Technical Data Sheet

SMARTLINK **Security Document**

1. General information

This document serves as a comprehensive guide to understanding the data security measures within the **SMART**LINK platform, detailing how Atlas Copco connects devices, uploads telemetry data, and protects the infrastructure of the IoT platform. By providing a clear step-by-step overview of processes to secure customer data during upload and outlining the built-in security measures within our network, this document offers valuable insight into Atlas Copco's approach to cybersecurity.

Document edition	:	04
Applicable to	:	**SMART**LINK

2. Review and distribution

This document will be reviewed by our IoT Manager and approved by the CTBA Security Officer. The standard review cycle for this document is **annually** or upon any significant changes.

Rev No.	Reason for revision	Date
01	Initial release	05/2023
02	Additional mentions of the Azure China infrastructure, compliance, and certification.	11/2023
03	New document lay-out New versions of figure 1 & 2 Add a figure in Appendix about **SMART**LINK China	04/2024
04	Cleaning up document Adding references to SMARTBOX (PRO)	11/2024

3. Document overview

4. Document information

4.1. Scope

This document covers the data flow from the controller, sensors, and input modules, via the gateway device, towards the **SMART**LINK IoT platform.

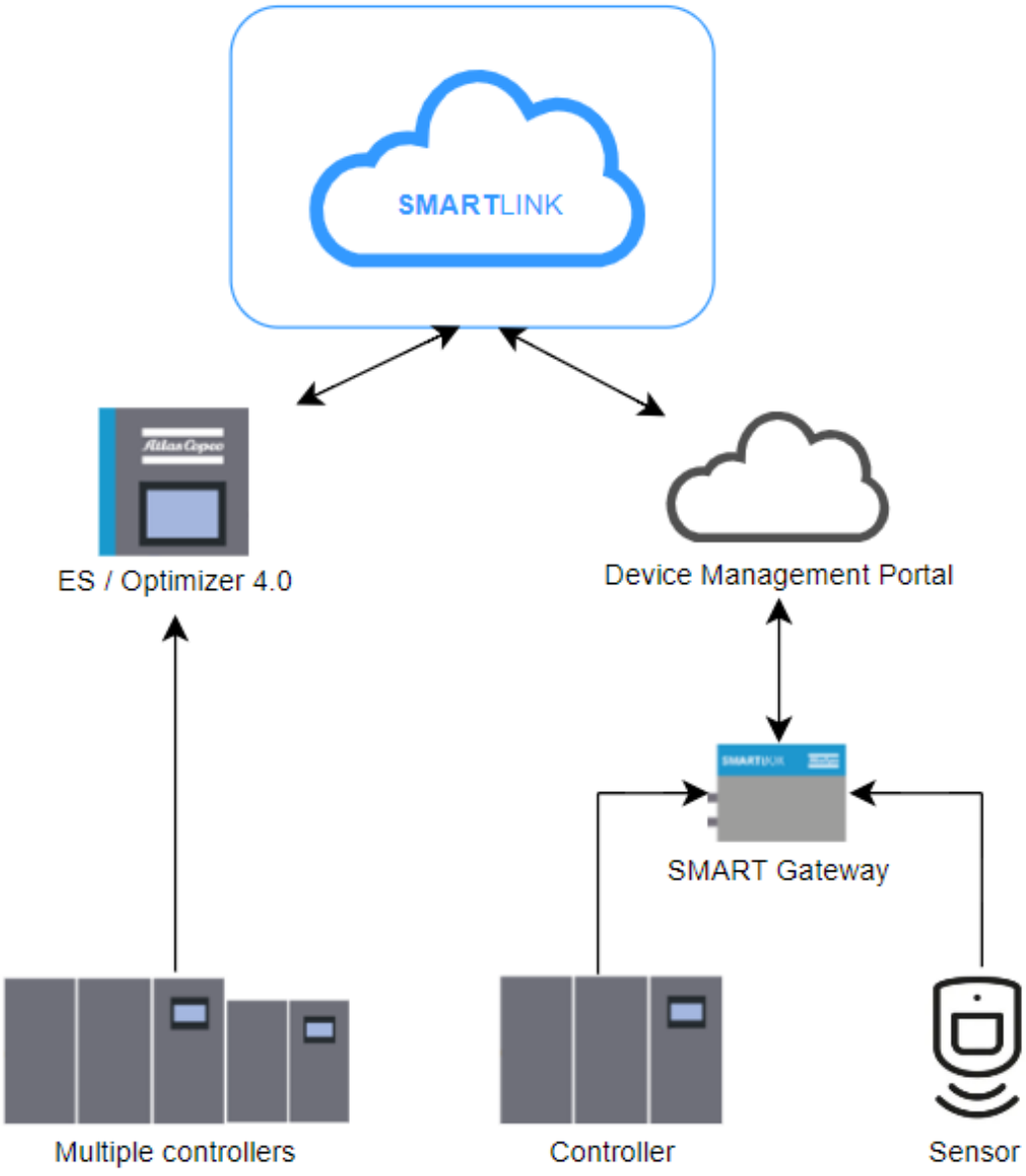

*Figure 1: **SMART**LINK Data Flow – From Sensor & Controller to IoT Platform*

4.2. Objective

This document serves as a comprehensive guide to understanding the data security measures within the **SMART**LINK platform, detailing how Atlas Copco connects devices, uploads telemetry data, and protects the infrastructure of the IoT platform. By providing a clear step-by-step overview of processes to secure customer data during upload and outlining the built-in security measures within our network, this document offers valuable insight into Atlas Copco's approach to cybersecurity.

4.3. Network diagram

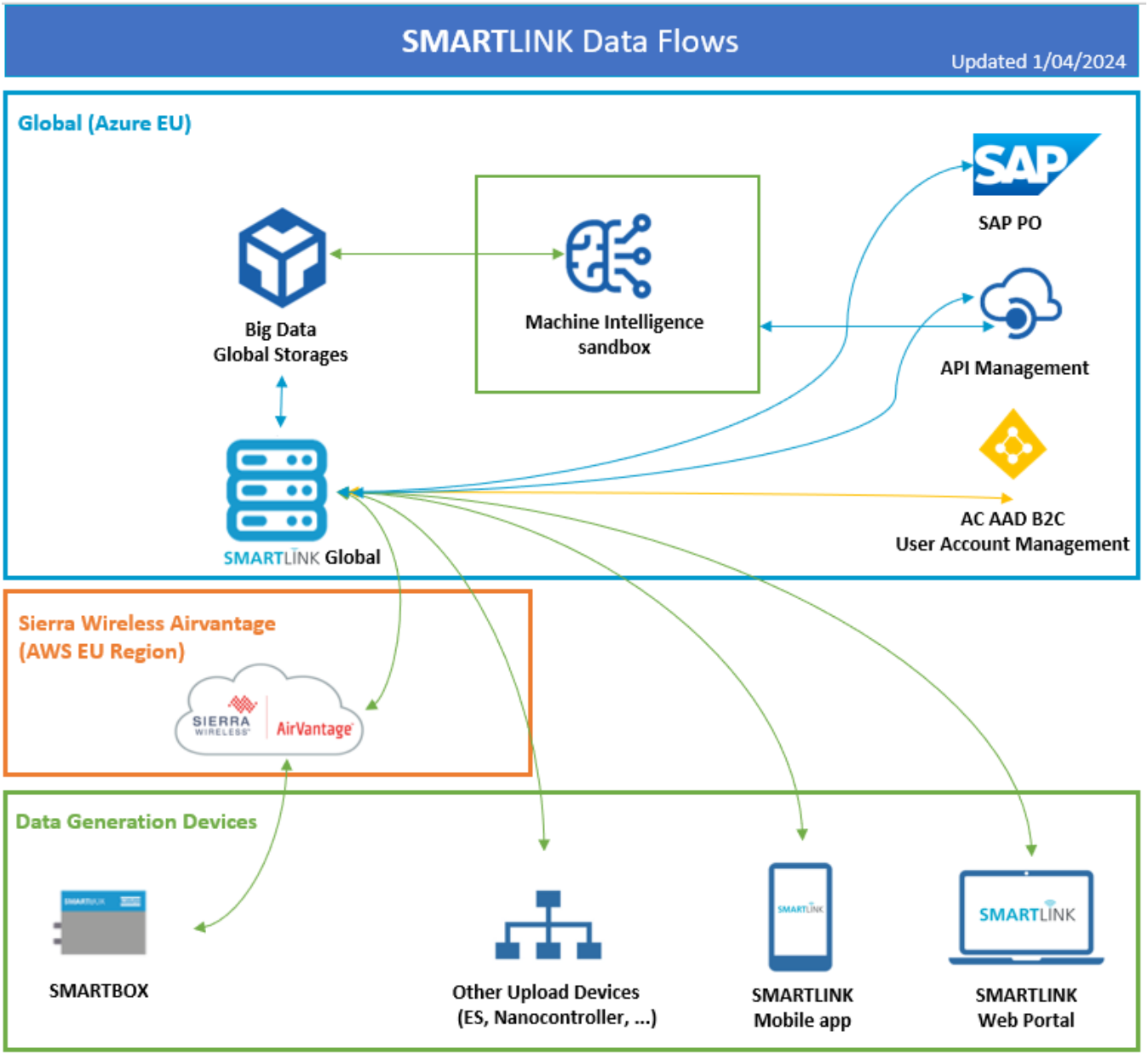

*Figure 2: **SMART**LINK Data Flow - Network diagram for **SMART**LINK Global*

5. SMARTBOX (PRO) data upload

The SMARTBOX or SMARTBOX PRO wirelessly uploads data via a private 3G or 4G APN (Access Point Name) to the communication provider using a secure connection to our back-office. The SMARTBOX (PRO) functions solely as an upload device, transmitting data from the machine to the back-office, **with no control or command of the machine executed through the device.**

Software updates for the SMARTBOX (PRO) can be performed over-the-air (OTA) via the same secure connection, but this does not apply to the machine controller.

5.1. SMARTBOX (PRO) Portal and Device Management Platform

The SMARTBOX service platform and its relevant security services are diligently maintained and validated by its hosts (see chapter Solution Partners). This includes active security monitoring and secured and continuously updated data centers. The SMARTBOX device management portal is compliant with the following global security standards:

- ISO 27001
- SOC
- PCI Data Security Standard
- Australian Signals Directorate (ASD) Information Security Manual
- Singapore Multi-Tier Cloud Security Standard (MTCS SS 584)
- FedRamp Agency ATOs (AWS GovCloud US Region and AWS US East/West regions)
- US granted a provisional authorization for DoD CSM Levels 1-5

SMARTBOX PRO device management platform:

- Working towards ISO 27001 certification
- Threat modelling by a state-of-the-art company in Belgium
- OWASP SAMM assessment which lead to valuable insights that have been tackled

5.2. Communication protocol

The communication protocol transmits data without including any customer, plant, location, or compressed air application details. All data is tagged using GUIDs. Customer commissioning is handled at the back-office and through the secured upload connection.

6. ES / COMBOX-E / OPTIMIZER 4.0 Data Upload

Since there are no incoming connections to the ES/COMBOX-E, data is only uploaded to the **SMART**LINK platform. There are three methods for uploading data from the ES/COMBOX-E to **SMART**LINK:

- Via a modem connection
- Via a LAN (Local Area Network) connection
- Via a SMARTBOX (PRO)

6.1. Modem upload connection:

In this setup, the modem connects directly to the internet provider. Since there are no physical connections to the LAN network, there is no security risk to the local network of the customer.

6.2. LAN upload connection:

The LAN data upload uses web services on the Atlas Copco servers. The data is transferred using a SOAP protocol, which uses HTTP protocol (internet protocol) as a transfer mechanism. This means that all upload communication is going through the usual internet channels.

- The ES/COMBOX-E device is connected to the local network which needs to be secured by a firewall.
- The ES device has some open ports to upload and for the local debug and service connection. The LAN firewall can close all ports except port 80 for the Internet.
- The ES/COMBOX-E uploads data to the Atlas Copco website airconnectupload.atlascopco.com (on default port 80). If desired, all but this connection can be blocked by the firewall.

7. SMARTLINK IoT platform and web portal

SMARTLINK services and its relevant security services are maintained and validated by its host (see chapter Solution Partners), which includes regular updates.

The service operates in data centers managed by our partner, Microsoft, in Western Europe, and by 21Vianet in partnership with Microsoft in China. These geographically distributed data centers adhere to key industry standards for security and reliability, including ISO/IEC 27001:2022 and NIST SP 800-53. They are managed, monitored, and maintained by experienced operations staff, ensuring 24/7 continuity for some of the world's largest online services.

SMARTLINK is a full cloud-native solution without any on-premises components.

More details are available on this website: https://docs.microsoft.com/en-us/azure/security/fundamentals/infrastructure. Here you can find a series of articles, which contain information about what our partner does to secure its infrastructure. The articles address:

- Physical security
- Availability
- Components and boundaries
- Network architecture
- Production network
- SQL Database
- Operations
- Monitoring
- Integrity
- Data protection

7.1. Field gateways

Field gateways are specialized devices or general-purpose gateways primarily designed to enable communication. The Legacy ES/Optimizer 4.0 Field Gateway not only provides connectivity but also functions as a machine controller, whereas the SMARTBOX (PRO) field gateway solely provides connectivity.

Both the Legacy ES/Optimizer 4.0 and the SMARTBOX (PRO) aggregate data, with machines frequently sampling sensor data and the gateways responsible for uploading it.

The sampling and upload frequencies vary depending on the device, with both the Legacy ES and SMARTBOX (PRO) uploading data only when changes occur, though they follow fixed but distinct upload schedules. The scope of a field gateway includes the gateway itself and all connected devices. As the name suggests, field gateways operate outside of dedicated data processing facilities and are typically collocated with the devices they manage.

7.2. Firewall restrictions

Global

The **SMART**LINK portal is accessible over the secured https protocol via Azure's Web Application Firewall (WAF). In case you have a policy to set firewall restrictions, please allow https (port 443) traffic for the following two domains:

- *.atlascopco.com
- *.connectivityicons.com

For the installation, the service technician requires the following ports to be temporarily enabled (port 443), which can be disabled after installation:

- *serviceclampconnectivity.com
- *machineconnectivity.com
- *wirelessconnectivitysetup.com

China

The Chinese **SMART**LINK portal is accessible over the secured https protocol via Azure's Web Application Firewall (WAF) (which is hosted in China). In case you have a policy to set firewall restrictions, please allow https (port 443) traffic for the following two domains:

- *.atlascopco.com.cn
- *.connectivityicons.com.cn

For installation, the service technician requires the following ports to be temporarily enabled (port 443), which can be disabled after installation:

- *serviceclampconnectivity.com.cn
- *.machineconnectivity.com.cn
- *.wirelessconnectivitysetup.com.cn

8. Security

8.1. Data protection

SMARTLINK safeguards your data through multiple layers of protection:

- All data is encrypted both at rest and in transit
- Data in transit is secured with TLS 1.2 encryption, with one exception—Legacy ES devices upload data via HTTP
- Data is stored with geographic redundancy
- All data is regularly backed up

SMARTLINK relies on Microsoft Entra ID (formerly Microsoft Azure Active Directory or Azure AD) B2B and B2C for authentication. It is the IT Administrator of the employee's company's responsibility to remove them from their company's AAD when they leave the organization. When an employee is removed from company's AAD, they automatically lose access to **SMART**LINK.

Password policies are managed by the user's IT department. Atlas Copco enforces multi-factor authentication (MFA) to be enabled on all AAD B2C accounts.

8.2. Access to networks and audit logs

All remote administration of servers, workstations, network equipment, and similar systems is conducted through secure connections using certificates issued by a Certificate Authority (CA). Self-signed certificates are not allowed. Our Azure cloud infrastructure is configured to retain audit logs for a minimum of 90 days.

8.3. Application security (Vulnerability Assessment & Penetration Testing)

Atlas Copco's Security team employs a combination of automated tools and manual penetration testing to identify vulnerabilities in **SMART**LINK. These tests cover both the infrastructure, and the code developed for **SMART**LINK.

Any identified security issues are addressed in accordance with Atlas Copco's vulnerability management policy.

8.4. Certification

The entire Compressor Technique business area, where **SMART**LINK was developed, is already ISO 9001 certified, demonstrating our commitment to quality.

The **SMART**LINK portal and platform are now actively pursuing ISO/IEC 27001 certification, guided by the Atlas Copco CTBA Security Officer and a specialized third-party. Certification is targeted for completion by May 2025. Security is a top priority, and we are diligently implementing our Information Security Management System (ISMS) to the highest standards.

9. Solution Partners

Atlas Copco carefully and diligently selects their business partners for all products and operations. Their quality of supply, level of service and security levels are continuously evaluated. For the **SMART**LINK connectivity solution, the below partners have been selected:

The SMARTBOX device management platform is hosted within the Amazon Web Services (AWS) cloud platform, or together with the **SMART**LINK services, which are hosted within the Azure cloud platform from Microsoft in Europe and 21Vianet/Microsoft in China.

10. FAQ

10.1. Which personal data is collected when using SMARTLINK?

SMARTLINK collects a limited amount of personal data (also known as PII) from users to facilitate platform functionality and ensure effective communication. The following data points are collected:

- **Name**: Required for user registration and identification within the system.
- **Email Address**: Mandatory for account creation, login credentials, and communication related to platform updates or user notifications.
- **Mobile Phone Number**: Optional but may be provided to enable SMS notifications for real-time alerts and system messages.

SMARTLINK minimizes the collection of PII and adheres to strict privacy standards, ensuring that user data is handled securely in compliance with applicable data protection regulations.

10.2. Where is the service hosted?

The **SMART**LINK Global platform primarily operates in the Azure Western Europe region, based in Amsterdam, The Netherlands.

SMARTLINK China utilizes the Azure China North region. Following Chinese cybersecurity regulations, all machines and customers located in Mainland China have been migrated in October 2022 to dedicated infrastructure hosted on Azure China.

10.3. Do you have a structured Information Security Management Program (ISMS) in place?

As mentioned earlier, Atlas Copco is actively working towards ISO/IEC 27001 certification for the **SMART**LINK portal and platform. We are collaborating with a highly reputable third-party to implement a robust Information Security Management System (ISMS). Additionally, our internal compliance team is assisting in the development and setup of this ISMS and aligning it with the one from ISO 9001.

Our implementation partners are ISO/IEC 27001 certified, and their ISMS is set up in their Quality Management System.

10.4. Is there a segregation of duties implemented for privileged roles?

(e.g., service desk, system administration, database administration, backup, information security management)

Yes, a segregation is implemented on 2 levels:

1. **SMART**LINK system management on Azure uses role-based access control.
2. Within the **SMART**LINK web portal, multiple roles with different permissions are supported.

10.5. What is the remote access policy for administrators, incl. allowed locations and security controls?

SMARTLINK system management can only be executed using the Azure Management portal or other Azure tools like Powershell scripts and CLI. To gain access, the administrator must log on to the Atlas Copco Azure environment. There is no restriction on geographical location.

10.6. Do you maintain an asset inventory of relevant data repositories, systems, and applications?

Atlas Copco relies on a CMDB (configuration management database) which provides an organized view of systems, applications, and configuration data. The Azure Management Portal provides standard access to all Azure resources and configurations.

10.7. How do you separate the data of your customers?

SMARTLINK follows the standard SaaS (Software as a Service) model and applies logical sharding in all data stores.

10.8. Are user credentials (including technical accounts) of an application or system always stored by using cryptographic mechanisms?

(e.g., hashed password)

All system credentials are stored in Azure Key Vault. User credentials are stored at the user's Identity Provider and not in **SMART**LINK itself.

10.9. Can you provide a list of the available technical documentation?

(e.g., service, architecture, authentication, interfaces, security controls)?

More detailed and up to date information can be found at https://helpsmartlink.atlascopco.com/

10.10. Is customer data in transit over public networks (e.g., Internet) encrypted?

- All customer data in the web portal is always encrypted in transit
- The customer's machine data is encrypted when a SMARTBOX (PRO) is used
- Customer's machine data is not encrypted when a legacy ES/optimizer 4.0 gateway is used

10.11. Describe your internal software development process.

SMARTLINK applies a wide range of policies, best-practices, techniques, and tools:

- Key Vault to store sensitive information like certificates and passwords
- Azure AD for authentication
- RBAC is used to give users access to development environments and code repository
- "Definition of Ready" and "Definition of Done" are used to check the specification of functionality and its realization. They are embedded in a defined workflow that is used to have a controlled way of building and delivering features
- Execute code reviews on every code change with SonarQube for the quality of our code and Snyk for more secure code
- Audit trails in Azure are used (e.g., to log Database access)
- Azure Monitor and Azure Dashboards

10.12. Are employees regularly trained and tested on data privacy topics?

Atlas Copco regularly conducts comprehensive security and privacy awareness training. Atlas Copco Group holds an annual mandatory training session for all employees. Additionally, we run quarterly phishing tests, and employees who click on a phishing email are required to complete mandatory follow-up training.