element

Element Materials Technology
6775 NE Evergreen Pkwy
Suite 400
Hillsboro, OR
97124, USA

P: 503 844 4066
contactus.enw@element.com
element.com

Software Questionnaire

Dear Applicants,

On July 23, 2024, the Federal Communications Commission (FCC) added Kaspersky Lab to the Covered List, designating them, and other related entities as entities that pose an unacceptable risk to the national security of the United States. In response to this development, the FCC has issued Public Notice DA-24-886A1 on September 3, 2024, providing guidance on the FCC's new requirements for all Applicants seeking equipment authorization.

Specifically, as outlined in Question 2a of KDB 986446 D01, Element Materials Technology is now requiring all Applicants to complete a Software Questionnaire as part of an application for equipment authorization. This questionnaire is designed to ensure that the equipment being certified does not contain any software or software components from entities that have been added to the Covered List, such as Kaspersky Lab.

The equipment authorization will be limited to equipment that does not contain software provided or produced by a company listed on the FCC Covered List. The applicant must implement software controls to ensure that authorized equipment continues to meet this requirement through the life of the product. FCC KDB 442812 D01 guides applicants that "third parties (end users, professional installers, and distributors) cannot have any ability to configure or operate transmitters...in any way that violates the approved certification."

It is important to note that this questionnaire will not be included in the submission package to the FCC but will be retained in Element Materials Technology's records associated with your FCC application. By implementing this new requirement, Element Materials Technology aims to strengthen the security and integrity of the equipment authorization process, protecting the national security interests of the United States.

We encourage all Applicants to carefully review the Public Notice to better understand the necessity of completing the Software Questionnaire as part of your application. If you have any questions or require further assistance, please do not hesitate to contact us.

Sincerely,
Jody House
Certification Manager
Element Materials Technology

Element Materials Technology
6775 NE Evergreen Pkwy
Suite 400
Hillsboro, OR
97124, USA

P: 503 844 4066
contactus.enw@element.com
element.com

Software Questionnaire

Declaration: In relationship to the product with the FCC ID listed below.	
FCC ID:	WP5TWN4F24
☐	The product hardware does not have the capability to install or operate software by any manufacturer, end-user, or third party.
☐	Product hardware has the capability to install software by the equipment manufacturer only at the time of manufacturing and is not updatable at any later time.
☒	Product hardware has the capability to install or operate software by: (select all that apply)
☒	the equipment manufacturer
☐	another entity in the supply chain
☒	end-users or other third parties

Questionnaire	
Please provide a detailed description of the cybersecurity and anti-virus software components integrated into the equipment for which you are seeking authorization. Specifically, address whether any of these components are produce or provided by Kaspersky Lab, Inc. or any of its subsidiaries and affiliates.	
Response:	The device in question does not include any integrated cybersecurity or anti-virus software components. It operates on a microcontroller without a traditional operating system and cannot host or execute third-party software beyond precompiled C applications specifically designed for its API. These applications are executed within a virtualized processor environment, and memory access is controlled by a firewall. No software or components developed, produced, or provided by Kaspersky Lab, Inc., or any of its subsidiaries and affiliates are integrated into the device. The device's architecture and security features (such as the optional "Device Security" feature that enforces signature-based app verification) are designed and implemented independently of any external software entities, ensuring compliance with the Covered List restrictions.
Explain the measures you have taken to ensure that the equipment does not include any Kaspersky Lab, Inc. cybersecurity or anti-virus software.	
Response:	The device's design ensures that no third-party cybersecurity or anti-virus software can be installed or executed. All firmware and software components are internally developed, with no involvement from Kaspersky Lab, Inc. Only user C-Skripts can be run on the device. For devices with "Device Security" enabled, only signed C applications are allowed, preventing unauthorized software. Additionally, the supply chain and components are verified to exclude any entities on the Covered List,

element

Element Materials Technology
6775 NE Evergreen Pkwy
Suite 400
Hillsboro, OR
97124, USA

P: 503 844 4066
contactus.enw@element.com
element.com

	including Kaspersky Lab.
Describe in detail the authentication protocols that are in place to ensure that the source of the software is valid. Describe in detail how the software is protected against modification and any encryption methods to support the use of legitimate software.	
Response:	The device uses a robust authentication protocol to ensure the validity of software sources. Specifically, the optional "Device Security" feature enforces the use of cryptographic signatures for all C applications. Only applications signed with a pre-approved, cryptographically secure signature are allowed to be executed on the device. This signing process uses industry-standard encryption algorithms to prevent tampering or forgery (AES_128bit). This is also true for the firmware, which is by standard encrypted and signed. Once an application is signed and loaded onto the device, the custom bootloader verifies the signature before execution. The device firmware itself is immutable and cannot be updated via external interfaces, ensuring that the authentication process remains secure. In addition, the device incorporates a memory firewall that continuously monitors and restricts unauthorized access to critical memory areas. This prevents any runtime modification of the application code or data. The user script itself runs on a virtualized processor that acts as a sanbox. Together, these measures ensure that only legitimate software can be executed, protecting the device from unauthorized modifications and ensuring compliance with security standards.
Describe in detail the process you have in place to continuously monitor for and remove any Kaspersky Labs, Inc. cybersecurity or anti-virus software that may be inadvertently integrated in the equipment during the manufacturing or supply-chain process.	
Response:	The device manufacturing and development processes include rigorous controls to prevent the inadvertent integration of any Kaspersky Lab, Inc. cybersecurity or anti-virus software. Internal Development Protocols: The firmware and software are developed entirely in-house, with no reliance on third-party software libraries, components, or services that could introduce prohibited software. Code Integrity Checks: The development process incorporates automated tools and manual reviews to continuously monitor for any unauthorized software or dependencies that may inadvertently enter the codebase. These measures collectively ensure that the risk of integrating any

element

Element Materials Technology
6775 NE Evergreen Pkwy
Suite 400
Hillsboro, OR
97124, USA

P: 503 844 4066
contactus.enw@element.com
element.com

	Kaspersky Lab software is effectively mitigated and promptly addressed if detected.
Describe how any software updates will be obtained, downloaded, validated and installed. For software that is accessed through the manufacturer's software or device's management system, describe the different levels of security as appropriate.	
Response:	Validation: Before installation, the device verifies the cryptographic signature of the application. If the signature does not match the authorized key, the update is rejected. Installation: Once validated, the application is securely installed using the device's API. If "Device Security" is enabled, only applications with the correct signature can replace existing applications. Security Levels: The system architecture ensures that no unauthorized software can be installed. Additionally, the lack of an internet connection or other public network interfaces eliminates remote exploitation risks. These mechanisms provide robust protection against unauthorized updates while ensuring only legitimate, validated software can be installed on the device.
Explain if any third parties have the capability to operate a U.S. device on any other regulatory domain, or in any manner that may allow the device to operate in violation of the device's authorization if activated in the U.S.	
Response:	No third parties have the capability to operate the device outside of its authorized regulatory domain or in a manner that would violate its U.S. authorization. The Device Security feature ensures that only applications signed with a valid, cryptographically secure signature can be installed or executed on the device. This signature-based validation mechanism prevents any unauthorized software from being loaded, making it impossible for third parties to bypass regulatory controls or alter the device's operation.
Is the country code factory set? Can it be changed in the user interface? If it can be change, what controls exist to ensure that the device can only operate within its authorization in the U.S.?	
Response:	No, it is not.
What are the default parameters when the device is restarted?	

Element Materials Technology
6775 NE Evergreen Pkwy
Suite 400
Hillsboro, OR
97124, USA

P: 503 844 4066
contactus.enw@element.com
element.com

Response:	When the device is restarted, it is initialized to a default state where: Hardware Reset: The hardware is returned to a standard configuration. All inputs and outputs are pulled to ground, and internal buses are initialized to ensure proper functionality. Firmware Integrity: The device checks for any tampering or unauthorized modifications to its firmware or software components. The device will only boot if all components pass validation. Security Features: The Device Security feature is enabled, ensuring that only authorized, signed applications can be loaded. Device State: Connected devices are polled and checked to ensure they are functioning properly, and the virtualized processor is initialized to begin executing the user script. These default parameters ensure that the device starts in a secure and controlled environment, with all necessary components validated and functioning as expected.
For radio equipment that requires software installation onto third party or host equipment, what controls are in place to ensure installed software is compliant with the U.S. requirements?	
Response:	Since it is not necessary to install software on another device, the device operates independently without requiring any third-party or host equipment for software installation. All software, including C-Skripts, is precompiled and directly executed on the device.

Name:	Birgit Bachl
Title:	International Compliance
Signature:	ELATEC RFID Systems Elatec GmbH • Zeppelinstr. 1 • 82178 Puchheim • Germany Phone: +49 89 5529961 0 • Fax: +49 89 5529961 129 info-RFID@elatec.com • www.Elatec-RFID.com
Phone:	+49 89 552 9961 0
Email:	b.bachl@elatec.com
Date:	12.03.2025