

XoT – Product description for the machine builder's technical file

Version 1.0 · 28 October 2026 · Xertified AB

1. Purpose and scope

This description gives a machine builder the facts about XoT needed in the technical file of a machine that includes XoT. It supports the builder's own risk assessment under the Machinery Regulation (EU) 2023/1230 and the Cyber Resilience Act (EU) 2024/2847.

It is not a declaration of conformity for the machine. The machine builder remains responsible for the risk assessment, the conformity assessment and the technical documentation of the machine. It is Xertified's description of its own product, not legal advice.

Technical details that change between releases are published at docs.xertified.com: firewall ports and destinations, verified protocols and router models, measured latency and release notes. Refer to the release that is delivered with the machine.

2. Product identification and intended purpose

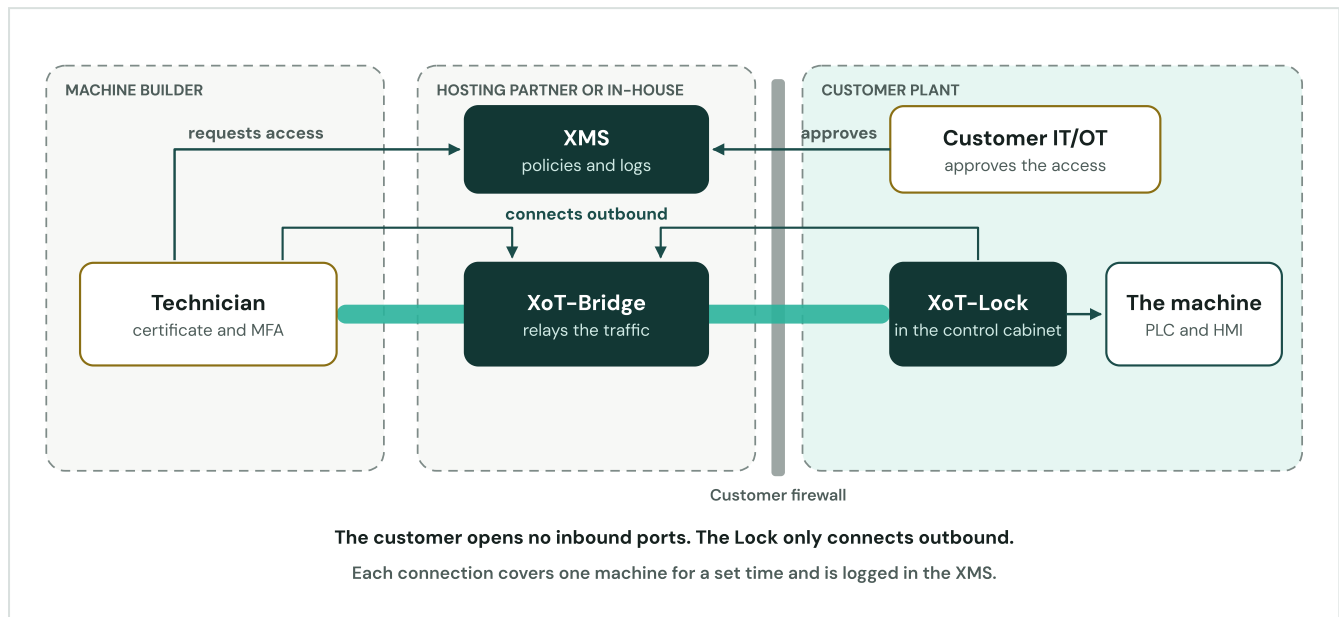
XoT (Xertified of Things) controls network access to equipment such as PLCs, HMIs and industrial PCs. It lets only authorised users and devices reach the equipment, encrypts the traffic and logs every connection.

Item	Description
Manufacturer	Xertified AB, Dragarbrunnsgatan 35, 753 20 Uppsala, Sweden. Org. no. 559211-3251
Product	XoT Technology: XoT-Lock, XoT-S1, XoT-Bridge, XMS (XoT Management System), XoT-Desktop Client, headless client, XoT-WebAccess
Part normally in or at the machine	XoT-Lock, on XoT-S1 hardware, on a Teltonika router or as software on an industrial PC
Software release	The release delivered with the machine. Release notes at docs.xertified.com
Intended purpose	Access control, encryption and logging of network traffic to and from the equipment behind the Lock
Not intended for	Carrying or replacing safety functions of the machine. The machine's safety functions must not depend on XoT

The Lock sits on the network path between the machine's control system and the customer's network. It does not change the control system's software, settings or addresses.

3. Architecture, components and deployment variants

Only the Lock is installed in or at the machine. The other parts run outside it, at a hosting partner, at the machine builder or at the customer.



Component	Where it runs	Role
XoT-Lock	In or next to the machine	Enforces the rules. Lets through only traffic that a rule and a valid ticket allow
XMS	Hosting partner, machine builder or customer	Holds users, devices and rules. Issues certificates and time-limited access tickets. Keeps the logs
XoT-Bridge	Hosting partner or machine builder	Relays encrypted traffic between client and Lock. Cannot read it
XoT-Desktop Client, XoT-WebAccess	The technician's computer or browser	Signs in with a certificate and opens the connection to the Lock

Variant of the Lock	Installation	Power and environment
XoT-S1 hardware	DIN rail in the control cabinet. Two Ethernet ports: one towards the equipment, one towards the network	5 V DC via USB-C. A 24 V DC adapter is available. Operating temperature -28 to 75 °C. No radio, no moving parts
Teltonika router	Software package in RutOS. Verified models at docs.xertified.com	As specified by Teltonika, which is the hardware manufacturer
Software	x86-64 or ARM64 industrial PC, or a virtual machine	As specified for the host

4. Network interfaces and data flows

The Lock opens only outbound connections. The customer's firewall needs no inbound rule for XoT. The ports and destinations for the outbound rules are listed at docs.xertified.com.

Flow	Direction from the Lock	Protection
Lock to XMS: settings, rules, tickets, logs	Outbound	TLS with certificates on both sides (mTLS)
Lock to XoT-Bridge: remote access traffic	Outbound	WireGuard encryption end to end between client and Lock. The Bridge cannot read it
Lock to another Lock: machine to machine	Outbound	WireGuard, with the same rules and tickets
Lock to the machine's control system	Local, on the protected side	Only the protocols, ports and directions a rule allows

All TCP and UDP protocols are expected to work through the Lock. Layer 2 protocols do not pass. Verified protocols are listed at docs.xertified.com.

Encryption through the Lock adds a small delay. Measured values are published at docs.xertified.com. Traffic with hard real-time requirements should be tested before it is routed through the Lock.

5. Security functions

Function	How XoT does it
Deny by default	The Lock drops all traffic that no rule allows and does not answer scans or ping
Identity	Every person and device has its own X.509 certificate from the XMS certificate authority or an external one. Keys can be held in a TPM, a smart card or a hardware key
Sign-in	Through the customer's or builder's identity provider, for example Entra ID, with multi-factor authentication. No passwords in XoT
Authorisation	Rules state who, what, where, when and how (protocol, port, direction). Access can require approval by another person; a requester cannot approve their own request
Time limit	Signed access tickets with a set validity. The tunnel closes when the ticket expires. Access can be revoked at once
Continuous check	Client and Lock re-authenticate each other inside the tunnel every 30 seconds
Encryption	WireGuard (Curve25519, ChaCha20-Poly1305, BLAKE2s). Not FIPS 140-validated
Logging	Event log of every connection (who, what, from where, when, how long). Audit log of every change to rules and permissions, protected against later modification. Kept up to 36 months; export to SIEM
Session recording	Sessions through XoT-WebAccess are recorded automatically

6. Behaviour on faults and effect on the machine

A fault in XoT stops network access through the Lock. It does not change the machine's control system. The builder decides in the risk assessment what the machine does when that access is lost.

Event	What happens
The Lock fails or loses power	Connections through it break. Redundancy: several Locks with traffic failing over between them
Configured failover in the Lock	A manual setting, made separately for each connection that needs it. Traffic to that device or IP address can then fall back to unencrypted traffic. It is a deliberate exception to the rules and must be part of the builder's risk assessment
XMS cannot be reached	Open connections continue while their tickets are valid. Locks keep enforcing rules on cached authorisation. No new access can be granted
XoT-Bridge cannot be reached	Remote access stops. Bridges can run in groups for redundancy
Software update of XoT-S1	Traffic through the Lock stops during the update and restart, a few minutes. An over-the-air update cannot leave XoT-S1 unusable. Updates are started from the XMS, so they can be planned for a production stop

XoT does not take part in the machine's safety functions. The builder should confirm that no safety function depends on traffic through the Lock.

7. Mapping to the Machinery Regulation and the CRA

XoT supports parts of the requirements below for network access to the machine. It does not cover what happens inside the control system.

Requirement	What XoT contributes	Not covered by XoT
MR Annex III 1.1.9, protection against corruption	Connecting another device or remote access goes through the Lock: only authorised, authenticated and logged access reaches the control system	Protection of the control system's own software, firmware and safety data
MR Annex III 1.2.1, safety and reliability of control systems	Reduces the network attack surface; traffic without a valid certificate and rule is dropped	The control system's own resistance to manipulation; the safety functions
CRA Annex I Part I 2(d), unauthorised access	Certificates, MFA via the identity provider, rules, approval, time limits	Local access at the machine, for example the HMI
CRA 2(e), confidentiality	WireGuard encryption in transit	Data at rest in the machine
CRA 2(f), integrity	Integrity of traffic in transit	Integrity of programs and data in the machine
CRA 2(j), limited attack surface	No inbound ports; equipment invisible to unauthorised parties	Other interfaces of the machine
CRA 2(k), reduced impact of incidents	Access limited per machine, revocable at once; traffic mirroring to intrusion detection	Recovery of the machine
CRA 2(l), recording of access	Event log and audit log, export to SIEM	Logging inside the control system
CRA 2(a) and 2(c), vulnerabilities and updates of the machine	Compensating control for equipment that cannot be patched	The machine's own vulnerability handling and updates

Letters refer to Annex I, Part I, point 2 of Regulation (EU) 2024/2847. Descriptions of requirements are simplified; the legal texts govern.

8. What the machine builder must assess

- Whether XoT is sufficient for the machine's risk assessment under EN ISO 12100 and the cybersecurity risk assessment under the CRA
- That no safety function depends on traffic through the Lock, and what the machine does when the Lock fails
- Whether a configured failover to unencrypted traffic is acceptable, and for which devices
- Which rules, users and approvers apply, and who runs the XMS and the Bridge
- Local interfaces of the machine that do not pass the Lock, such as the HMI and service ports
- The machine's own vulnerability handling, updates, SBOM and support period
- For machines already in the field: whether adding the Lock is a substantial modification
- Due diligence on XoT as a third-party component (CRA Article 13(5)), using the documents below

9. Regulatory status, support and documents

Topic	Status, October 2026
CE marking of XoT-S1	CE-marked. EMC tested to EN 55032:2015 Class B, EN 55035:2017, EN 61000-3-2:2014 and EN 61000-3-3:2013 at a DAkkS-accredited laboratory, December 2020
Low Voltage and Radio Equipment Directives	Do not apply to XoT-S1: 5 V DC, no radio
Machinery Regulation	Does not apply to XoT: it is not machinery
Cyber Resilience Act	Applies to Xertified as manufacturer. Our assessment: XoT-Lock and XMS are Annex III Class I. Reporting to ENISA in place since 11 September 2026; EU declaration of conformity under the CRA by 11 December 2027
IEC 62443	Development follows IEC 62443-4-1 practices and Microsoft SDL. Not certified; no level claimed
Support period	Five years for XoT-S1, XoT-Lock, XMS and the clients. One long-term release a year, with security updates for five years. Security updates are free of charge
Vulnerability reports	security@xertified.com, receipt confirmed within five working days

Available on request: Quality at Xertified, SBOM, penetration-test reports (under NDA), report of known issues, XMS logging and telemetry description, XoT-S1 EMC test report and EU declaration of conformity. Technical documentation, release notes and installation and hardening guides: docs.xertified.com.

Questions about this description or about fitting XoT to your machines: sales@xertified.com.