Smart Remote Service

Concept de sécurité 10.0

Votre connexion intelligente aux services digitaux

SIEMENS Healthineers

Contenu

" Le support que nous recevons par le biais de SRS nous permet d'avoir une réponse rapide et personnalisée à nos questions ou problèmes [...]. En ayant un accès à distance à notre serveur, les ingénieurs support syngo (Remote Support Engineers) sont vraiment efficaces, et peuvent accéder à nos postes de travail, prendre le contrôle, pour nous guider pas à pas, à chaque demande que nous avons, afin que nous ne nous sentions jamais abandonnés."

Jeremy Brachet
Technicien IRM, IRM Lyon Nord, Lyon, France.

Smart Remote Service (SRS)

Votre connexion sécurisée pour accompagner la digitalisation des soins de santé

Une disponibilité de haute qualité, une confiance dans le diagnostic et les opérations en cours sont essentielles pour répondre à vos exigences de performance. Dans le même temps, le maintien des équipements à la pointe de la technologie figure en tête des priorités pour protéger les équipements et les données des patients. Compte tenu de ces besoins, nous nous efforçons systématiquement d'être proactifs pour vous maintenir sur la voie du succès. Smart Remote Services (SRS) est une liaison rapide, sécurisée et puissante qui connecte votre équipement médical à nos experts, lesquels vous fournissent des services proactifs et interactifs qui vous aident dans votre routine quotidienne et accélèrent vos opérations courantes. La connexion SRS vous donne accès à notre vaste gamme de services à distance, qui vous permettent de :

- **Optimiser les résultats diagnostiques et cliniques** - grâce à une interaction adaptée au contexte et à un support immédiat des applications à distance.
- **Améliorer les performances et les fonctionnalités** - grâce à des mises à jour logicielles régulières à distance permettant à votre système d'être constamment à jour.
- **Maximiser le temps de fonctionnement du système** - grâce à la surveillance à distance en temps réel du système et à la programmation proactive des événements de service.

Ce concept de sécurité décrit les mesures que nous avons prises, chez Siemens Healthineers, pour protéger les données des patients lors des prestations de services utilisant le SRS, tant dans le domaine de l'assistance technique que dans celui des applications cliniques, sur nos dispositifs médicaux. Il est utilisé en conjonction avec tous les produits pour lesquels le SRS est proposé.

1. Mesures de sécurité dans notre processus de prestation de services à distance

Smart Remote Services est notre canal de réponse réactive et interactive (support technique et d'application à distance à vos demandes d'assistance) et permet de vous fournir des services proactifs basés sur des données concrètes. En raison de la nature différente des services que nous fournissons par le biais de Smart Remote Services, nous suivons différentes approches pour protéger vos données, et que ces services soient fournis par nos employés Siemens Healthineers ou par des partenaires autorisés.

a. Assistance technique à distance

Notre processus de traitement des incidents suit une approche d'escalade en trois étapes dans laquelle nous utilisons les Smart Remote Services comme canal direct pour fournir un dépannage à distance et une assistance spécialisée pour nos produits.

Dans le cadre de ce processus, nos ingénieurs du Centre de support réagiront à votre demande de support et accéderont à votre système à distance pour un diagnostic et un dépannage précoces. En outre, les spécialistes de notre Centre de support à distance peuvent également accéder à distance à votre système pour prendre en charge les problèmes nécessitant un second niveau d'analyse. Pour les systèmes informatiques - comme les PACS ou les systèmes de post-traitement avancés - le premier niveau est assuré par les spécialistes de notre Centre de support à distance.

Nos produits utilisant le logiciel d'application *syngo*®[1] comprennent des mécanismes permettant de masquer toutes les données relatives aux patients avant de les transférer au Centre de support chargé du dépannage à distance.

Les versions les plus récentes du logiciel[2] permettent également de définir quels utilisateurs ont accès à quelles données dans l'appareil (voir section 2). La décision d'accorder l'accès à un ingénieur Service ou à vos propres employés est donc entre vos mains.

Pour les produits ne fonctionnant pas sous *syngo*, un mécanisme de contrôle d'accès aux données n'est pas techniquement implémenté. Dans ces cas, nous nous appuyons sur nos mesures organisationnelles et notre infrastructure informatique (voir section 4) pour protéger vos données.

b. Assistance applicative à distance

Afin d'aider votre personnel clinique à répondre aux questions relatives aux applications, notre Centre de support clients ou nos ingénieurs Application peuvent utiliser les services à distance intelligents pour reproduire l'affichage de vos systèmes et guider l'utilisateur à l'aide d'outils de gestion de bureau à distance.

Nos produits vous demandent explicitement d'accorder cet accès à distance et vous permettent de suivre et d'interrompre l'accès à tout moment au cours de la session d'assistance en ligne.

La plupart des produits In Vitro, offrent une couche de sécurité supplémentaire en masquant les Informations de Santé Protégée (PHI) lorsqu'une session à distance est détectée, afin de réduire le risque que des PHI soient visibles à l'exterieur de votre établissement. Vous trouverez des informations supplémentaires dans le Livre Blanc sur la Sécurité du dispositif médical correspondant.

c. Services de surveillance proactive

Certains services proactifs exigent que votre appareil envoie régulièrement un ensemble prédéfini de données à nos centres de services. Il s'agit notamment de journaux système, de données statistiques et de fiabilité, telles que le nombre d'analyses effectuées et la fréquence de redémarrage du système.

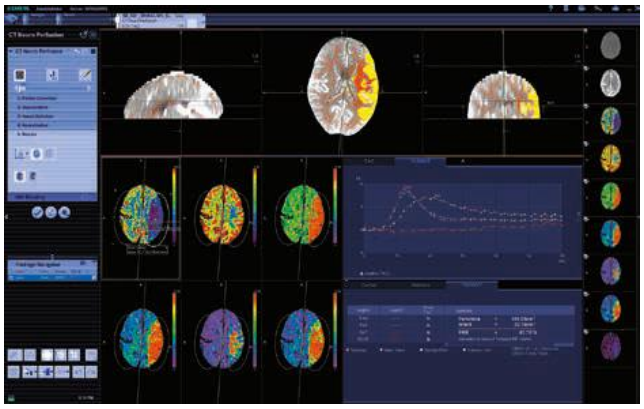


Fig 1 : interface utilisateur *syngo* – mode opératoire d'anonymisation des données patients

[1] *syngo est une marque déposée de Siemens Healthcare GmbH.*

[2] *Les informations concernant la version du logiciel de votre système peuvent être obtenues auprès de votre représentant Siemens Healthineers.*

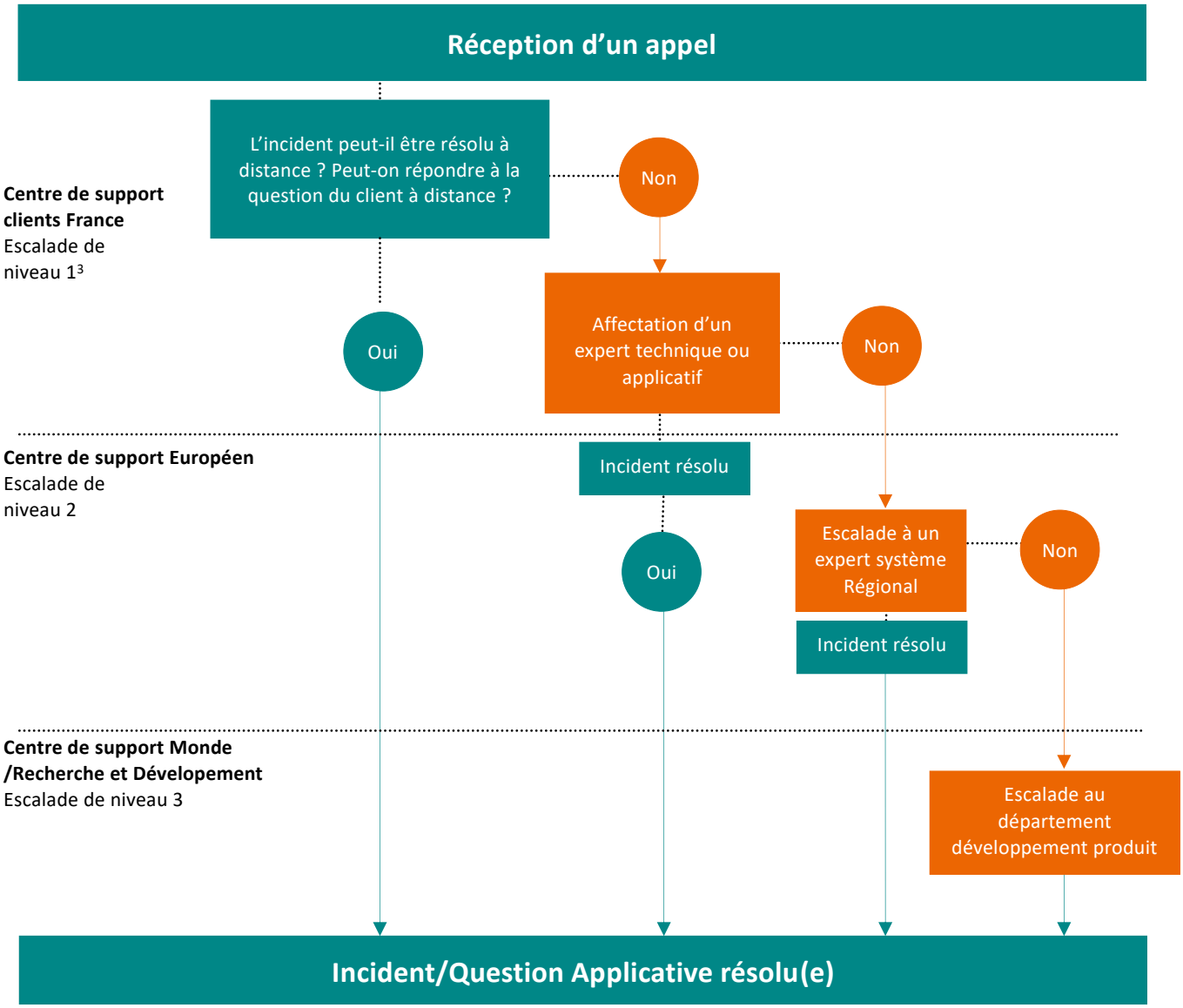


Fig 2 : Processus d'escalade pour le traitement des appels de service

[3] *En fonction de notre gamme de produits, la gestion des incidents peut être assurée directement par notre centre de services à distance.*

2. Mesures de sécurité SRS dans nos logiciels d'application

a. Mesures de sécurité dans notre logiciel d'applications *syngo*

Nos produits utilisant le logiciel d'applications *syngo*[4] peuvent compter sur les fonctionnalités suivantes pour assurer la sécurité des données tout au long de l'interaction à distance.

Contrôle des sessions

Le niveau d'accès accordé à un système exécutant notre logiciel d'applications syngo est entièrement déterminé par le client. Chaque session de support applicatif nécessite un mot de passe de session ad-hoc. Vous pouvez ainsi décider au cas par cas si vous partagez votre écran avec notre expert. Après avoir résolu le problème, la connexion est interrompue. L'accès à vos systèmes sans votre autorisation n'est pas possible.

Lorsque vous établissez une connexion à un service à distance, vous pouvez choisir entre quatre niveaux d'accès :

- **Aucun accès**

Vous fournissez un accès uniquement au cas par cas pour effectuer la tâche approuvée. Les examens des patients utilisant le système peuvent toujours être effectués.

- **Accès limité**

Pendant une période prédéfinie, l'ingénieur de Service Siemens Healthineers autorisé a accès à un sous-ensemble de fonctionnalités du système qui n'interfèrent pas avec les examens en cours.

- **Accès limité permanent**

L'ingénieur de Service autorisé de Siemens Healthineers a accès sans limite de temps à un sous-ensemble de fonctionnalités du système qui n'interfèrent pas avec les examens en cours.

- **Accès complet**

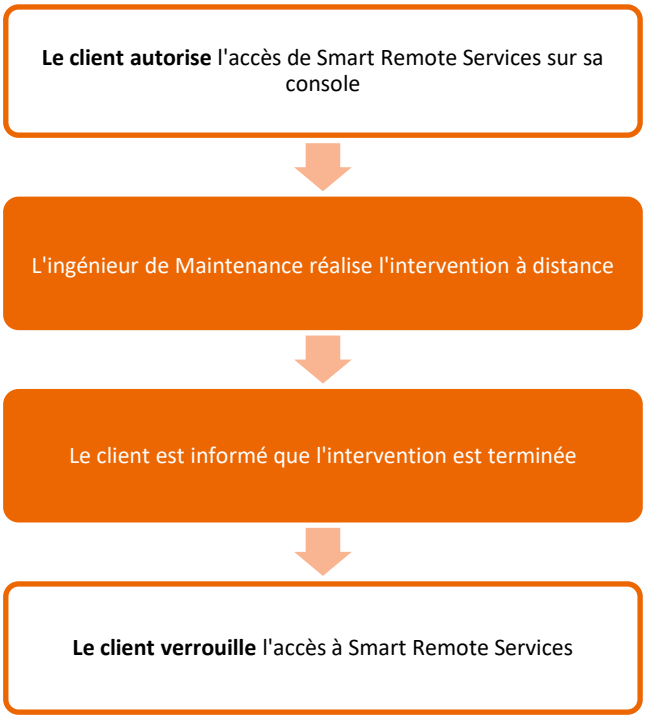
L'ingénieur de service autorisé a un accès complet à votre système. Les examens des patients ne sont pas possibles pendant la réalisation de la mainteance à distance.

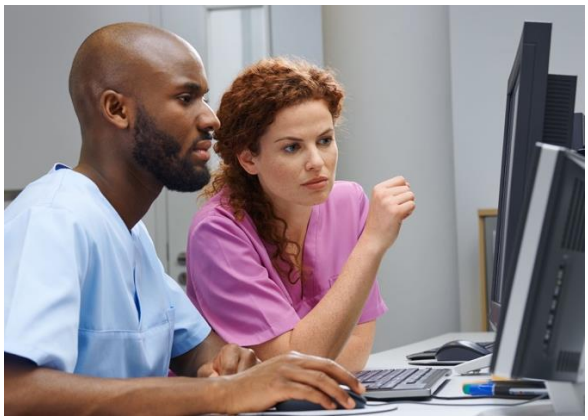
Ces niveaux d'accès déterminent à eux seuls le degré et la durée pour lesquels vous souhaitez accorder l'accès à votre système. À tout moment, vous avez le contrôle de la session pour accorder ou révoquer les droits d'accès.

Si l'accès limité permanent est le niveau d'accès le plus fréquemment choisi, vous pouvez toujours opter pour le niveau sans accès. La figure 3 montre le déroulement d'une tâche de service à distance à ce niveau.

Remarque : le contrôle de session décrit ci-dessus n'est pas applicable aux systèmes informatiques basés sur des serveurs, comme les PACS ou les postes de post-traitement avancés. L'accès à distance pour ces systèmes peut être établi sans interaction directe avec les utilisateurs finaux, car ils n'affectent pas nécessairement un poste de travail dédié.

Fig 3 : Flux des activités d'intervention à distance avec le niveau « Aucun accès »





[4] *Comprend généralement nos modalités d'imagerie diagnostique, et exclut les systèmes basés sur des serveurs tels que syngo.via et syngo.plaza.*

Contrôle des accès

Comme prérequis à toute activité de service, le client doit accorder expressément l'accès à distance à un ingénieur Siemens Healthineers. Le réglage des paramètres de l'installation ou l'accès aux protocoles d'utilisation, ne sont techniquement possibles que lors d'un support applicatif et avec la permission du client. Enfin, par sécurité, toute session distante inactive sera automatiquement interrompue après une durée fixée.

Protection par un mot de passe

Après accord explicite de votre part, l'ingénieur Siemens Healthineers doit s'authentifier sur votre système grâce à un mot de passe temporaire, afin d'être autorisé à passer votre système en mode service.

Pour les systèmes informatiques intégrés dans votre domaine, il est possible d'adapter la politique de mot de passe et les mesures de sécurité à votre environnement, afin de ne pas impacter le fonctionnement de vos systèmes.

Contrôle assuré par le client

Le client reçoit une indication visuelle sur la console principale l'informant que des activités de suivi à distance sont en cours. De plus, l'ingénieur Siemens Healthineers communique avec le client par téléphone et lui explique les actions en cours de réalisation.

Au cours de chaque session distante, l'utilisateur peut mettre fin à tout moment à la connexion, dans ce cas, tous les programmes de maintenance en cours d'exécution sont alors immédiatement fermés de manière contrôlée, sans aucun impact sur la sécurité et la continuité de l'exploitation du système.

Notification de pré-connexion par e-mail

De manière optionnelle, nous pouvons activer sur demande un service de messagerie via le serveur à distance Siemens Healthineers, qui fournira à votre personnel clinique, technique ou informatique tous les détails de connexion avant chaque connexion à distance. Cet e-mail pourra être complété par un second message lors de la déconnexion indiquant la raison de l'intervention. Ces e-mails sont envoyés depuis la zone démilitarisée du SRS et non depuis les systèmes médicaux eux-même.

b. Mesures de sécurité pour nos équipements et logiciels de diagnostic de laboratoire

Nos systèmes Instruments de diagnostic de laboratoire utilisent l'infrastructure SRS dans le cadre de la maintenance et du support à distance. La fonctionnalité SRS repose sur trois éléments :

- Un protocole logiciel propriétaire pour faciliter la communication avec la passerelle SRS Atellica Connectivity Manager (ACM)
- Le logiciel SRS (installé sur la passerelle SRS) initie et maintient une connexion cohérente avec l'infrastructure SRS par le biais de l'adaptateur de réseau virtuel grâce à la connexion Internet du site
- L'infrastructure SRS

La passerelle SRS est connectée à l'infrastructure SRS via une connexion internet supportant les requêtes HTTPS sur le port 443. SRS permet la surveillance permanente des équipements connectés Siemens Healthineers et un partage de bureau à distance à la demande.

Accès au système

L'accès à distance est réservé au personnel Siemens Healthineers ayant les identifiants d'authentification appropriés.

Un compte administrateur est dédié au personnel Siemens Healthineers. Afin d'assurer une gestion efficace des fonctionnalités du produit, des comptes utilisateurs Service supplémentaires sont créés. Lors d'un incident, les équipes Siemens Healthineers peuvent avoir à accéder à la console de l'équipement : ils se connecteront au système d'assistance à distance Entreprise et demanderont une connexion directe au système. Toutes les interactions entre les équipes Siemens Healthineers et les systèmes connectés de l'hôpital ou du laboratoire sont effectuées via l'applications SRS et gérées par les gestionnaires de connectivité Atellica® Connectivity Manager (ACM), ce qui empêche vos appareils d'être directement exposés au réseau exterieur. Toutes les interactions menées pas Siemens Healthineers avec les utilisateurs et le système sont enregistrées et disponibles pour audit.

Contrôle des connexions

Vous pouvez définir les accès attribués aux différents utilisateurs grâce à l'interface graphique de la passerelle SRS (instructions fournies séparément). Vous avez un contrôle total sur l'import et le téléchargement des fichiers ainsi que sur les connexions à vos systèmes. Les opérateurs ont la possibilité d'autoriser ou d'interdire les connexions, les mises à jour logicielles et l'accès aux applications. Dans le cas d'un incident informatique sur l'un de vos PC, vous pouvez demander au personnel Siemens Healthineers de se connecter à distance sur le système. Afin d'assurer une gestion efficace des fonctionnalités du produit, des comptes utilisateurs Service supplémentaires sont créés : ils ne doivent en aucun cas être supprimés ou modifiés.

Les sessions de contrôle à distance SRS sont initiées selon le besoin, généralement pour investiguer des incidents liés aux systèmes.

Le personnel Siemens Healthineers autorisé qui est connecté sur l'application SRS peut demander l'accès à un instrument ou à la passerelle SRS. La demande d'accès doit être validée dans les 30 secondes sinon la demande expire. Si l'accès est validé, toutes les activités effectuées à distance seront visibles sur le moniteur du système. L'infrastructure SRS enregistre les connexions à distance et les transferts de fichiers. Dans tous les cas, l'utilisateur local doit approuver la session de contrôle à distance pour que l'utilisateur à distance puisse continuer.

Contrôle du réseau

SRS prend en charge les éléments suivants :

- Adresse IP statique et affectation DHCP
- Authentification NTLM lors de l'utilisation du serveur ISA comme proxy. Communication via des serveurs proxy standards et d'authentification selon besoin

Transfert de données

Toutes les communications entre l'infrastructure SRS et la passerelle SRS locale (Atellica CM) sont encryptées par conception.

La communication entre la passerelle SRS locale et les instruments peut être chiffrée pour certains instruments. (Pour des détails spécifiques, veuillez vous référer au Livre Blanc sur la Sécurité de votre dispositif médical Siemens Healthineers)

La surveillance à distance est facilitée par le transfert de données de l'instrument à l'infrastucture SRS via la passerelle SRS. Selon l'instrument et l'ensemble de données concernés, le transfert vers l'infrastructure SRS peut être initié soit par l'instrument lui-même, soit par le personnel de service de Siemens Healthineers connecté à l'application SRS.

3. Sécurisation de la transmission des données

Afin d'assurer une transmission sécurisée de vos données vers notre environnement, nous vous proposons différentes techniques de cryptage. De plus, vous avez la possibilité de choisir de faire passer tout le trafic réseau par votre pare-feu, ce qui vous confèrera un contrôle total sur vos communications.

Les dispositifs médicaux In Vitro offrent une technologie de connexion basée sur Internet (IBC) pour créer un Réseau Privé Virtuel (VPN). En plus de l'IBC, les dispositifs médicaux In Vivo offrent également des technologies IPsec et WebSocket/TLS pour créer la connexion VPN.

a. Mesures de sécurité pour la connectivité IPSec

SRS utilise une solution IPsec (Internet Protocol Security) pour connecter deux environnements.

Si vous n'avez pas de point de terminaison VPN, Siemens Healthineers peut vous fournir l'appareil servant de point de terminaison VPN nécessaire pour la connexion SRS. Nous surveillons régulièrement les avis de sécurité et mettons à jour à distance le logiciel de ces points de terminaison VPN, si nécessaire. Nous suivons tous les changements de configuration dans notre base de données de gestion de configuration et mettons, en conséquence, à jour les équipements sur le terrain.

Si vous disposez de votre propre solution, nos techniciens peuvent vous aider à implémenter les paramètres nécessaires à la connexion. Ces paramètres doivent alors être sauvegardés et protégés contre tout changement non autorisé.

Les terminaisons VPN de notre réseau sont des routeurs Cisco®. Pour se prémunir de toute incompatibilité lors de la configuration de la connexion, nous recommandons de contacter votre représentant local Siemens Healthineers. Pour garantir la sécurité, nous mettons à votre disposition les mesures techniques suivantes :

- **Listes des contrôles d'accès**

Les listes de contrôles d'accès (Access Control Lists) du routeur de services proposent une fonction similaire à celle des pare-feux qui n'autorisent que le trafic des données circulant à destination et en provenance des adresses IP connues. Le trafic des données est routé à travers le proxy inversé de la zone démilitarisée vers le système. Ceci permet également d'empêcher Siemens Healthineers ou des tiers d'accéder à d'autres composantes de votre réseau.

- **Protocole IPSec**

Pour s'affranchir des écoutes réseau et de la falsification des données, Siemens Healthineers utilise le standard reconnu IP Security (IPSec) avec des clés pré-partagées pour assurer une transmission de données cryptées et authentifiées.

Les clés pré-partagées consistent en des chaines de caractères aléatoires. Le protocole ISAKMP (Internet Security Association and Key Management Protocol) est employé pour échanger les informations de cryptage des clés. En raison de la compatibilité descendante avec certaines connexions héritées, nous devons encore supporter des paramètres tels que SHA1, MD5 et 3DES en consultation avec certains clients. Néanmoins, nous travaillons diligemment avec eux pour migrer la configuration actuelle vers les paramètres recommandés.

Pour les nouvelles connexions, nous recommandons les paramètres de configuration minimum suivants :

Authentification/intégrité SHA-256

Chiffrement AES-256/AES-GCM-256

Échange de clé DH-groupe-16 (4096 bits)

Pour améliorer la confidentialité des données tout en protégeant l'intégrité des données, nous prenons également en charge des niveaux de chiffrement plus élevés, par exemple, les méthodes d'authentification SHA-384 ou SHA-512, les Groupes Diffie-Hellman (19-256 bits ec, 20-384 bits ec, 21-521 bits ec, 24-2048/256 bits) pour la sécurité de l'échange de clés.

b. Mesures de sécurité pour la connectivité basée sur Internet

Le concept de sécurité SRS repose ici sur la connectivité basée sur Internet (IBC), en utilisant la technologie TLS (Transport Layer Security). Cette technologie fournit un mécanisme de communication sécurisé et privé pour les données et autres transmissions d'informations entre IBC et SRS, en établissant un tunnel réseau direct pour des données cryptées. Cela fournit un support supplémentaire dans la protection de vos données en vous protégeant contre la divulgation de celles-ci et contre les attaques virales introduites par des tiers non autorisés lors d'une connexion SRS.

Le certificat est émis par l'Autorité de Certification privée SRS située dans le backend SRS. Le certificat n'est pas stocké dans le Store de Certificats (c'est-à-dire le Gestionnaire de Certificats), mais plutôt livré et stocké dans un fichier dans le répertoire d'installation du client SSL VPN. Pour plus de détails, veuillez vous référer au Livre Blanc sur la Sécurité du dispositif médical (in vivo) ou de la passerelle ACM (in vitro), ou contactez votre représentant local de Siemens Healthineers.

La connectivité basée sur Internet utilisant TLS a rapidement été reconnue dans toute l'industrie comme étant une solution hautement viable et économique pour l'accès à distance.

L'IBC permet à vos dispositifs médicaux d'être connectés à l'infrastructure SRS sur la base d'une connexion internet sans exigences supplémentaires en matière de matériel ou de réseau, tout en protégeant vos données et en offrant une mobilité système accrue.

c. Mesures de sécurité pour la connectivité WebSocket/TLS

WebSocket est une technologie de connexion récemment introduite par SRS qui remplacera progressivement l'IBC à l'avenir. Cette technologie fournit un canal de communication full duplex via une seule connexion TCP utilisant le port 443. Comme c'est le cas avec IPsec et l'IBC, WebSocket fournit un canal de communication bidirectionnel sécurisé et chiffré entre le dispositif médical et la "zone dématérialisée" (DMZ) SRS, où le client (situé sur le dispositif médical) établit la connexion initiale avec l'infrastructure SRS. Chaque fois que le dispositif médical le permet, WebSocket sera la technologie privilégiée pour connecter vos systèmes à SRS, car elle offre une sécurité renforcée et une amélioration de la prestation de services.

- **Options de connectivité pour la connectivité Websocket/TLS**

1. Connectivité directe via l'accès Internet du client

Le dispositif médical se connecte directement via l'accès Internet du client au cloud dédié au SRS ou aux terminaisons de la DMZ SRS.

2. Connectivité centralisée via un proxy client

Le dispositif médical se connecte directement via le proxy client du client au cloud dédié au SRS ou aux terminaisons de la DMZ SRS.

3. Connectivité centralisée via la terminaison VPN SHS

Le dispositif médical se connecte directement via la terminaison VPN fournie par Siemens Healthineers au cloud dédié au SRS ou aux terminaisons de la DMZ SRS

d. Transmission de données à partir de vos systèmes vers l'infrastructure SRS

L'echange de données via la connexion SRS est déclenchée par deux mécanismes différents. Le volume de données transférées dépend du produit et de son cycle de vie, aucune généralité ne peut être faite à ce sujet.

- **Transmission de données initiée par les utilisateurs**

La transmission des données à partir de vos systèmes est réalisée soit à la demande ponctuelle d'un ingénieur Siemens Healthineers, soit programmée dans le cadre de la résolution d'un problème technique. Les extractions de données sont nécessaires lorsque le personnel de notre Centre de support clients tente de résoudre un incident signalé, en utilisant les données stockées localement sur votre système. Si la résolution du problème nécessite une expertise plus poussée, nos ingénieurs Siemens Healthineers peuvent déclencher un transfert des données vers le Centre de support maison-mère. Les données seront alors accessibles aux spécialistes du Centre de support clients, du Centre d'assistance technique et du Centre de support maison-mère incluant les équiqes R&D. Dans certains cas spécifiques, il pourra être nécessaire d'extraire des données patients (par exemple la taille et le poids du patient pour un examen IRM) en plus des données techniques. Ces données seront récoltées et utilisées dans le seul but de résoudre l'incident. Le personnel Siemens Healthineers est formé à manipuler des données personnelles et des données de santé patients.

- **Transmission de données initée par le système**

Les transferts automatiques de données sont réalisés à horaire fixe prédéfini et à intervalles réguliers. Les données sont transmises par transfert de fichiers pour un nombre limité de systèmes par email à partir des systèmes vers la zone démilitarisée du SRS. Pour les dispositifs In Vitro, les transferts sont effectués à l'aide d'un protocole propriétaire. Les détails techniques des données transmises et de leur utilisation prévue sont décrits dans les Termes et Conditions Générales du SRS qui doivent être acceptés à l'avance.

4. Mesures de sécurité de notre infrastructure SRS

Nos Smart Remote Services sont basés sur la sécurisation des opérations de notre plateforme SRS et la "zone dématérialisée" (DMZ) entre l'intranet Siemens Healthineers et Internet. Les mesures mises en place permettent la protection des données au sein de notre infrastructure SRS.

a. Authentification et autorisation des ingénieurs Siemens Healthineers

Le serveur central d'accès à distance utilisé par le Centre d'assistance technique est accessible exclusivement via l'intranet Siemens et ne peut être accédé hors de ce réseau. L'accès à ce serveur est fortement sécurisé grâce une authentification à deux facteurs par une carte à puce (PKI) et/ou un mot de passe temporaire unique (OTP). La granularité de notre concept d'authentification nous permet de déterminer les utilisateurs autorisés à accéder aux systèmes. Dans la pratique cela veut dire que les ingénieurs Siemens Healthineers ne peuvent accéder qu'aux systèmes des clients pour lesquels ils sont explicitement autorisés et pour ne réaliser que les seules opérations auxquelles ils sont autorisés.

b. Enregistrement des accès à distance

Nous enregistrons chaque accès à votre système via le SRS ainsi que la date et heure des connexions. De plus, chaque ingénieur Siemens Healthineers qui se connecte au système se voit attribuer un identifiant utilisateur unique. Ces informations sont stockées pendant 6 ans, sauf si les réglements et lois en vigueur prévoient une période différente de conservation des informations. Vous pouvez accédez à toutes les informations enregistrées sur demande.

c. « Zone démilitarisée » SRS

Entre votre réseau et l'intranet de Siemens Healthineers, nous avons établi une Zone de Démilitarisée SRS (SRS DMZ) qui empêche toute connectivité directe entre les deux environnements. Il existe plusieurs emplacements SRS DMZ à travers le monde, sur site ou basés sur le cloud, pour fournir une connexion fiable tout en réduisant la latence de la communication à distance en même temps. L'accès à vos équipements médicaux n'est autorisé qu'aux utilisateurs autorisés via la SRS DMZ, et toutes les sessions sont suivies à des fins d'audit. Cette architecture est conçue pour atténuer le risque d'accès réseau non autorisé via un serveur proxy inversé, afin de se protéger contre la transmission de logiciels malveillants entre nos réseaux respectifs.

Vous trouverez ci-dessous le schéma de principe de l'infrastructure de sécurité des services à distance Siemens Healthineers :

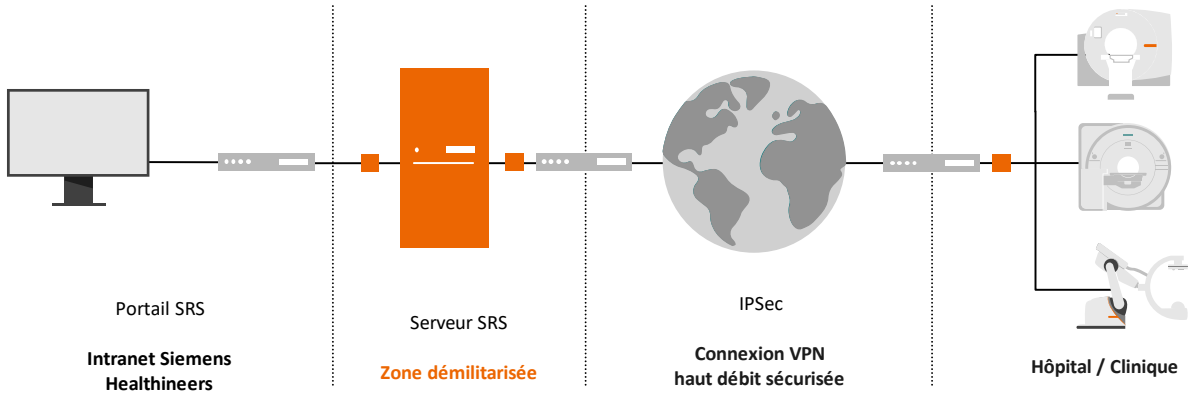


Fig 4 : infrastructure sécurisée SRS

d. Protection de l’infrastructure SRS

SRS est opéré à partir d’une infrastructure interne ou sur le Cloud conformément aux directives de Siemens Healthineers en matière de sécurité de l'information. L'efficacité des mesures de protection est régulièrement vérifiée et l’infrastructure SRS est exploitée avec une technologie de pointe.

e. Mesures organisationnelles

Siemens Healthineers a implémenté un Système de Gestion sécurisé validé au plan international (ISMS) pour l’accès distant aux appareils médicaux. Cela a été certifié par TÜV Süd en Allemagne conformément à la norme internationale DIN EN ISO/IEC 27001, 2e édition. De plus, Siemens Healthineers exploite un Système de Gestion de l'Information sur la Confidentialité basé sur la norme ISO/IEC 27701:2019.

Les ingénieurs Siemens Healthineers sont sensibilisés au respect de la confidentialité et l’intégrité des données des patients. Seuls les ingénieurs Siemens Healthineers qui ont été formés à la confidentialité des données et aux problèmes de sécurité, et qui déclarent leur engagement dans ces domaines, sont habilités à réaliser des opérations de maintenance à distance sur les équipements médicaux.

Vous trouverez plus de détails sur les sujets liés à la confidentialité des données dans le Livre Blanc sur la Confidentialité des Données du SRS.

5. Protection contre les attaques malveillantes

Toutes les mesures décrites dans ce document ont pour but d'offrir une protection globale pour vos systèmes et votre environnement, et notamment de minimiser les risques liés aux menaces ci-dessous.

a. Protection contre les infections par des logiciels malveillants

En connectant votre système au SRS, votre connexion à la DMZ est également sécurisée par une technologie de pointe. Tant que l’accès Internet est uniquement utilisé pour les besoins des services à distance Siemens Healthineers et que l'équipement est utilisé selon les recommandations de son livre blanc relatif à la sécurité, une infection virale est improbable.

b. Aucun risque lors de l’échange d’e-mails

Certains types d’équipements médicaux in vivo envoient des e-mails à l‘infrastructure SRS, uniquement dans ce sens. Les e-mails envoyés à partir d’un de vos systèmes vers le serveur d’accès SRS sont transmis au serveur de courrier électronique de Siemens Healthineers approprié, puis envoyés au destinataire. Il peut s’agir d‘ une adresse Siemens Healthineers ou celle de votre propre service informatique.

Chaque adresse destinataire doit être sur liste blanche avant d'autoriser un envoi d'e-mail. Aucun e-mail n’est envoyé depuis la zone démilitarisée vers l'équipement médical.

Les instruments in-vitro n’envoient aucuns e-mails vers notre DMZ SRS.

c. Infection réciproque

L’infection crossée entre l’ordinateur de l’ingénieur Service et votre système est improbable étant donné qu’il n’y a pas de routage IP direct entre ces systèmes (Voir la fonction de proxy inversé en section 3).

6. Aller plus loin

Malgré notre engagement ferme envers la cybersécurité, la nature de nos différents produits peut nécessiter votre implication pour les exploiter en toute sécurité. Tous nos équipements et produits logiciels sont livrés avec un Livre Blanc sur la Sécurité et/ou une Déclaration de Divulgation du Fabricant pour la Sécurité des Produits Médicaux (MDS2). Dans ces documents, vous trouverez des informations supplémentaires sur les contrôles de sécurité mis en place sur le dispositif médical, ainsi que les facteurs supplémentaires que vous devez prendre en compte lors de la configuration de votre infrastructure informatique, en suivant attentivement le principe de la sécurité avec des politiques de sécurité strictes à tous les niveaux informatiques. Cela signifie que tous les dispositifs réseau, les systèmes d'exploitation, les logiciels d'application, les dispositifs informatiques de bureau et cliniques ont leurs propres contrôles de sécurité adéquats pour se protéger contre les vulnérabilités qui pourraient avoir été négligées dans d'autres éléments informatiques.

Veuillez contacter votre représentant des Services Clients de Siemens Healthineers pour obtenir le Livre Blanc sur la sécurité de votre dispositif médical Siemens Healthineers.

De plus, SRS est notre canal rapide pour fournir des correctifs de sécurité tiers lorsque cela est nécessaire. Par conséquent, sauf indication contraire, il est fortement recommandé de rester activement connecté à SRS dans les situations où de nouvelles vulnérabilités affectant vos dispositifs médicaux sont divulguées.

7. Foire Aux Questions (FAQ)

Le SRS permet-il à Siemens Healthineers d'accéder aux données patients sur le système connecté ?

Il existe 2 cas de figure lors desquels Siemens Healthineers accède au système via SRS :

Lors d'un diagnostic et/ou d'une réparation à distance, les experts techniques Siemens Healthineers ont seulement accès aux données techniques et aux données de maintenance. Si l'accès aux données patients est nécessaire à la résolution du problème, le client en est informé préalablement et doit donner son accord. (Voir section 1.a pour plus d'informations)

Le deuxième scénario possible est l'assistance à distance. Dans ce cas de figure, l'utilisateur doit explicitement donner son consentement à l'ingénieur Siemens Healthineers d'accéder à la vue de son écran, lequel peut contenir des informations sensibles. (Voir section 1.b pour plus d'informations)

Un ingénieur Siemens Healthineers peut-il se connecter à l'un de mes systèmes sans mon accord ?

Un accès permanent peut être activé sur demande dans le logiciel d'applications *syngo*. Le client a la possibilité de révoquer cet accès à tout moment. Vous avez également la possibilité de configurer le SRS afin de valider expressément chaque accès[5]. Des exceptions peuvent s'appliquer.

(Voir section 2.a pour plus d'informations)

Je ne veux pas avoir à approuver chaque accès mais j'aimerais en être informé. Comment faire ?

Nous pouvons activer le service d'e-mail, qui vous permettra d'être notifié des détails de connexion avant et/ou après chaque accès.

Comment l'utilisateur sait-il si une activité de service est en cours ?

Une icône en bas à droite de l'écran vous notifie qu'une session SRS est en cours. L'utilisateur peut terminer une session à tout instant si besoin. Dans ce cas, tous les programmes de service seront immédiatement interrompus.

(Voir section 2.d pour plus d'informations)

Comment vous assurez-vous que seul le personnel Siemens Healthineers et les prestataires mandatés ont accès aux systèmes connectés ?

L'accès à la maintenance à distance et aux fonctions de support de vos systèmes est contrôlé par une authentification à deux facteurs dans notre infrastructure SRS :

a) Identifiant utilisateur SRS, carte à puce et code PIN

b) Identifiant utilisateur SRS, mot de passe et code PIN temporaire unique via SMS ou e-mail

Important : le personnel Siemens Healthineers et les prestataires n'ont accès qu'aux systèmes pour lesquels ils ont une autorisation spécifique. (Voir section 4.a pour plus d'informations)

[5] *La fonctionnalité décrite n'est pas disponible sur les systèmes basés sur des serveurs comme le syngo.via ou le serveur syngo.plaza.*

Comment la connexion entre le serveur SRS et le réseau de l'hôpital est-elle sécurisée ?

Le serveur SRS et le réseau de l'hôpital sont connectés via une connexion VPN sécurisée par le protocole IPSec ou SSL. Pour les systèmes mobiles nécessitant une connexion directe au serveur SRS nous proposons une connexion VPN basée sur TLS.

(Voir section 3 pour plus d'informations)

Je suis inquiet que la connexion au SRS engendre une vulnérabilité dans la cybersécurité du réseau de mon hôpital. Serait-il plus sécurisant de ne pas connecter le système du tout ?

Pour prévenir le risque de cyberattaques sur le réseau de l'hôpital, nous recommandons de suivre les principes de sécurité et d'implémenter des mesures de sécurité strictes à tous les niveaux de l'infrastructure informatique. Tous les appareils réseaux, systèmes opérationnels, logiciels et appareils informatiques cliniques doivent donc avoir leurs propres contrôles de sécurité afin d'assurer une protection optimale.

La solution de sécurité SRS permet de contrôler et limiter l'accès à votre réseau ce qui empêche les attaques venant de notre DMZ de s'infiltrer dans votre environnement. Cependant, cette mesure n'est qu'un complément aux mesures de sécurité que vous mettez en place au sein de votre établissement.

De plus, SRS est notre moyen rapide de livrer les correctifs tiers de sécurité lorsque nécessaire. Autrement dit, sauf indication contraire, il est fortement recommandé de maintenir la connexion SRS dans le cas où votre équipement serait potentiellement la cible de nouvelles vulnérabilités.

8. Conditions générales relatives à la connexion à distance en imagerie & laboratoire

Valables à compter de mai 2021

1. Champ d'application et définitions

1.1 Les présentes Conditions générales relatives à la connexion à distance intègrent les conditions générales en vertu desquelles Siemens Healthineers fournira au Client une Connexion SRS pour l'Équipement. L'ensemble des autres services ou fournitures que le Client peut recevoir est soumis à des conditions générales supplémentaires et n'est pas couvert par les présentes.

1.2 En ce qui concerne l'objet visé à la section 1.1, seuls le Concept de sécurité en vigueur et les présentes Conditions générales relatives à la connexion à distance s'appliqueront. Les Conditions générales du Client ne s'appliqueront que si elles sont expressément acceptées par Siemens Healthineers.

1.3 Définitions
Les termes commençant par une majuscule ont la signification qui leur est donnée à la section 1.3.

1.3.1 Client désigne l'entité qui passe la commande, telle que mentionnée dans le Bon de commande.

1.3.2 Équipement désigne les produitset solutions consistant en du matériel et/ou des logiciels qui est/sont vendu(s), concédé(s) sous licence ou autrement mis à la disposition du Client et qui est/sont défini(s) dans le Bon de commande, qu'il(s) soi(en)t fabriqué(s) par SHS ou non.

1.3.3 Bon de commande désigne le formulaire qui mentionne les détails de la connexion à distance convenue, en particulier concernant l'Équipement connecté.

1.3.4 Concept de sécurité désigne le concept de sécurité informatique de Siemens Healthineers, qui figure sous le lien suivant :
https ://www.healthcare.siemens.com/services/customer-services/rapid-response-services/smart-remote-services.

1.3.5 Siemens Healthineers ou SHS désigne l'entité Siemens Healthineers telle que mentionnée dans le Formulaire de commande.

1.3.6 SHC GmbH désigne Siemens Healthcare GmbH.

1.3.7 Connexion SRS signifie connexion « Smart Remote Services », c'est-à-dire une connexion en ligne entre Siemens Healthineers ou l'une de ses entités affiliées et l'Équipement concerné sur le site du Client.

1.3.8 Données techniques intelligentes désignent les Données techniques corrélées dérivées de l'Équipement pour prendre en charge la prédiction des exigences de service de l'Équipement.

1.3.9 Données techniques désignent les informations disponibles via la Connexion SRS et peuvent inclure :

(i) les fichiers journaux de l'application, les erreurs survenues ; les propriétés du dispositif, le contrôle qualité (informations sur l'état technique) ;
(ii) la configuration, les versions logicielles, correctifs, licences, paramètres réseau ; l'historique des services liés au dispositif (données sur les actifs et la configuration) ;
(iii) les séquences ou performances de diverses tâches, applications/licences utilisées, et interactions avec l'application (données d'utilisation) ;
(iv) les réactifs et consommables chargés sur l'Équipement ;
(v) et toutes autres données explicitement convenues ;

dans chaque cas, sans lien avec une personne physique identifiée ou identifiable.

2. Utilisation de la Connexion SRS

2.1 SHS, SHC GmbH, ses entités affiliées et autres sociétés engagées par SHS ou SHC GmbH sont autorisées à accéder à l'Équipement, entretenir, réparer, calibrer, mettre à jour ou corriger l'Équipement qui fait l'objet du présent Contrat SRS, ou à fournir une formation à distance dans tous les cas via la Connexion SRS et à utiliser toutes les Données techniques recueillies via la connexion SRS aux fins susmentionnées.

2.2 Si un contrat de service est conclu entre le Client et SHS ou si une période de garantie pour l'Équipement fourni par SHS est en cours de validité, alors SHS, SHC GmbH, ses entités affiliées et d'autres sociétés engagées par SHS ou SHC GmbH sont également autorisées à exécuter, via la Connexion SRS, des services supplémentaires de surveillance du système qui sont pris en charge par l'Équipement couvert.

3. Accès aux données et utilisation des données

Sauf accord contraire, le Client autorise irrévocablement SHS, SHC GmbH et ses entités affiliées à utiliser pour leur propre activité, ou à des fins de surveillance des produits, recherche ou développement (par exemple, déterminer les tendances des produits et services d'utilisation, l'amélioration des produits, services et logiciels), pour faciliter et conseiller sur l'utilisation continue et durable des produits et services, la justification de l'ensemble des réclamations marketing concernant les produits/services ainsi qu'à des fins d'analyse comparative, sans restrictions en termes de temps, transférabilité, réplication, localisation ou contenu :

(i) les données techniques conformément à la section 1.3.9 qui sont recueillies via la Connexion SRS ; et
(ii) les données techniques intelligentes conformément à la section 1.3.8 qui sont recueillies via la Connexion SRS à partir de l'Équipement couvert, lors d'une relation commerciale en cours entre les parties.

4. Obligations des parties

4.1 SHS doit mettre en place le processus technique et organisationnel pour la Connexion SRS et l'infrastructure informatique utilisée par SHS pour l'établissement de la connexion SRS conformément au Concept de sécurité.

4.2 SHS peut fournir au Client des informations sur l'état de la Connexion SRS et des informations générales sur la manière de restaurer la connexion au cas où elle ne fonctionnerait pas correctement.

4.3 Le Client devra permettre que la Connexion SRS soit établie en connectant l'Équipement à la liaison de télécommunications sécurisée via une connexion haut débit, à ses propres frais. Le Client devra assumer le coût de toutes les exigences techniques pour toute connexion ne faisant pas partie de l'Équipement, par exemple pour établir une connexion haut débit.

4.4 Afin de protéger l'Équipement contre les cybermenaces, il est nécessaire que le Client mette en œuvre, et maintienne en permanence, un concept de sécurité holistique et conforme à l'état de l'art, protégeant son infrastructure informatique. Le Client devra également apporter un soutien à SHS dans le cadre de la protection contre les cybermenaces. Cela signifie que le Client ne devra pas, en particulier :

4.4.1 connecter l'Équipement à une Connexion SRS qui n'est pas conforme aux politiques de sécurité de pointe ou qui n'est pas à défaut approuvé par SHS ;

4.4.2 utiliser la Connexion SRS d'une manière qui compromet ou perturbe l'intégrité de la Connexion SRS ou de l'infrastructure informatique SHS ; ou

4.4.3 transmettre des données renfermant des virus, chevaux de Troie ou autres programmes susceptibles d'endommager ou d'altérer la Connexion SRS ou l'infrastructure informatique de SHS.

5. Garantie limitée

5.1 Sauf disposition contraire explicite, la Connexion SRS est fournie « en l'état » et SHS ne fournit au Client aucune garantie concernant la disponibilité, performance ou qualité de la Connexion SRS autre que celle indiquée dans la section 4.1.

5.2 SHS ne fournira pas de Connexion SRS :

5.2.1 si la mise à disposition est empêchée par tout obstacle découlant d'exigences nationales ou internationales en matière de commerce extérieur ou de douane, ou par tout embargo ou autres sanctions ; ou

5.2.2 s'il y a un défaut, dysfonctionnement ou autre problème concernant le réseau de télécommunications ; ou

5.2.3 s'il y a un défaut, dysfonctionnement, une configuration insuffisante ou un autre problème en lien avec l'infrastructure du Client.

6. Mise à jour des Conditions et du Concept de sécurité

6.1 SHS est en droit de modifier et/ou mettre à jour les présentes Conditions générales relatives à la connexion à distance et/ou au Concept de sécurité pour refléter les progrès techniques, changements de la législation, et les développements ultérieurs des offres.

6.2 Ces modifications et/ou mises à jour ne doivent pas compromettre la qualité et le fonctionnement de la Connexion SRS.

6.3 SHS devra informer le Client des modifications en lui fournissant un préavis raisonnable de 30 jours au minimum. SHS fournira au Client l'accès aux Conditions générales mises à jour.

7. Certification

7.1 L'organisation de service SHS devra maintenir un système de gestion de la sécurité de l'information certifié aux fins de la Connexion SRS. À cet égard, SHS fera régulièrement l'objet d'audits externes effectués par des tiers indépendants. Le champ d'application et les détails de la certification sont définis dans le Concept de sécurité en vigueur.

8. Suspension et résiliation

8.1 Sauf accord contraire figurant dans des conditions générales prévalant sur les présentes, le présent Contrat SRS peut être résilié par l'une ou l'autre des parties, par écrit, à tout moment, en donnant un préavis de quatre (4) semaines. La validité de tout autre accord entre le Client et SHS ne sera pas affectée par la résiliation du présent Contrat SRS. Si d'autres accords ont été conclus sur la base du présent Contrat SRS, ils sont susceptibles de devoir être adaptés lors de la résiliation, par exemple en ce qui concerne la rémunération ou les délais de réponse.

8.2 Chaque partie sera autorisée à résilier le présent Contrat SRS avec effet immédiat si l'autre partie l'enfreint et si ladite violation n'est pas corrigée pendant une période de 14 jours à compter de la réception de l'avis de violation de l'autre Partie.

8.3 SHS sera en droit de suspendre le présent contrat SRS et/ou la Connexion SRS avec effet immédiat si le Client est en violation du présent contrat SRS ou si SHS est d'avis -en agissant raisonnablement - que la Connexion SRS à un ou plusieurs Équipements du Client comporte un risque pour la sécurité et la performance de l'Infrastructure informatique utilisée par SHS.

8.4 Si le présent Contrat SRS est résilié par l'une ou l'autre partie conformément à la section 8.1 et que les parties se livrent à des négociations pour conclure de nouveaux accords de service ou renouveler les accords de service, les dispositions du présent Contrat SRS survivront à la résiliation pendant huit (8) semaines supplémentaires, à moins que le Client n'informe explicitement SHS que cette survie ne s'applique pas.

9. Propriété intellectuelle

SHS (et ses concédants de licence, le cas échéant) conservera tous les droits de propriété intellectuelle relatifs à l'Équipement, y compris les améliorations y afférentes, toute amélioration dérivée des Données techniques ou des Données techniques intelligentes, ainsi que les suggestions, idées, demandes d'amélioration, commentaires, recommandations ou autres informations fournies par le Client qui sont par les présentes assigné(e)s à SHS.

Les informations de ce document contiennent des descriptions générales qui peuvent ne pas être forcément applicables pour chaque cas spécifique.

Siemens Healthcare SAS se réserve le droit de modifier sans préavis préalable la conception et les spécifications décrites dans ce document.

Veuillez contacter votre représentant Siemens Healthineers local pour obtenir les informations les plus récentes.

Siemens Healthcare SAS
6 rue du Général Audran
92400 Courbevoie

0 820 807 569 Service 0,05 € / min + prix appel

Département Service Clients
Marketing Services
H_DSC_MS_31441_9_138

www.siemens-healthineers.com/fr