Living up to Life

Service et support sécurisés à distance pour systèmes intelligents

La sécurité est l'élément le plus important pour Leica Microsystems et pour les clients utilisant les services à distance. Leica Microsystems a besoin d'une solution de services à distance qui protège contre les virus et les pirates informatiques et qui puisse prendre en charge nos instruments intelligents. Par ailleurs, cette solution ne doit pas entraîner de modifications majeures du système de l'utilisateur final, elle doit nous permettre de travailler avec notre modèle de sécurité réseau actuel et enfin, elle doit obtenir la certification officielle d'une entreprise de sécurité tierce. Étant donné que les instruments Leica Microsystems sont connectés aux réseaux de nos clients, les clients finaux doivent également être sûrs que la solution de services à distance prend en charge leur modèle de sécurité, qu'elle fournit un contrôle granulaire de l'accès utilisateur et qu'elle offre un audit facile d'utilisation et des possibilités de traçage.

Pour le nouveau système de services à distance Leica RemoteCare, Leica Microsystems, comme de nombreux ensembliers, fournit des services à distance essentiels pour les entreprises via l'infrastructure serveur et le logiciel Axeda® ServiceLink™. Axeda ServiceLink permet de régler facilement la question de la sécurité de Leica et de nos clients et contribue de manière proactive à minimiser les temps d'arrêt, à gérer les risques et à assurer que l'équipement est toujours en mesure de fournir des résultats maximaux.

Avec Axeda ServiceLink, le système RemoteCare de Leica Microsystems connecte sans problème les instruments Leica Microsystems aux environnements de nos clients. Parce que ces instruments tracent souvent les dossiers des patients et tout autre type d'informations protégées et à caractère personnel, les possibilités en matière de sécurité et de conformité font partie des exigences les plus importantes évaluées dans toute solution de services à distance. Le présent document examine les *ses* exigences de Leica Microsystems et de ses clients ainsi que la manière dont Axeda ServiceLink y répond dans le cadre des services et supports sécurisés à distance qu'il apporte.

Les exigences de Leica Microsystems en matière de services sécurisés à distance
Leica Microsystems a choisi les produits Axeda pour son système RemoteCare afin de répondre aux exigences de sécurité les plus strictes de Leica Microsystems et des clients de Leica Microsystems pour que ceux-ci puissent utiliser les services à distance efficacement et de manière routinière tout en sachant que leurs connexions sont sûres et qu'elles restent protégées.
Parmi nos exigences les plus communes, certaines comprennent :

- La conception éprouvée par l'entreprise : la connexion d'un ordinateur à Internet implique des questions de sécurité et il en va de même pour la connexion des dispositifs intelligents. Que les pirates informatiques tentent de nuire à un dispositif par le biais de données corrompus ou de virus, de dérober des données circulant entre l'instrument et Leica Microsystems, ou bien d'accéder de manière illégale à des informations sensibles, un système commandé à distance se doit de protéger contre ces menaces-ci et contre d'autres menaces.

- Le support pour dispositifs multiples : Leica Microsystems doit fournir un support sûr aux différents types de dispositifs et aux configurations client complexes sans que cela n'implique de modification majeure pour l'utilisateur final.

- Le déploiement rapide : pour que les clients adoptent les systèmes de services à distance, les possibilités en matière de sécurité doivent exister au sein même du modèle de sécurité réseau du client.

- La validation par une entreprise de sécurité tierce : une certification officielle obtenue suite à un audit de sécurité fournit au client la preuve des capacités de la technologie et du vendeur.

Engagement :
Leica Microsystems estime que la vie privée et la sécurité revêtent une importance capitale pour nos clients. RemoteCare veille au maintien des principes de sécurité suivants :
- Protection de l'intégrité du système (réseau, équipement et données)
- Traçage des accès et activités pour garantir la conformité réglementaire
- Flexibilité et contrôle visant à mettre en place les politiques des entreprises
- Audit et certification régulières des processus et solutions Leica Microsystems par un tiers

Les exigences des clients en matière de services sécurisés à distance
Des instruments intelligents sont connectés aux réseaux de nos clients. Chaque client a sa propre politique de sécurité et son propre dispositif de protection réseau qui prend la forme de pare-feu, de serveurs proxy et de schémas d'adressage. Un dispositif connecté au réseau du client sera protégé par ces barrières de sécurité. Si une offre de services à distance requiert des changements dans le système de protection réseau de notre client, celle-ci ne sera vraisemblablement pas acceptée. De ce fait, il est donc important de tenir compte des exigences du client qui incluent :

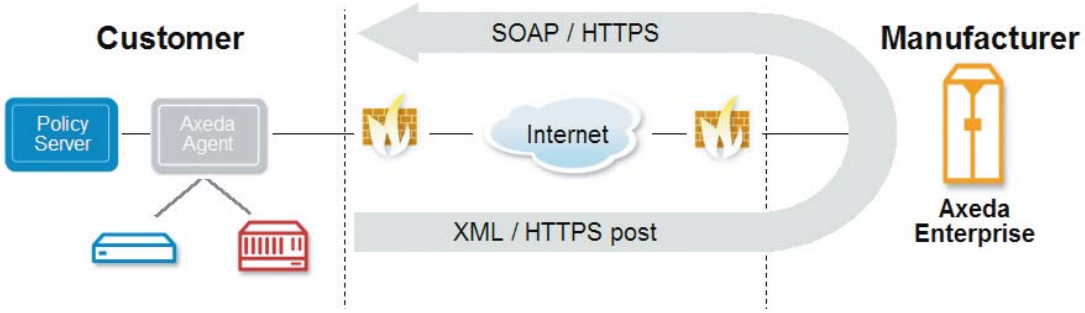
- le maintien du modèle de sécurité actuel : le dispositif Leica Microsystems doit prendre en charge la façon dont l'entreprise gère les opérations, politiques ou procédures de sécurité, et doit correspondre aux normes industrielles acceptées.

- le contrôle de l'accès utilisateur : conformément au modèle de sécurité du client, le dispositif Leica Microsystems doit fournir au client, et non à Leica Microsystems, un contrôle granulaire et doit définir des politiques à partir desquelles des actions pourront être entreprises sur le dispositif, telles que la collecte des données et la mise à jour de logiciels, et il doit en outre préciser quand ces actions doivent être exécutées. Ces politiques doivent être définies au niveau central pour tous les instruments du site d'un client.

- l'audit et le traçage : selon les exigences en matière de politique et de conformité réglementaire, le système de l'entreprise doit faciliter l'audit et le traçage de toutes les activités des utilisateurs et de l'administration.

Axeda ServiceLink apporte la performance, la flexibilité et l'extensibilité requises pour répondre aux besoins de la majeure partie des clients du RemoteCare de Leica Microsystems en fournissant la plus large palette possible de dispositifs de protection des données et des caractéristiques de sécurité.

Figure 1 : Communication Axeda Firewall-Friendly™



Pas de changement requis des infrastructures IT ou de sécurité
L'utilisation de la technologie Firewall-Friendly™ d'Axeda permet à RemoteCare de fournir une transmission bidirectionnelle basée sur les normes des services Web incluant le protocole de transfert hypertexte (HTTP), le protocole "Simple Object Access Protocol" (SOAP), et le langage de balisage "eXtensible Markup Language" (XML). L'infrastructure de sécurité IT du client final ne requiert aucun changement pour la prise en charge de la commande et des diagnostics à distance. Par ailleurs, toute la communication entre le centre de traitement de l'information de Leica ou le prestataire de services et le site du client est cryptée via le protocole Secure Sockets Layer (SSL) jusqu'à 168 bits.

Aucun RPV ni modem requis
L'agent RemoteCare émet toutes les communications conformément à l'environnement informatique sécurisé sur le site du dispositif. Il n'est donc pas nécessaire de régler des RPV coûteux pour la mise en place de RemoteCare ni de transiger sur la sécurité en utilisant des communications par ligne commutée. Une connexion à Internet constitue la seule exigence.

Dispositifs de sécurité principaux de RemoteCare :
- Communications Firewall-Friendly™
- Aucun changement requis des infrastructures IT et de sécurité
- Aucun RPV ni modem requis
- Commande entièrement gérée par le client final afin de mettre en œuvre les politiques de l'entreprise
- Déploiement rapide et gestion aisée de la sécurité des utilisateurs, de l'application et du dispositif
- Données de cryptage HTTPS, PKI et SSL 128 bits

Gestion aisée de l'authentification utilisateur et du contrôle d'accès
Le système RemoteCare utilise le protocole standard Lightweight Directory Access Protocol (LDAP) pour authentifier les utilisateurs.

Le contrôle d'accès utilisateur s'effectue via contrôle d'accès dépendant de l'activité et sur un contrôle d'accès dépendant du dispositif. Ces méthodes sont combinées d'une multitude de façons pour permettre aux utilisateurs de travailler de manière efficace tout en protégeant l'accès aux informations sensibles.

Le contrôle d'accès dépendant de l'activité permet à l'administrateur système de RemoteCare d'affecter et de classer les utilisateurs via Axeda ServiceLink, et de définir les activités pouvant être exécutées. Chaque groupe d'utilisateurs reçoit un accès contrôlé aux niveaux des applications, pages et fonctions Axeda.

Le contrôle d'accès dépendant du dispositif fournit une méthode de définition des dispositifs spécifiques accessibles à chaque groupe d'utilisateurs. Cette méthode de contrôle limite la visualisation des informations du dispositif uniquement aux dispositifs dont un utilisateur est responsable.

Communications sécurisées et confidentialité
La plupart des informations circulant sur l'Internet public utilisent du texte en clair encapsulé dans des messages HTTP standard. Les pirates informatiques peuvent avoir accès au réseau à un point proche de la source ou de la destination du message, puis le capturer et visualiser le texte de ces messages HTTP à l'aide d'outils facilement disponibles.

RemoteCare, via le logiciel et l'infrastructure serveur Axeda, prend en charge le même protocole de cryptage standard SSL que les banques pour leurs transactions en ligne. SSL prend en charge une longueur de clé de 168 bits max. et une authentification mutuelle utilisant des certificats. RemoteCare permet également de crypter les messages par la clé secrète AES 256 bits pouvant être utilisée avec le protocole SSL pour crypter les informations au-delà de la zone démilitarisée (DMZ).

Déploiements éprouvés
RemoteCare est déployé dans le monde entier par les fabricants de divers secteurs tels que la sécurité intérieure, la médecine, les sciences biologiques la technologie de l'information, les télécommunications, l'impression et l'imagerie, les kiosques, les semi-conducteurs et l'automatisation industrielle.

Caractéristiques de sécurité et avantages

La technologie Axeda pourvoit RemoteCare des caractéristiques de sécurité et avantages suivants

Sécurité réseau

Caractéristiques :
- La technologie Firewall-Friendly™ est basée sur les normes de services Web comme HTTP, SOAP et XML.
- L'agent Axeda émet toutes les communications pour que les dispositifs ne requièrent pas d'adresses publiques IP et qu'elles ne soient pas visibles à l'extérieur du pare-feu.

Avantages :
- Les clients n'ont pas besoin de modifier les réglages de leur pare-feu ou de leur serveur proxy, ce qui facilite le déploiement et l'obtention des objectifs de conformité d'adressage.
- Pas besoin de connexion RPV ou modem.

Sécurité du système et des données

Caractéristiques :
- Le cryptage SSL prend en charge la longueur de clé 168 bits max. et l'authentification mutuelle utilisant des certificats numériques bidirectionnels.
- Cryptage de messages via la clé secrète AES 256 bits qui peut être utilisée avec le protocole SSL pour crypter les données au-delà de la zone démilitarisée.

Avantages :
- Seules les parties autorisées ont accès aux dispositifs et données désignées. Les clients finaux peuvent limiter l'accès, la visualisation et même les actions selon le rôle de l'utilisateur ce qui leur permet de garder le contrôle sur les utilisateurs et les actions exécutées.
- Les communications éprouvées basées sur les normes garantissent la conformité avec les exigences réglementaires.

Sécurité des utilisateurs et des applications

Caractéristiques :
- L'accès au système est contrôlé de manière centrale et authentifié en fonction du système LDAP d'une entreprise.
- Des mots de passe forts sont utilisés : un minimum de six caractères combinant lettres, chiffres et symboles.
- Tout accès à distance est tracé et enregistré.

Avantages :
- Les clients peuvent recourir aux comptes utilisateurs LDAP existants, facilitant ainsi le démarrage.
- Les utilisateurs finaux reçoivent une piste d'audit détaillée lors de l'analyse de l'activité du vendeur en vue de vérifier s'il répond aux critères.

Résumé

Leica Microsystems a choisi Axeda ServiceLink pour RemoteCare afin d'apporter le niveau de sécurité le plus élevé. Les entreprises du monde entier fournissent à leurs clients des services à distance utilisant Axeda ServiceLink. Car Axeda intègre minutieusement les normes et principes de sécurité dans la conception et l'exploitation de l'infrastructure et des services Axeda. Comme pour Leica Microsystems, la priorité la plus élevée d'Axeda est une sécurité sans compromis permettant aux clients d'atteindre leurs objectifs en termes de service à distance de manière sûre et efficace.

95.8796 Rev A