Providing Secure Remote Service and Support for Intelligent Devices

Security is a primary concern of Leica Microsystems and Leica Microsystems' customers that employ remote services. Leica Microsystems requires a proven remote service solution that protects against viruses and hackers and supports our intelligent instruments without major end-user modifications, while working within our current network security model and achieving official certification by a third-party security company. Since Leica Microsystems' instruments are connected to our customer's networks, the end-customers also need to be assured that the remote service solution supports their security model, provides granular control over user access, and offers easy-to-use audit and tracking capabilities.

For the new Leica RemoteCare remote service system, Leica Microsystems, like many equipment manufacturers, delivers business-critical remote services using Axeda® ServiceLink™ software and server infrastructrure. Axeda ServiceLink eases the security concerns of Leica and our customers, while proactively minimizing downtime, managing risk and ensuring the equipment is always enabled to provide maximum results.

Using Axeda ServiceLink, Leica Microsystems' RemoteCare seamlessly connects Leica Microsystems and the Leica Microsystems instruments within our customer's environments. Because these instruments often track patient records and other types of private and protected information, security and compliance capabilities are among the most important requirements evaluated in any remote service solution. This paper examines the requirements of Leica Microsystems and Leica Microsystems' customers as well as how Axeda ServiceLink provides the proven and secure remote service and support to address those requirements.

Leica Microsystems' Requirements for Remote Service Security

Leica Microsystems chose Axeda's products for RemoteCare to meet the most stringent security requirements of Leica Microsystems and Leica Microsystems' customers so that they can use remote services effectively and routinely – feeling confident that their connections are secure and kept private.
Some of our most common requirements include:

- Enterprise proven design – Connecting any computer to the Internet raises security concerns, and connecting intelligent devices is no different. Whether hackers are trying to harm a device with corrupt data or viruses, steal data travelling between the instrument and Leica Microsystems, or gain unauthorized access to critical information, a remote monitoring system has to protect against these and other threats.

- Support for multiple devices – Leica Microsystems needs to securely support different device types and complex customer configurations without requiring major end-user changes.

- Rapid deployment – For customers to adopt remote service systems, the security capabilities must exist within the customer's current network security model.

- Third-party security firm validation – Official certification by a security audit provides customers with confidence in the capabilities of the technology and vendor.

Commitment:
Leica Microsystems believes that privacy and security are of the highest importance to our customers. RemoteCare maintains the following security principles:

- Protect the integrity of the system – network, equipment, and data
- Track access and activity to achieve regulatory compliance
- Provide flexibility and control to enforce business policies
- Audit and certify Leica Microsystems processes and solutions regularly by a third-party

Customer Requirements for Remote Service Security

Intelligent instruments are connected to our customer's networks. Each customer has their own security policy and network protection in the form of firewalls, proxy servers, and addressing schemes. A device connected to their network will be protected behind these layers of security. If a remote service offering requires changes to our customer's network protection, it will likely fail to gain acceptance. Because of this, it is important to consider the requirements of the customer, including:

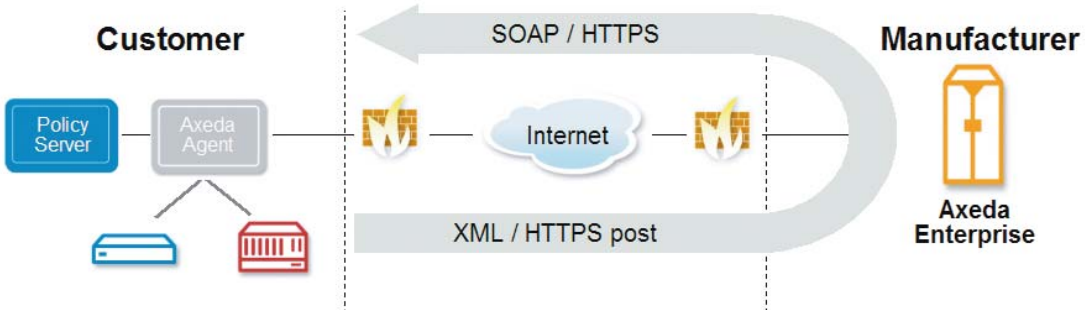
- Maintain current security model – Leica Microsystems' device must support the way that the organization manages security operations, policies, or procedures, and should adhere to accepted industry standards.

- Control user access – In line with the customer's security model, Leica Microsystems' device must provide the customer – not Leica Microsystems – with granular control and set policies on what actions can be performed on the device such as data collection and software updates, and when those actions can be performed. These policies need to be centrally defined for all instruments at a customer location.

- Audit and track activity – Policy and regulatory compliance requirements dictate that the enterprise system must make auditing and tracking all user and administration activity easy.

Axeda ServiceLink delivers the performance, flexibility, and scalability required to meet the needs of the broadest range of Leica Microsystems' RemoteCare customers by providing the widest range of data protection safeguards and security features.

Figure 1: Axeda Firewall-Friendly™ communications



No Changes Required to IT or Security Infrastructures
Using Axeda's Firewall-Friendly™ technology allows RemoteCare to provide two-way communication based on Web Services standards including Hypertext Transfer Protocol (HTTP), Simple Object Access Protocol (SOAP), and eXtensible Markup Language (XML). No changes to the IT security infrastructure of the end customer are required to support remote monitoring and diagnostics. In addition, all communication between the data center of Leica or service provider and the customer site is encrypted using Secure Sockets Layer (SSL) up to 168 bits.

No VPN or Modem Needed
The RemoteCare agent initiates all communications in compliance with the secure computing environment at the device site. There is also no need to set up expensive VPNs to implement RemoteCare or to compromise security by using dial-up communications. The only requirement is an Internet connection.

RemoteCare Security Highlights:
- Firewall-Friendly™ communications
- No changes required to IT and security infrastructures
- No VPN or modems needed
- Complete end-customer control to enforce business policies
- Easy to deploy and manage user, application, and device security
- HTTPS, PKI, and 128-bit SSL encryption data

Easily Managed User Authentication and Access Control
The RemoteCare system uses the Lightweight Directory Access Protocol (LDAP) standard to authenticate users.

User access control is addressed through activity-based access control and device-based access control. These methods are combined in a wide variety of ways to allow users to do their jobs effectively while protecting access to sensitive information.

Activity-based access control enables the RemoteCare system administrator to assign and classify users using Axeda ServiceLink, and define the activities that can be performed. Each user group is given controlled access at the Axeda application, page, and function levels.

Device-based access control provides a method for defining the specific devices accessible to each user group. This method of control limits the view of device information to only those devices for which a user is responsible.

Secure Communications and Data Confidentiality
Much of the information that travels across the public Internet uses plain text encapsulated within standard HTTP messages. Hackers can gain access to the network at a point close to the source or destination of the message and then capture and view the text of these HTTP messages with readily available tools.

RemoteCare, through the Axeda software and server infrastructure, supports the same standard SSL encryption as banks use for online transactions. SSL supports key length up to 168 bits and mutual authentication using certificates. RemoteCare can also enable secret key AES 256-bit message encryption, which may be used with SSL to encrypt data beyond the Demilitarized Zone (DMZ).

Proven Deployments
RemoteCare is deployed around the world by manufacturers in a range of industries, including homeland security, medical, life sciences, information technology, telecommunications, print and imaging, kiosks, semiconductor, industrial, and building automation.

Security Features and Benefits

Axeda technology provides RemoteCare with the following security features and benefits

Network Security

Features:
- Firewall-Friendly™ technology is based on Web Services standards, including HTTP, SOAP, and XML.
- Axeda Agent initiates all communication, so devices do not require public IP addresses and are not visible from outside the firewall.

Benefits:
- Customers don't have to make changes to firewall settings or proxy servers, easing deployment and addressing compliance objectives.
- No need for VPN or modem connections.

System and Data Security

Features:
- SSL encryption supports key length up to 168 bits and mutual authentication using bidirectional digital certificates.
- Secret key AES 256-bit message encryption, which can be used with SSL to encrypt data behind the DMZ.

Benefits:
- Only authorized parties have access to designated devices and data. End-customers can limit access, views, and even actions based on the user's role, which gives them control over users and actions.
- Proven, standards-based communications ensure compliance with regulatory requirements.

User and Application Security

Features:
- Access to the system is centrally controlled and authenticated against an enterprise LDAP system.
- Strong passwords are enforced – a minimum of six characters with a combination of letters, numbers, and symbols.
- All remote access activity is tracked and recorded.

Benefits:
- Customers can leverage existing LDAP user accounts, making it easy to get started.
- End-users have a comprehensive audit trail when analyzing vendor activity for compliance needs.

Summary

Leica Microsystems chose Axeda ServiceLink for RemoteCare to provide the highest level of security. Companies throughout the world are providing remote service to their customers using Axeda ServiceLink. This happens because Axeda carefully incorporate security principles and standards in the design and operation of the Axeda infrastructure and services. Like Leica Microsystems' a top priority at Axeda is stringent security that enables customers to achieve their remote service goals securely and efficiently.

95.8641 Rev A