Software dieser VPN-Endpunkte bei Bedarf per Fernzugriff. In unserer Konfigurations-management-Datenbank verfolgen wir alle Konfigurationsänderungen und aktualisieren entsprechend die Geräte.

Sollten Sie bereits eine eigene Lösung haben, können unsere Techniker*innen Sie unterstützen, die notwendigen Parameter für die Verbindung zu implementieren. Diese Parameter sind anschliessend gegen unbefugte Änderungen zu sichern.

Zum Schutz der Verbindung haben wir eine Reihe von Sicherheitsmassnahmen ergriffen:

- **Zugriffsregelung über Access Control Lists**
Access Control Lists (ACLs) auf Ihrem Service-Router funktionieren ähnlich wie Firewalls: Sie erlauben Datenverkehr nur von und zu bekannten IP-Adressen. Der Datenverkehr in Richtung System erfolgt dank "Reverse-Proxy"-Funktionalität in der DMZ (siehe Abschnitt 4). Zudem verhindern ACLs jeglichen Zugriff von Siemens Healthineers auf andere Teile Ihres Netzwerks sowie den Zugriff durch unbefugte Dritte.

- **IP Security Protocol suite**
Um Netzwerk-Sniffing und Datenmanipulation zu verhindern, setzt Siemens Healthineers zur verschlüsselten und authentifizierten Datenübertragung das Protokoll IP Security (IPSec) mit Pre-shared Secret Keys ein, die aus einer beliebigen Zeichenkette mit zufälligen Zeichen bestehen. Zum Austausch der Schlüsselinformationen dient das Internet Security Association and Key Management Protocol (ISAKMP). Aufgrund der Abwärtskompatibilität mit einigen älteren Verbindungsprotokollen müssen wir in Absprache mit einigen Kund*innen weiterhin Parameter wie SHA1, MD5 und 3DES unterstützen. Gemeinsam mit unseren Kund*innen, die solche Verbindungsprotokolle nutzen, arbeiten wir daran, dass diese ihre Parameter auf die neu empfohlenen Parameter umstellen.

Für neue Verbindungen empfehlen wir die folgenden Mindestkonfigurationsparameter:

Authentifizierung/Integrität	SHA-256
Verschlüsselung	AES-256/AES-GCM-256
Key Exchange	DH-Gruppe-16 (4096 Bit)

Um den Datenschutz zu verbessern und gleichzeitig die Datenintegrität zu schützen, unterstützen wir auch höhere Verschlüsselungsstufen, z. B. die Authentifizierungs-methoden SHA-384 oder SHA-512, Diffie-Hellman-Gruppen (19-256 Bit EC, 20-384 Bit EC, 21 -521 BIT EC, 24-2048/256 BIT) zur Key Exchange Sicherheit.

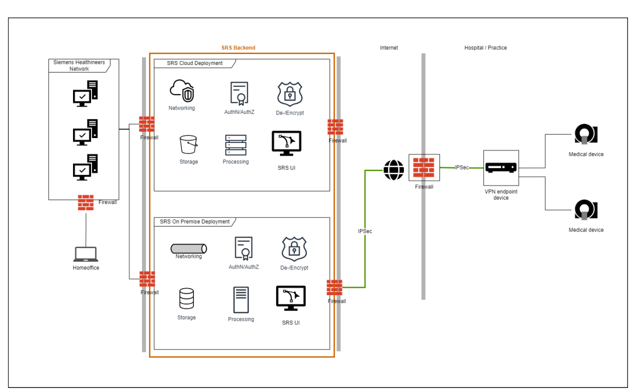


Abb. 4: IPSec-Verbindung

b Sicherheitsmassnahmen bzgl. der Internet-Based Connectivity

Das SRS Sicherheitskonzept basiert auf Internet-Based Connectivity (IBC), welche die TLS-Technologie (Transport Layer Security) nutzt. Es werden ausgehende HTTPS-Anfragen auf Port 443 verwendet. Bei dieser Technologie wird für die Datenübertragung zwischen dem System und der SRS DMZ im Netzwerk ein privater, sicherer, verschlüsselter "Datentunnel" eingerichtet. Auf diese Weise werden Ihre Daten geschützt und das Risiko gesenkt, dass diese während einer SRS-Verbindung durch unautorisierte Dritte mit Viren infiziert werden.

Internet-basierende Verbindungen über TLS haben sich in der Branche sehr schnell als ausgesprochen nützliche und wirtschaftliche Lösung für den Fernzugriff durchgesetzt. IBC ermöglicht über das Internet die Anbindung Ihrer Medizinprodukte bzw. des ACM an die Smart Remote Services Infrastruktur – ohne zusätzliche Anforderungen an die Hardware oder das Netzwerk. Daraus ergibt sich eine grössere Systemmobilität ohne signifikante Kompromisse in Sachen SRS-Konnektivität und Datensicherheit.

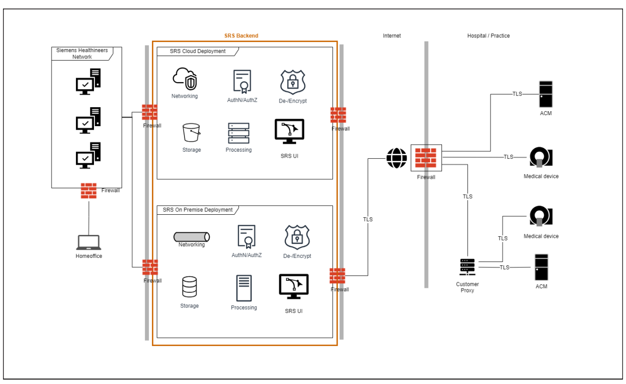


Abb. 5: IBC-Verbindung

c Sicherheitsmassnahmen für WebSocket-Verbindungen

WebSocket ist eine von SRS neu eingeführte Verbindungstechnologie, die IBC in Zukunft schrittweise ersetzen wird. Diese Technologie bietet einen Vollduplex-Kommunikationskanal über eine einzige TCP-Verbindung mit Port 443. Wie bei IPSec und IBC bietet WebSocket einen gesicherten, verschlüsselten bidirektionalen Kommunikationskanal zwischen dem medizinischen Gerät und der SRS-DMZ, wo der Client (auf dem medizinischen Gerät) die erste Verbindung mit der Smart Remote Services-Infrastruktur herstellt.

Verbindungsoptionen für Websocket/TLS-Verbindungen

1. **Direkte Verbindung über Internetzugang des*der Kund*in**
   Medizinische Geräte verbinden sich direkt über den Internetzugang des*der Kund*in mit dedizierten SRS-Endpunkten.
2. **Zentralisierte Verbindung über Kundenproxy**
   Medizinische Geräte verbinden sich direkt über den Kundenproxy mit dedizierten SRS-Endpunkten.
3. **Zentralisierte Verbindung über IPSec VPN-Endpunkt**
   Medizinische Geräte verbinden sich direkt über den von IPSec VPN-Endpunkt mit dedizierten SRS-Endpunkten.

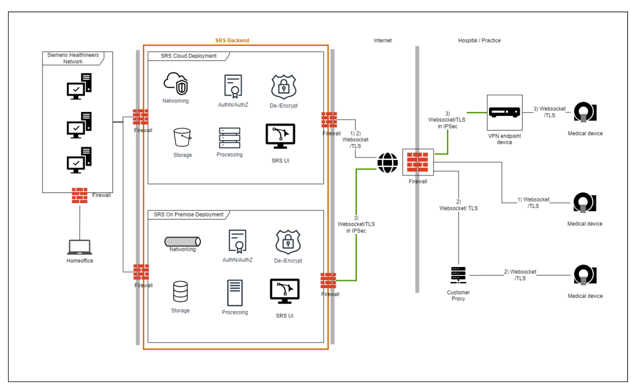


Abb. 6: WebSocket-Verbindung

d Datenübertragung von Ihren Systemen zur Smart Remote Services Infrastruktur

Der Datenaustausch über die SRS-Verbindung wird durch zwei verschiedene Mechanismen ausgelöst. Hinweis: Eine pauschale Messung des übertragenen Datenvolumens ist nicht möglich, da es in hohem Masse vom Produkt selbst und dessen Lebenszyklusphase bestimmt wird.

Benutzerinitiierte Datenübertragung
Der autorisierte Service Engineer ruft die Daten per Fernzugriff aus dem System ab ("Pull-Verfahren") oder plant einen "Daten-Push", um ein bestimmtes Problem auf dem System zu lösen.

Der Datenabruf (Pull) erfolgt immer dann, wenn unsere Servicemitarbeitenden zunächst versuchen, ein gemeldetes Problem anhand der auf dem medizinischen Gerät gespeicherten Log-Daten zu beheben. Ist dies nicht möglich und wird weitere fachkundige Unterstützung benötigt, kann der Service Engineer eine Datenübertragung an das SRS Backend veranlassen. Diese Daten stehen somit den Spezialisten des Customer Services zur Verfügung. Gewisse Störfälle machen es ggf. erforderlich, neben technischen Daten auch PHI/PII-Daten abzufragen (wie z. B. Körpergrösse und Gewicht der zu untersuchenden Person für MRT-Untersuchungen). Diese Daten werden ausschliesslich zur Lösung des jeweiligen Problems herangezogen und verwendet. Die Service Engineers werden im Umgang mit möglicherweise personenbezogenen, direkt oder indirekt identifizierbaren PHI/PII-Daten regelmässig geschult und an die Datenschutzmassnahmen erinnert.

Systeminitiierte Datenübertragung
Automatische "Push"-Datenübertragungen werden zu regelmässigen, vordefinierten Zeitpunkten eingeleitet. Bei In-vivo-Geräten werden Dateien für eine begrenzte Anzahl von Systemen per E-Mail vom System an das SRS Backend gesendet.
Bei In-vitro-Geräten erfolgt die Übertragung über ein proprietäres Protokoll. Weitere Einzelheiten zu den übermittelten technischen Daten und deren Verwendungszweck ergeben sich aus den jeweiligen Geschäftsbedingungen und Datenschutz-Vereinbarungen für Fernverbindungen, die im Vorfeld abzustimmen sind.

Zentraler Weiterleitungsdienst
Verschiedene Zusatzdienste der Geräte erfordern den Zugriff auf Ressourcen im Intranet von Siemens Healthineers bzw. im Internet. Der erforderliche Zugriff wird über einen Weiterleitungsdienst im SRS Backend realisiert.

Die Ressourcen, auf die bestimmte Geräte zugreifen dürfen, werden im SRS Backend sorgfältig überprüft und überwacht. Der Zugriff ist beispielsweise erforderlich, um die Updatefähigkeit von Mobilgeräten, die zusammen mit dem Medizingerät ausgeliefert werden, auf sichere Weise zu ermöglichen oder um die Taste "Fast Contact" zu aktivieren, ohne dass das Medizingerät einen direkten Internetzugang benötigt.

4 Sicherheitsmassnahmen für unsere Smart Remote Services Infrastruktur

Unsere Smart Remote Services machen sich den sicheren Betrieb unserer SRS-Verbindung und die "demilitarisierte Zone" (SRS DMZ (siehe Kapitel 4c)) zwischen dem Siemens Healthineers Intranet und dem Internet zunutze. Durch nachstehende Massnahmen sorgen wir für Datenschutz und Datensicherheit in unserer Smart Remote Services Infrastruktur.

a Authentifizierung und Zugriffsberechtigung

Die Zugriffskontrolle für die Smart Remote Services Infrastruktur erfolgt durch eine Zwei-Faktor-Authentifizierung für Single Sign-On. Der erste Faktor ist eine Kombination aus PKI und Benutzername/Passwort und der zweite ist ein Einmalpasswort (OTP) über eine mobile App/SMS oder E-Mail.

Dank der Granularität unseres Authentifizierungskonzepts sind wir in der Lage zu bestimmen, welche Anwender*innen auf welche Systeme zugreifen dürfen ("Need-to-Know" Basis). Das bedeutet in der Praxis, dass Service Engineers nur dann direkten Zugang zu solchen Systemen haben, wenn sie zu Supportzwecken auf ein System zugreifen müssen und nicht ausdrücklich davon abgehalten werden. Zudem dürfen sie nur zuvor genehmigte Funktionen ausführen.

b Protokollierung

Jeder direkte Fernzugriff auf Ihr System wird bei uns lückenlos auf der Smart Remote Services Infrastruktur mit Zeitstempel aufgezeichnet, wobei dem*der zuständigen Service Engineer bzw. Applikationsspezialist*in eine eindeutige Benutzerkennung zugewiesen wird. Diese Daten werden bis zu sechs Jahre aufbewahrt, es sei denn, die geltenden Gesetze und Vorschriften schreiben eine andere Aufbewahrungsfrist vor, und der Zugang zu den Informationen kann, soweit verfügbar, auf Anfrage gewährt werden.

c SRS Demilitarisierte Zone

Zwischen Ihrem Netzwerk und dem Intranet von Siemens Healthineers haben wir eine SRS-demilitarisierte Zone (SRS DMZ) eingerichtet, um eine direkte Konnektivität zwischen beiden Umgebungen zu verhindern.
Es gibt mehrere SRS DMZ Standorte an verschiedenen Orten der Welt, die eine zuverlässige Verbindung gewährleisten und gleichzeitig die Latenz der Fernkommunikation reduzieren. Der Zugriff auf Ihre medizinischen Geräte ist nur autorisierten Benutzer*innen über die SRS DMZ gestattet, und alle Sitzungen werden zu Prüfzwecken nachverfolgt.
Mit dieser Architektur wird bezweckt, das Risiko eines unbefugten Netzwerkzugriffs über einen Reverse-Proxy-Server zu senken und so jegliche Malware-Übertragung zwischen unseren Netzwerken zu unterbinden.

d Geschützte Smart Remote Services Infrastruktur

Smart Remote Services betreibt eine On-Premise- oder eine cloudbasierte Infrastruktur nach den Leitlinien für Informationssicherheit von Siemens Healthineers. Die Wirksamkeit der Schutzmassnahmen wird regelmässig überprüft, damit die Smart Remote Services Infrastruktur mit stets aktueller Technologie betrieben werden kann.

e Organisatorische Massnahmen

Um medizintechnische Geräte und Softwaresysteme sicher aus der Ferne überwachen zu können, setzt Siemens Healthineers als einer der ersten Hersteller in der Medizintechnik ein Informationssicherheits-Managementsystem ein. Dieses wurde in Deutschland vom TÜV Süd nach der international gültigen Norm ISO/EC 27001:2022, 3. Auflage, zertifiziert.

Darüber hinaus betreibt Siemens Healthineers ein Datenschutz-Informationsmanagementsystem auf der Grundlage der Norm ISO/IEC 27701:2019.

Unsere Service Engineers und Applikationsspezialist*innen sind umfassend im Umgang mit personenbezogenen Daten geschult und dem Datenschutz und der Datensicherheit verpflichtet. Siemens Healthineers führt eine elektronische Aufzeichnung der zugelassenen Service Engineers und ihrer entsprechenden Zugriffsrechte.

Weitere Einzelheiten zu Themen im Zusammenhang mit dem Datenschutz finden Sie im Smart Remote Services Data Privacy White Paper.

5 Schutz vor böswilligen Angriffen

Alle Massnahmen dieses Sicherheitskonzepts bezwecken, einen ganzheitlichen, lückenlosen Schutz für Ihre Systeme und Ihre Umgebung zu erzielen und vor allem das Risiko nachstehender Bedrohungen zu minimieren.

a Malware-Infektionen

Die kontinuierliche Überwachung und Wartung des SRS Backends trägt dazu bei, dass die Verbindung zwischen Ihren medizinischen Geräten und dem SRS Backend geschützt ist. Solange der Internetzugang nur für SRS-Zwecke genutzt wird und das Produkt gemäss dem zugehörigen Security White Paper bedient wird, ist ein Virenbefall unwahrscheinlich.

b Bösartiger E-Mail-Verkehr

Bestimmte In-vivo-Medizingeräte senden E-Mails an die Smart Remote Services Infrastruktur. Diese E-Mails werden von Ihrem System in Richtung unserer SRS DMZ verschickt.

Von Ihrem System an die SRS DMZ gesendete E-Mails werden an den zuständigen Siemens Healthineers Mail-Server weitergeleitet und von dort aus an den*die Empfänger*in geschickt. Dies können E-Mail-Adressen von Siemens Healthineers, E-Mail-Adressen Ihrer eigenen IT-Abteilung oder interne E-Mail-Adressen sein. Die Weiterleitung von E-Mails an die Empfängeradresse ist erst gestattet, wenn diese zuvor auf eine Whitelist gesetzt wurde. Es werden keine E-Mails von der SRS DMZ an das medizinische Gerät geschickt.

In-vitro-Medizingeräte senden keine E-Mails an unsere SRS DMZ.

c Systemübergreifende Infektionen

Infektionen zwischen dem Arbeitsplatz des Service Engineers und Ihrem System sind unwahrscheinlich, da keine Möglichkeit zum direkten IP-Routing zwischen beiden Systemen besteht (siehe Reverse-Proxy-Server in Abschnitt 3).

6 Weitere unterstützende Massnahmen für Ihre Systeme

Trotz unserer intensiven Bemühungen um Cybersicherheit sind wir für den sicheren Betrieb Ihrer Systeme aufgrund der Beschaffenheit unserer verschiedenen Produkte mitunter auf Ihre Mitwirkung angewiesen. All unsere Geräte und reinen Softwareprodukte werden mit einem Security White Paper bzw. Manufacturer Disclosure Statement for Medical Product Security (MDS2) herausgegeben. In diesen Dokumenten finden Sie weitere Angaben zu den auf den medizinischen Geräten implementierten Sicherheitsmassnahmen sowie Hinweise zur Einrichtung der IT-Infrastruktur für eine sichere Betriebsumgebung unter Beachtung strenger Sicherheitsrichtlinien auf allen IT-Ebenen. Auf diese Weise verfügen alle Netzwerkgeräte, Betriebssysteme, Applikationssoftware , Büro- und klinische IT-Geräte über eigene angemessene Sicherheitsmassnahmen um Schwachstellen zu erkennen, die möglicherweise in anderen IT-Elementen übersehen wurden.

Bitte wenden Sie sich an Ihren Kontakt bei Siemens Healthineers Customer Services, um das Security White Paper Ihres Medizinprodukts von Siemens Healthineers zu erhalten.

Darüber hinaus nutzen wir SRS als Kanal, um bei Bedarf Sicherheitspatches von Drittanbietern möglichst rasch bereitzustellen. Deshalb wird, sofern nicht anders angegeben, dringend empfohlen, die SRS-Anbindung für Fälle beizubehalten, in denen neue Sicherheitslücken bekannt werden, die Ihre medizinischen Geräte betreffen.

Die (hier genannten) Produkte/Funktionen und/oder Service-Angebote sind nicht in allen Ländern und/oder für alle Modalitäten kommerziell verfügbar.

Wenn die betreffenden Serviceleistungen in bestimmten Ländern aus zulassungsrechtlichen oder anderen Gründen nicht vermarktet werden, kann das Leistungsangebot nicht garantiert werden.

Wenden Sie sich an Ihre örtliche Siemens Healthineers Organisation, um weitere Informationen zu erhalten (und technische Voraussetzungen zu erfahren, die für bestimmte Serviceangebote gelten).

Voraussetzungen:
Stabile SRS-Verbindung mit ausreichender Bandbreite

Eine Anbindung an die SRS-Infrastruktur (Smart Remote Services Infrastruktur) ist erforderlich. SRS verfügt über fortschrittliche Sicherheitsmassnahmen und entspricht der Norm ISO 27001:2022 für Informationssicherheit.

Siemens Healthineers International AG
Freilagerstrasse 40
8047 Zürich Schweiz
Tel.: +41 581 99 11 11
customercarecenter.ch@siemens-healthineers.com
siemens-healthineers.ch