IT Security – Remote Services

1. Overview

Security is a primary concern of METTLER TOLEDO and the end-customers that employ remote services. METTLER TOLEDO requires a proven remote service solution that protects against viruses and hackers, and supports METTLER TOLEDO intelligent products without major modifications for the end-user customers, while working within standard network security models. Since METTLER TOLEDO products are connected within the end-customer networks, they also need to be assured that the remote service solution supports the customers security model, provides granular control over user rights, plus offers auditing and tracking capabilities.

For InTouchSM Remote Services, METTLER TOLEDO, like many equipment manufacturers, has partnered with a proven leader to deliver business-critical remote services using Axeda® ServiceLink™ and their patented Firewall-Friendly™ technology. The selection of Axeda’s solution eases the security concerns of METTLER TOLEDO, as well as those of our end-customers, by providing the same proven and secure remote service & support applications required by Axeda’s other customers in high security environments such as in the banking, financial, healthcare, hospital, pharmaceutical, and IT industries.

InTouch™ Remote Services provides a seamless connection between the METTLER TOLEDO remote support engineers and METTLER TOLEDO intelligent products within the customer’s environments. Because these products often contain sensitive customer data, as well as 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 details the security requirements of METTLER TOLEDO and those of our end-customers, as well as how InTouch™ Remote Services provides proven and secure remote service platform to address those requirements.

Our Commitment
Privacy and security are of the up most importance to our end-customers. Therefore METTLER TOLEDO is committed to the following security principles;

• Maintain and protect the integrity of the system – network, equipment, and data
• Conceal data from unauthorized parties
• Ensure system users are authenticated
• Limit each user to specific data, views and actions
• Provide flexibility and control to enforce business policies
• Audit and certify the processes and technology solution regularly by a third-party

2. METTLER TOLEDO’s Requirements for Remote Service Security

METTLER TOLEDO’s solution needs to meet the most stringent security requirements of our end-customers so that remote services can be used effectively and routinely – feeling confident that their connections are secure and private. METTLER TOLEDO requirements include:

Enterprise proven design
Connecting a computer to the Internet raises security concerns; therefore connecting intelligent products are no different. A remote support & monitoring system must safeguard against all IT security threats.
Support for multiple devices
METTLER TOLEDO needs to securely support a wide variety and large number of different product types and complex customer configurations without requiring significant changes for our customers.

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

Third-party security firm validation
Official certification by a 3rd party security audit provides METTLER TOLEDO with the confidence in the capabilities of our vendor partner, the technology, and their process & procedures.

3. End-Customer’s Requirements for Remote Service Security

Intelligent products are connected to the end-customer’s networks. Each customer has their own security policies and network protection in the form of firewalls, proxy servers, and addressing schemes. A product connected to their network must 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 end-customer, including:

Maintain current security model
METTLER TOLEDO intelligent products must support the way the customer’s IT organization manages security operations, policies, or procedures, and should adhere to accepted industry standards.

Control user access
In compliance with the customer’s security model, InTouch™ Remote Services must provide the customer with granular control and set policies on the actions which can be performed on the device such as the data collection and software updates, and when those actions can be performed. These policies can be centrally defined for all connected devices at the customer’s location.

Audit and track activity
Policy and regulatory compliance requirements often dictate that the remote service system must make auditing and tracking all user and administration activity easy.

Data integrity and security
Data sent from the connected METTLER TOLEDO product to the enterprise server is protected through the use of secure data encryption methods. Only the data necessary to monitor, diagnose and troubleshoot the METTLER TOLEDO product is collected. No customer sensitive data is collected in the data set delivered to the enterprise. InTouch™ Remote Services delivers the performance, flexibility, and scalability required to meet the needs of the broadest range of METTLER TOLEDO customers by providing the widest range of data protection safeguards and security features.


- Firewall Friendly™ communications
- No changes required to IT & security infrastructure
- No VPN or modems required
- HTTPS, PKI, and 128-bit SSL encryption data protection
- VeriSign Security certified
- LDAP to manage user authentication, application access & device security
5. Maintaining Network Security Integrity

By utilizing Axeda’s ServiceLink™ and their patented Firewall-Friendly™ technology, InTouch™ Remote Services is provided by a two-way communication based on Web Services standards including Hypertext Transfer Protocol Secure (HTTPS), Simple Object Access Protocol (SOAP), and eXtensible Markup Language (XML). In addition, all communications between the end-customer site, the enterprise server, and the remote support technicians of METTLER TOLEDO, are encrypted using Secure Sockets Layer (SSL) with 128 bits.

The remote service agent software on the METTLER TOLEDO devices initiates all communication with the enterprise server. This intelligent agent software enables the device to act as a Web client, and initiates messages to the enterprise server that are sent as HTTP POST commands. Each message contains data encoded in XML format and is sent using SSL encryption across port 443. Also the software agent can only access the specific servers identified for InTouch™ Remote Services.

Since the device initiates all communications, there is also no need to set up and maintain VPNs to implement InTouch™ Remote Services or to compromise security by using dial-up communications.

The device does not have a public IP address. All devices remain securely hidden behind the end-customer’s IT security infrastructures of firewalls, routers, and proxy servers.

Essentially, if a Web browser can access the Internet using the customer’s current network infrastructure, the InTouch™ Remote Services enabled device can communicate with the enterprise server using that same network connection. Therefore no changes are required to the IT security infrastructure.

6. User Authentication & Access Control

The InTouch™ Remote Services system uses the Lightweight Directory Access Protocol (LDAP) standard to authenticate users. User access control is addressed through a combination of activity-based access control and device-based access control. These methods allow METTLER TOLEDO remote support users to do their jobs effectively while protecting access to sensitive information. Only authenticated users with access to specific customer devices can gain access to those devices. As well, their abilities to access specific functions are also controlled through the system.
The enterprise system also automatically logs off users after a period of inactivity and enforces the use of strong passwords by requiring a combination of letters, numbers, and symbols.

Furthermore, the enterprise system creates a full audit trail which documents every activity and event from both the intelligent devices and the remote support users. Therefore the system maintains records of who did what, when, and where.

7. Ensuring Data Confidentiality

The technology utilized to provide InTouch™ Remote Services uses Secure Sockets Layer (SSL) to provide secure transmission of data. SSL provides a protocol for transmitting private data via the Internet. In addition to encrypting data, the SSL standard also provides authentication to ensure that both the sender and receiver of data are known to each other. SSL supports 128 bit key length and mutual authentication using certificates. SSL is the same encryption standard used by banks for online transactions.

The InTouch™ Remote Service agent embedded into METTLER TOLEDO intelligent products, monitors and analyses only specific data items which are pertinent to operation and performance of the product. No customer sensitive data is included in the data set which is routinely monitored for product performance.

As well, only the data needed to monitor, diagnose, and troubleshoot the specific product is collected and analyzed at the enterprise. Again this is only equipment specific data, and does not contain any customer sensitive data.

8. Additional Security Features

VeriSign Security Certification

Axeda utilizes the services of VeriSign to conduct a comprehensive examination of their entire security program. The VeriSign assessment involves three primary areas of evaluation:

- **Application Architecture Design Analysis** – a review of security in how ServiceLink™ was architected
- **Application Code Review** – a review of ServiceLink™ source code for known security flaws and vulnerabilities
- **Application-Level Assessment** – detailed testing for known security vulnerabilities in Web-based applications

Proven Deployments

InTouch™ Remote Services utilizes the same technology that is currently deployed around the world by manufacturers in a wide range of industries, including homeland security, medical, life sciences, information technology, telecommunications, print and imaging, kiosks, semiconductor, industrial, and building automation. Axeda supplies those manufacturers and their end-customers the same high level of security and data protection as expected by our end-customers.

Data centers commonly utilize solutions from companies such as 3PAR, Egenera, EMC2, Inilon, NetApp, Quantum, or Teradata, and those companies provide remote support of their products. If your IT department utilizes solutions from these companies, then you might already be familiar with Axeda’s technology, as these companies employ the same technology from Axeda that is used by METTLER TOLEDO.
Remote Infrastructure

InTouch™ Remote Services infrastructure is maintained in a state-of-the-art data center which fulfills the TIA 942 standards defined by the American Uptime Institute. The TIA 942 standard determines parameters for describing the availability and failure safety of computer centers, among others, for the redundant design of subsystems, energy supply, air conditioning and network cabling. This provides for greater than 99.95% availability. In addition, the data center undergoes an SAS 70 audit for service organizations on an annual basis. SAS 70, which is defined by the AICPA (American Institute of Certified Public Accountants), specifies in which way service providers must be audited so that they fulfill the expectations and information demands of the addressees.

9. Summary

METTLER TOLEDO has chosen Axeda as their remote service infrastructure provider to enable InTouch™ Remote Services in order to provide customers with the highest level of security without changing their current IT security infrastructure. Companies throughout the world are providing remote services to their end-customers using Axeda’s ServiceLink™. This is a result of careful incorporation security principles and standards in the design and operation of the infrastructure and services provided by Axeda.

A top priority for METTLER TOLEDO is stringent security, providing our customers with the confidence we can deliver InTouch™ Remote Services securely and efficiently. This ultimately provides customers with higher product availability, improved product performance, and delivers the highest quality output from their METTLER TOLEDO products.