PQC-Route

Security Target

v0.5

29/04/2026

Created by







Version control

Version	Comment	Date
0.1	Initial draft version	04/08/2025
0.2	Changes after ISDEFE comments	29/08/2025
0.3	Changes after Laboratory testing	19/02/2026
0.4	TOE version updated	06/03/2026
0.5	Changes in IAU.2 and IAU.3 requirements	29/04/2026

Table of contents

1 Introduction 4

1.1 Applicant, TOE and evaluation information 4

1.2 Methodology and evaluation criteria 5

2 TOE description 6

2.1 TOE Functional description 6

2.2 Identification of the TOE secure use, installation and configuration guides 8

2.3 TOE usage description 9

2.3.1 PQC-Link 9

2.3.2 PQC-Core 9

2.3.3 PQC-Host 11

2.3.4 TOE version checking 11

2.3.5 TOE update process 12

2.3.6 Audit logs checking 13

3 Operational environment 15

3.1 Operational environment description 15

4 Security Problem Definition 16

4.1 Operational Environment Assumptions 16

4.2 Assets to protect 17

4.3 Threat descriptions 18

4.3.1 Traceability threats/security requirements 19

5 Security Functional Requirements 20

5.1 SF. Trusted Administration 21

5.2 SF. Identification and authentication 22

5.3 SF. Trusted Communication Channels 23

5.4 SF. Protection of credentials and sensitive data 24

5.5 SF. Audit 25

5.6 SF. Trusted installation and updates 26

5.7 SF. Anti-exploitation capabilities 27

5.8 SF. Cryptography 28

5.9 SF. Connection requirements 29

6 Acronyms 30

7 Document references 31

8 Annex 32

8.1 Third party libraries used by the TOE 32

1 Introduction

This document is the Security Target for **PQC-Route**. This document includes the following information:

1. Information about this document.
2. Description of the functionality of the solution and use cases, which allows organizations or public services to address the threats and risks described in the document.
3. Description of the execution environment.
4. Threat and risk analysis of the product.
5. Fundamental security requirements covered by this solution and how they are covered to implement each security function.
6. Acronyms, Glossary of terms and Document references.

1.1 Applicant, TOE and evaluation information

Applicant data	MUMKEN S.L
Developer data	MUMKEN S.L
Contact information of developer	Avenida de Manoteras 24, Planta 2, 28050, Madrid Javier Bermúdez Pérez javier.bermudez@mumken.es +34 658926158
TOE name	PQC-Route
TOE version	2.5.5.0
Evaluation type	LINCE
User guidance and version	See *2.2: Identification of the TOE secure use, installation and configuration guides*
Taxonomy according to CCN-STIC-140	N/A

1.2 Methodology and evaluation criteria

CCN-STIC-2001	Definición de la Certificación Nacional Esencial de Seguridad marzo 2022 versión 2.0 (National Essential Security Certification Definition, March 2022 version 2.0).
CCN-STIC-2002	Metodología de Evaluación para la Certificación Nacional Esencial de Seguridad marzo 2022 versión 2.0 (Evaluation Methodology for National Essential Security Certification March 2022 version 2.0).
CCN-STIC-2003	Plantilla para la Declaración de Seguridad de la Certificación Nacional Esencial de Seguridad marzo 2022 versión 2.0 (Security Target template for National Essential Security Certification March 2022 version 2.0).

2 TOE description

2.1 TOE Functional description

The TOE is a composite software solution designed to facilitate secure connectivity to assets located within remote networks. Access to these assets is governed by the TOE with configurable access control policies that map specific user groups to corresponding remote network access. Furthermore, the TOE supports the enforcement of administrative approval workflows for time-bound access to remote network assets. It also provides the capability to define persistent IP-based blacklists to restrict unauthorized access attempts.

As previously mentioned, the TOE is a composite solution which is broken into the following components:

- **PQC-Link**. It is a software which acts as intermediate between the users and the assets from the remote network. This component receives two initial connections via mTLS v1.3, one from PQC-Core (users) and one from PQC-Host (agent installed on a remote network where the assets are located). Through these channels, PQC-Link will forward the communication between PQC-Core and PQC-Host.
- **PQC-Core**. It is a software client which offers a local interface which allows to establish connections to the remote network assets based on the access control policies defined by the administrator users. In addition, it allows to perform different management functionalities as create/edit/delete users, user groups, hosts or routes, authorize connections or add IP addresses to a permanent blacklist based on the user role assigned to each authorized user.
- **PQC-Host**. It is a software agent which allows the connection to the assets from the remote network. It forwards the connection request from PQC-Core (through PQC-Link) to the asset which the user wants to access.

The following figure illustrates the TOE:

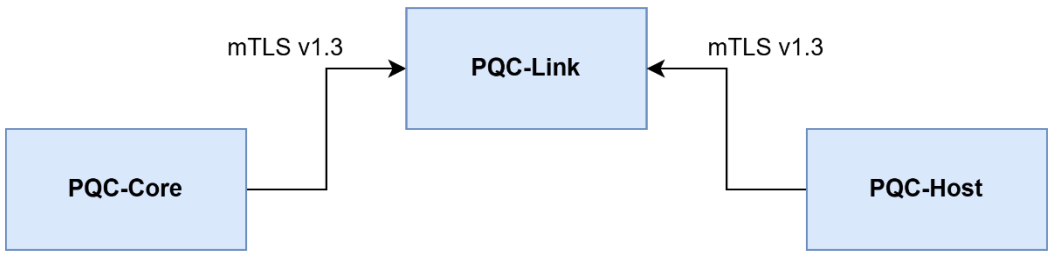


Figure 1: TOE architecture

The TOE provides the following security functionalities:

- **SF. Trusted administration**. The TOE allows users with the roles of *SuperAdministrator* and *Administrator* to perform different management functionalities through the PQC-Core local interface.
- **SF. Identification and authentication**. The TOE identifies and authenticates each user before granting access to the PQC-Core local interface (except for the functionalities related to PQC-Link configuration and Proxy IP addresses configuration), blocking users in case of multiples

invalid login attempts to prevent brute force attacks. All user passwords must complain with a password policy and the user sessions will be closed after a certain period of inactivity.

- **SF. Trusted communication channels**. The TOE establishes secure communications channels while exchanging sensible information through mTLS v1.3 and SMTP over TLS v1.3.
- **SF. Protection of credentials and sensitive data**. The TOE makes use of cryptographic algorithms authorized by the CCN to protect user passwords and private keys.
- **SF. Audit**. The TOE generates audit records when different events occur, and all these events contain information related with date and time of the event, type, outcome and the user (if it is applicable). The TOE sends the audit records to the MySQL database from the operational environment as they occur.
- **SF. Trusted installation and updates**. The TOE offers the possibility to check the current version.
- **SF. Anti-exploitation capabilities**. The TOE does not request the allocation of any explicit system memory address or the allocation of memory with simultaneous write and execute permissions.
- **SF. Cryptography**. The TOE uses secure cryptographic mechanisms authorized by the CCN for HIGH ENS category.
- **SF. Connection requirements**. The TOE allows users to access assets from the remote network, based on an access control policy previously established. In addition, the TOE allows to establish that administrator authorization is required to access the assets from the remote network.

2.2 Identification of the TOE secure use, installation and configuration guides

The following table lists the documents and user's guides necessary to carry out the configuration of the TOE properly:

Document's type	Document's name	Document's version (update-history-date)
Installation guide	PQC Core Install Manual	2.5.5.0 SHA-256: D8751B4E81FCF0468E18EB2E9E014E1B52B1E4DD7DFAD7401D86A520243356D0
User manual	PQC Core User manual	2.5.5.0 SHA-256: D16536789FB942C5DD656B4BCE3F046A4370881364DF068D18BAD085441A5F4E
Installation guide	PQC Host Windows Install manual	2.5.5.0 SHA-256: 71F5FD5DA124F75408736A488BF66D81A25BAEB2AB908C6F6BF7ACE930836D38
Installation guide	PQC Link Windows Install manual	2.5.5.0 SHA-256: 36D866241AB62B343BD21E6CD388B8A5084318C7536373B206F61EDAAAD2F6F8

2.3 TOE usage description

In order to fulfil the functions described in section *5 Security Functional Requirements* of this document, the following considerations must be taken into account.

Each TOE component must be installed on a Windows 11 host version 24H2, with build 26100.4351. Additionally, the TOE could be installed over other operating systems as defined in the different Installation guides included in section 2.2, but such operating systems are not included under the scope of the evaluation.

Each component must be installed individually on a separate host from the others. They are delivered in MSI format, and these MSI files must be executed to install/uninstall the different components.

2.3.1 PQC-Link

Installation

Follow *PQC Link Install manual* guide to install PQC-Link component. It must be installed with administration permissions of the underlying OS.

This TOE component shall be started in console mode. Refer section *8 Application start* from *PQC Link Windows Install manual* guide for more details.

This component offers two local interfaces which can be accessed executing the following executable files with administration permissions of the underlying OS: "Mumken.pqcRoute.LicenseManager.Link.exe" and "Mumken.pqcRoute.Link.Configurator.exe".

Both executable files offer a local interface which allows to perform the following post-installation task. However, this TOE component does not implement users nor requires a login. It leverages the identification, authentication and user management on the underlying OS. Therefore, all platform administrator users are able to access these local interfaces.

License request and upload. Follow section *5 PQC-Link Licensing* from *PQC Link Windows Install manual* guide to generate a license request file which shall be provided to the manufacturer or distributor, and to upload the license once the manufacturer provides it.

Certificate store configuration. The manufacturer will generate and provide by email a unique PQC-Link certificate and private key in PKCS #12 format (named as "Link.pqc"). The platform administrator must include this file into *c:\Program Files\Mumken\Mumken.pqcRoute.Link* directory.

The TOE does not offer the possibility to change this certificate.

PQC-Link configuration. Follow section *6 PQC-Link Configuration* from *PQC Link Windows Install manual* guide to configure the component. The configuration must be performed as specified in the guide, and no additional parameters or fields must be enabled, disabled or modified (enabling and using a Tor Filter is not included under the scope of the evaluation).

Mail sender configuration. Follow section *6.4 Mail sender* from *PQC Link Windows Install manual* guide to configure the sending of emails to users when a connection needs to be authorised.

2.3.2 PQC-Core

Installation

Follow *PQC Core Install Manual* guide to install PQC-Core component. It must be installed with administration permissions of the underlying OS.

In addition, perform the following post-installation tasks.

PQC-Core configuration. Follow section *6 PQC-Core Configuration* from *PQC Core Install Manual* guide to configure the connection to the PQC-Link.

First-time login. Follow section *7 First-Time Access to the Application* from *PQC Core Install Manual* guide to perform the necessary steps when login into the TOE for the first time. The keys storehouse file of the first user must be provided by the manufacturer.

Companies management. Follow section *9 Companies* from *PQC Core User manual* guide to create, edit and delete companies. At least, one company must be created by an administrator with SuperAdministrator role.

Groups management. Follow section *10 Groups* from *PQC Core User manual* guide to create, edit and delete user groups. At least, one user group shall be created.

Users management. Follow section *11 Users* from *PQC Core User manual* guide to create, edit and delete users, issue new user certificates, restrict routes and force logout.

Users must be created assigning them 30 minutes of Inactivity Timeout and Session Timeout. It shall be checked that the user with SuperAdministrator role created in the installation is configured by default with 30 minutes of Inactivity Timeout and Session Timeout. The TOE does not allow to configure these parameters for the SuperAdministrator user.

In addition, the administrator (with Administrator or SuperAdministrator role) must issue a new certificate for each new user and provide to the user the secure keys store created (PKCS #12 file).

The TOE does not offer the possibility to assign the SuperAdministrator role to any user. There is only a user called *root* with this role and its credentials are provided by the manufacturer. As specified in section *7.3 First-Time Access with a New User* from *PQC Core Install Manual* guide, the TOE forces to change the password after the first login. In addition, the manufacturer will generate and provide by email a unique PQC-Core certificate and private key in PKCS #12 format for the SuperAdministrator user. The TOE does not offer the possibility to change this certificate.

The TOE offers the possibility to assign routes to users. First, each user shall be included into a user group, and the user group shall be assigned to a PQC-Host. After it, the routes already created for the PQC-Host may be assigned to the users of the group. Follow section *11.3.3 Restrict routes* from *PQC Core User manual* guide for more details.

Hosts management. Follow section *12 Host* from *PQC Core User manual* guide to create, edit and delete host, issue new hosts certificates, download Hosts PQC Store (download the PQC-Host certificate and private key in PKCS#12 format) and disable hosts. At least, one host must be created and associated to a user group.

The administrator (with Administrator or SuperAdministrator role) must issue a new certificate for each new host and upload the secure keys store created in the respective PQC-Host.

Routes management and launch. Follow section *13 Routes* from *PQC Core User manual* guide to create, edit, delete and launch routes, and request authorization to access a route.

The option “Connection timeout” shall be configured to 1 hour.

The options “Allow any connection” and “Require Core Client Authentication” must not be enabled.

Authorizations. Follow section *17 Authorizations* from *PQC Core User manual* guide to enable or disable authorizations to access a host. Only the administrator user specified when creating the host will be able to enable or disable the authorization requests. No authorization request must be accepted if the requested time is higher than 1 hour.

Launchers allowed. Follow section *19 Launchers allowed* from *PQC Core User manual* guide to create, edit and delete launchers allowed.

Installers. Follow section *21 Installers* from *PQC Core User manual* guide to import the TOE installer file and new version installer files.

Blacklist. Follow section *23 Black List* from *PQC Core User manual* guide to add, edit and delete IP addresses to the permanent blacklist.

2.3.3 PQC-Host

Follow *PQC Host Windows Install manual* guide to install PQC-Host component. It must be installed with administration permissions of the underlying OS.

This component offers a local interface which can be accessed executing the following executable file with administration permissions of the underlying OS: “Mumken.pqcRoute.Host.exe”.

This executable file offers a local interface which allows to perform the following post-installation task. However, this TOE component does not implement users nor requires a login. It leverages the identification, authentication and user management on the underlying OS. Therefore, all platform administrator users are able to access this local interface.

License request and upload. Follow section *5 Licensing* from *PQC Host Windows Install manual* guide to generate a license request file which shall be provided to the manufacturer or distributor, and to upload the license once the manufacturer provides it.

Certificate store. Follow section *6 Certificate store distribution* from *PQC Host Windows Install manual* guide to import the certificate store (PKCS #12 file) created during the PQC-Core installation and configuration processes.

PQC-Host configuration. Follow section *8 PQC-Host configuration* from *PQC Host Windows Install manual* guide to configure the component. The use of a proxy by the TOE is not included under the scope of the evaluation and, therefore, no proxy address and port shall be configured.

2.3.4 TOE version checking

As defined previously, the TOE is a solution composed of three parts which have the same version. Therefore, the TOE version is 2.5.5.0 as the particular version of PQC-Link, PQC-Core and PQC-Host is 2.5.5.0.

Follow the next steps to check the current version for each TOE component.

PQC-Link. Access *About* tab from the local PQC-Core interface to check the current PQC-Link version.

PQC-Core. Access *About* tab from the local PQC-Core interface as described in section *24 About* from *PQC Core User manual* guide to check the current PQC-Core version.

PQC-Host. Access *About* tab from the local Host interface to check the current PQC-Host version. In addition, it can be consulted by accessing *Host* tab from the local PQC-Core interface and check the value of *Version* column to check the current PQC-Host version.

2.3.5 TOE update process

When a new version of the TOE components is released, the manufacturer will provide the update installer packages to the SuperAdministrator by email. In particular, the manufacturer provides an MSI file for PQC-Link, and two PKCS #7 files with ".ins" extension, one for PQC-Core and one for PQC-Host.

The update files for PQC-Core and PQC-Host provided in ".ins" format are signed with both ML-DSA-87, and ECDSA with P-521 (R) elliptic curve and SHA-512 (R). This digital signature is checked during the importation process as described below.

The MSI installation files for the different TOE components are signed with ECDSA using P-521 and SHA-512, and this digital signature is checked by the underlying OS prior installing.

Regarding the PQC-Link update installation, the MSI installation file must be executed by the Platform Administrator on the platform where it is installed.

Regarding the PQC-Core and PQC-Host update installations, the TOE administrator must import both files to the TOE through the local Core interface as section *21 Installers* from *PQC Core User manual* guide states.

When the packages are uploaded, PQC-Core sends them to PQC-Link over the mTLS v1.3 channel described in COM.1 once the ML-DSA-87 and ECDSA digital signatures are checked. Once PQC-Link receives the packages, it checks the digital signatures again and sends the packages to the MySQL database of the operational environment where they will be stored.

If a TOE administrator needs to download the installation packages, the package must be selected in *Installers* tab from the local PQC-Core interface, perform a right-click and click on *Download*. The instruction is sent by PQC-Core to PQC-Link, and the PQC-Link obtains the installer from the MySQL database of the operational environment. The installer file will be provided in MSI format, only if the PQC-Link validates the ML-DSA-87 and ECDSA digital signatures when receiving the package from the MySQL database.

Once this process is successfully completed, the TOE administrator will obtain the MSI installer files, and they must be executed by a Platform Administrator in the respective platform.

When the installer files are executed by the Platform Administrator (for the three TOE components), the digital signature generated with ECDSA using P-512 and SHA-512 is checked by the underlying operating system. If the signature is correct, the TOE will be uninstalled and the new version will be installed.

Regarding new versions available, the TOE does not offer the possibility to check if new PQC-Host and PQC-Link are available. Regarding new PQC-Core versions available, the TOE allows the possibility to check if new updates are available as described in section *24 About* from *PQC Core User manual* guide. However, the TOE will only confirm that there is a new PQC-Core version available if an administrator has imported a new PQC-Core version to the TOE.

2.3.6 Audit logs checking

All audit logs are stored in the MySQL database from the operational environment and they have to be consulted by accessing this database, as explained in this section.

Access to *AuditData* table and consult the following records regarding the events included in **AUD.1** requirement:

- **Login attempts**. Consult *SESSION INIT* records.
- **Logout**. Consult *SESSION FINISH* records.
- **Changes in user credentials**. Consult *CHANGE CREDENTIALS* records.
- **Create, edit and delete companies**. Consult *CREATE COMPANY*, *MODIFY COMPANY* and *DELETE COMPANY* records.
- **Create, edit and delete users**. Consult *CREATE USER*, *MODIFY USER* and *DELETE USER* records.
- **Configuration of the inactivity timeout for each user**. Consult *INACTIVITY TIMEOUT CHANGED* records.
- **Configuration of the session timeout for each user**. Consult *SESSION TIMEOUT CHANGED* records.
- **Create, edit and delete user groups**. Consult *CREATE GROUP*, *MODIFY GROUP* and *DELETE GROUP* records.
- **Create, edit, delete and disable hosts**. Consult *CREATE HOST*, *MODIFY HOST* and *DELETE HOST* records.
- **Create, edit and delete routes**. Consult *CREATE ROUTE*, *MODIFY ROUTE* and *DELETE ROUTE* records.
- **Create, edit and delete allowed launchers**. Consult *CREATE LAUNCHER ALLOWED*, *MODIFY LAUNCHER ALLOWED* and *DELETE LAUNCHER ALLOWED* records.
- **Issue new user certificates**. Consult *ISSUE USER CERTIFICATE* records.
- **Issue new host certificates**. Consult *ISSUE HOST CERTIFICATE* records.
- **Download Hosts PQC Stores**. Consult *DOWNLOAD PQC STORE HOST* records.
- **Enable hosts**. Consult *ENABLE HOST* records.
- **Disable hosts**. Consult *DISABLE HOST* records.
- **Restrict routes**. Consult *RESTRICT ROUTE* records.
- **Force user logout**. Consult *FORCE LOGOUT* records.
- **Force session logout**. Consult *FORCE SESSION LOGOUT* records.
- **Import host licenses**. Consult *IMPORT LICENSE* records.
- **Import installers**. Consult *IMPORT INSTALLER* records.
- **Connections to host**. Consult *CONNECTION TO ROUTE* records.

Apart from these considerations, the TOE does not require any other pre-configuration or particular usage to obtain the security features described in section 5 Security Functional Requirements of this document beyond the TOE guide's steps.

3 Operational environment

3.1 Operational environment description

The figure below shows the operational environment:

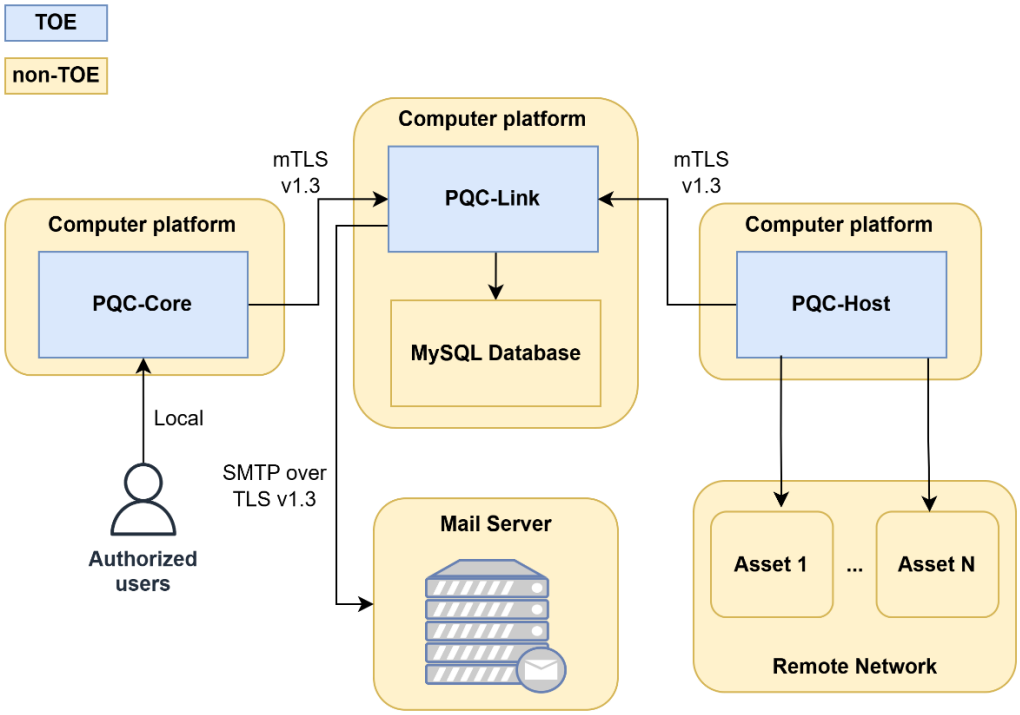


Figure 2: Operational environment

The main entities that compose the operational environment are described below:

- **Authorized users**. These users can access to the PQC-Core local interface (including administrators and users without administrative privileges) and perform the different management functionalities based on the assigned user role.
- **Computer platform**. It corresponds to the platforms where the TOE components may be installed. In particular, the underlying operating system for the three platforms shall be Windows 11 host version 24H2, with build 26100.4351.
- **MySQL database**. It is a database to which the PQC-Link will connect to transmit and obtain data. All user passwords and audit records are stored in this database. A MySQL database with version 8.0.42 must be installed in the same platform in which the PQC-Link is installed.
- **Remote Network**. It corresponds to the corporative network where the different assets are located, to be accessed by the authorized users. The PQC-Host must have a network interface in this network.
- **Assets**. It corresponds to the different services to which the authorized users access using the TOE.
- **Mail server**. It corresponds to a mail server installed and maintained by the customer, which will receive mails from PQC-Link when a connection needs to be authorised by the administrator.

4 Security Problem Definition

4.1 Operational Environment Assumptions

Assumption	Description
A.PHYSICAL PROTECTION	The product must be installed in an area where access is only possible for authorized personnel and with suitable environmental conditions.
A.TRUSTED ADMINISTRATION	Administrators shall be members of the organization who are fully trusted and have the best security interests for the organization. They shall be properly trained and shall be free of any malicious intent or conflict of interest in managing the TOE.
A.PROTECTION OF THE CREDENTIALS	All credentials, especially the administrator's, must be properly protected by the organization using the TOE.
A.TRUSTED PLATFORM	The TOE shall run on a trusted platform, including the operating system or any runtime environment on which it is used, and the internal communications.
A.PERIODIC UPDATES	The software of the TOE is updated when new updates that fix known vulnerabilities appear.
A.TRUSTED PLATFORM ADMINISTRATOR	Administrators of the platforms where the different TOE components run shall be members of the organization who are fully trusted and have the best security interests for the organization. They shall be properly trained and shall be free of any malicious intent or conflict of interest in managing the TOE environment.

4.2 Assets to protect

This section describes the assets that the TOE's security features protect.

Asset	Description	Security Dimensions
AS.ADMINISTRATION	Product management interfaces and the information transmitted through them, in both directions.	Confidentiality, Authenticity and Integrity.
AS.COMMUNICATIONS	TOE's communications, established between its own components.	Confidentiality, Integrity and Authenticity.
AS.UPDATES	Updates that may affect TOE's configuration and functionality.	Integrity and Authenticity.
AS.PSS CONF	Configuration data.	Integrity and Traceability.
AS.PSS AUD	Audit records of the TOE.	Integrity.
AS.PSC	User credentials, assets credentials and private keys.	Confidentiality and Integrity.
AS.REMOTE ASSETS	Connections to the remote network assets.	Confidentiality and Authenticity.

4.3 Threat descriptions

Threat	Description	Assets
T.NOAUT - UNAUTHORIZED USER ACCESS	An attacker can gain access as a product administrator or user by one of the following scenarios: • Impersonating as an administrator to the product. • Impersonating as the product to an administrator. • Replaying an administration session. • Performing man-in-the-middle attacks.	*AS.ADMINISTRATION* *AS.PSS CONF* *AS.PSS AUD* *AS.PSC* *AS.REMOTE ASSETS*
T.CRYPTO - WEAK CRYPTOGRAPHIC MECHANISMS	Use of weak cryptographic mechanisms or weak key lengths in the product that allow an attacker to compromise it, primarily through brute force attacks.	*AS.ADMINISTRATION* *AS.PSC* *AS.COMMUNICATIONS* *AS.UPDATES*
T.COM - UNAUTHORIZED COMMUNICATION PROTOCOLS	Use of unauthorized protocols that allow an attacker to compromise the integrity, authenticity and confidentiality of critical product communications.	*AS.COMMUNICATIONS* *AS.ADMINISTRATION*
T.ACT - MALICIOUS UPDATE	An attacker can perform a malicious update that weakens the product's security features.	*AS.UPDATES*
T.UNAC - UNDETECTED ACTIVITIES	An attacker may attempt to access, change or modify the product's security functionality without the administrator's knowledge.	*AS.PSS CONF*
T.AUD – AUDIT INTEGRITY COMPROMISE	An attacker may attempt to change or delete the audit data.	*AS.PSS AUD*
T.INT - SOFTWARE INTEGRITY COMPROMISE	An attacker may attempt to compromise the integrity of the product through unprivileged software running on the same platform on which the product is running.	*AS.ADMINISTRATION* *AS.COMMUNICATIONS* *AS.UPDATES* *AS.PSS CONF* *AS.PSS AUD* *AS.PSC* *AS.REMOTE_ASSETS*
T.PSC - COMPROMISE OF CRITICAL SECURITY PARAMETERS	An attacker may compromise credentials and private keys to continuously access the product and its critical data.	*AS.PSC*
T.NOASSETAUT - UNAUTHORIZED ASSET ACCESS	An attacker can gain access to the assets from the remote network for which it is not authorized.	*AS.REMOTE ASSETS*

4.3.1 Traceability threats/security requirements

The following table maps the Fundamental Security Requirements defined in section *5: Security Functional Requirements* that address the defined threats:

	T.NOAUT	T.CRYPTO	T.COM	T.ACT	T.UNAC	T.AUD	T.INT	T.PSC	T.NOASSETAUT
ADM	X								
IAU	X							X	
COM	X	X	X						
ACT		X		X					
AUD					X	X			
EXP							X		
PSC		X						X	
CIF	X	X	X	X				X	
CON									X

5 Security Functional Requirements

Regarding the cryptographic material listed in this section, the following nomenclature is considered:

- ***Recommended (R)***: refers to the cryptographic algorithms that are considered secure and suitable in the long term even considering the increase in computing power expected in the coming years.
- ***Legacy (L)***: refers to the cryptographic algorithms, that are considered with acceptable security in the short term, due to current computational power and that expected in the coming years.

5.1 SF. Trusted Administration

Requirement	Description
ADM.1	The TOE shall define the **SuperAdministrator** and **Administrator** roles as administrator roles and **User** role as non-administrator role. In addition, the TOE shall be able to associate roles to users excluding SuperAdministrator role.
ADM.2	The TOE shall allow to locally perform the following management functionalities through PQC-Core local interface: • Create, edit and delete companies. • Create, edit and delete users. • Configuration of the inactivity timeout for each user. • Configuration of the session timeout for each user. • Create, edit and delete user groups. • Create, edit and delete hosts. • Create, edit and delete routes. • Create and delete allowed launchers. • Issue new user certificates and private keys. • Issue new host certificates and private keys. • Download Hosts PQC Stores. • Enable and disable hosts. • Restrict routes. • Force user logout. • Force session logout. • Import host licenses. • Import installers.
ADM.3	The TOE shall ensure that users with **SuperAdministrator** role assigned are able to perform all the functionalities described in **ADM.2**. The TOE shall ensure that users with **Administrator** role assigned are able to perform all the functionalities described in **ADM.2** excluding *create, edit and delete companies*.

5.2 SF. Identification and authentication

Requirement	Description
IAU.1	The TOE shall identify and authenticate each user before granting access to the PQC-Core local interface, except for the functionalities related to PQC-Link configuration and Proxy IP addresses configuration.
IAU.2	The TOE shall block users after 3 invalid login attempts when introducing the user password through PQC-Core local interface within 5 minutes for 5 minutes. After 3 sets of 3 invalid login attempts, the TOE shall block users permanently.
IAU.3	The TOE shall enforce the following passwords policy for PQC-Core local interface users: • The password shall be configurable with a minimum or equal length of 12 characters and 16 characters as maximum length. • The password shall be able to be composed of lowercase vowels, lowercase consonants, uppercase vowels, uppercase consonants, numbers and special characters ["!", "@", "#", "$", "%", "^", "&", "*", "(", ")"].
IAU.4	The TOE shall close the user sessions after 30 minutes of inactivity in PQC-Core local interface.
IAU.5	When access is made using the password established by the administrator through PQC-Core local interface, the TOE shall force the change of credentials on the next access.

5.3 SF. Trusted Communication Channels

Requirement	Description

COM.1	The TOE shall establish the following secure channels when exchanging sensitive information with authorized entities or between different parts of the product:
	• PQC-Core communicates with PQC-Link via mTLS v1.3.
	• PQC-Host communicates with PQC-Link via mTLS v1.3.
	• PQC-Link communicates with SMTP server via SMTP over TLS v1.3.
	
	For the previously mentioned mTLS v1.3 communications, all the TOE components shall use the following cryptographic mechanisms, authorized by the CCN for ENS HIGH Category:
	• TLS_AES_256_GCM_SHA384 (R) cipher suite.
	• ECDHE as key exchange method, using P-521 (R) elliptic curve.
	
	For the previously mentioned SMTP over TLS v1.3 communication, PQC-Link shall use the following cryptographic mechanisms, authorized by the CCN for ENS HIGH Category:
	• TLS v1.3 cipher suites:
	  ○ TLS_AES_256_GCM_SHA384 (R)
	• DHE and ECDHE as key exchange methods, using the following mechanisms:
	  ○ ffdhe4096 (R)
	  ○ P-384 (R)
	  ○ P-521 (R)
	  ○ BrainpoolP384r1tls13(R)
	  ○ BrainpoolP512r1tls13 (R)

COM.2	The TOE shall only establish the following communication channels and no other than the following: • **COM.1** communications. • **PQC-Link** with **MySQL database**.
COM.3	The TOE shall make use of ECDSA with P-521 (R) elliptic curve and SHA-512 (R) digital certificates for authentication when communicating via mTLS v1.3 as defined in **COM.1**.

5.4 SF. Protection of credentials and sensitive data

Requirement	Description
PSC.1	PQC-Link shall protect the user passwords using PBKDF2 (R) with HMAC-SHA-512 (R) using 4096 iterations and a 192-bits salt, and send them to the MySQL database from the operational environment, which will store them. The TOE shall make use of private keys stored in PKCS12 (.p12) files encrypted with AES-256-CBC (R), with a key derived from a password known to each user and not stored in the TOE with PBKDF2 (R) with HMAC-SHA-512 (R) using 4096 iterations and a 192-bits salt.

5.5 SF. Audit

Requirement	Description
AUD.1	The TOE shall generate audit records when any of the following events occur: • Login and logout of registered users. • Changes in user credentials. • Changes in product configurations as defined in **ADM.2**. • Events related with TOE functionality: successful connections to remote network assets.
AUD.2	Audit records shall contain at least the following information: • Date and time of the event. • Type of identified event. • Result of the event. • User producing the event (if applicable).
AUD.4	PQC-Link shall transmit the generated audit information to the MySQL database from the operational environment.
AUD.5	PQC-Link shall send the logs to the MySQL database from the operational environment as they occur.

5.6 SF. Trusted installation and updates

Requirement	Description
ACT.1	PQC-Core shall provide the ability to query the current version of PQC-Core and PQC-Link components. In addition, PQC-Host shall provide the ability to query its current version.
ACT.2	PQC-Core and PQC-Link shall authenticate the PQC-Core and PQC-Host update packages (*.ins* files) when they are imported via PQC-Core local interface using both ML-DSA-87 (R) and ECDSA with P-521 (R) elliptic curve and SHA-512 (R). In addition, PQC-Link shall also authenticate the PQC-Core and PQC-Host update packages (*.ins* files) when they are downloaded from the PQC-Core local interface using both ML-DSA-87 (R) and ECDSA with P-521 (R) elliptic curve and SHA-512 (R). The TOE installation packages shall be digitally signed with ECDSA with P-521 (R) elliptic curve and SHA-512 (R) such that the platform can cryptographically verify them before installation.
ACT.4	The TOE shall be packaged in such a way that, if removed, it leaves no trace of its installation (except for configurations, certificate store, license or audit files).
ACT.5	The TOE shall not download or modify its own binary code.

5.7 SF. Anti-exploitation capabilities

Requirement	Description
EXP.1	When the TOE is running, it shall not request the allocation of any explicit system memory address, nor shall it allocate memory with simultaneous write and execute permissions.
EXP.2	The TOE shall be configured by default with file permissions that protect it from unauthorized access.

5.8 SF. Cryptography

Requirement	Description
CIF.1	The TOE shall use the following cryptographic mechanisms authorized by the CCN for ENS HIGH Category: • Cipher suites and cryptographic algorithms of the communication channels defined in **COM.1**. • The certificates used for authentication as specified in **COM.3**. • The hash and encryption algorithms used by the TOE to protect the private keys used in the **COM.1** communications and user passwords, as defined in **PSC.1**. In addition, the TOE shall invoke the platform to use the following cryptographic mechanisms authorized by the CCN for ENS HIGH Category: • The certificates for software updates authentication, as defined in **ACT.2**.

5.9 SF. Connection requirements

Requirement	Description
CON.1	The TOE shall allow the establishment of access control policies that restrict the remote network assets that can be accessed by each user. The access control policies are based on: • Assignment of user groups to a PQC-Host. • Assignment of routes from the PQC-Host to users of the group.
CON.2	PQC-Host shall allow users to access through the PQC-Core to the assets from the remote network based on the access control policy defined in **CON.1**.
CON.3	The TOE shall allow administrators to configure whether administrator authorization is required to access a remote network access. The administrator user which will allow the connections shall be configured.
CON.4	In case administrator authorization is configured as defined in **CON.3**, the users shall request authorization to access the assets from the remote network for a limited time. The TOE shall send a notification to the administrator via email through the Mail Server using the SMTP over TLS v1.3 channel declared in **COM.1** to notify the request.
CON.5	In case administrator authorization is configured as defined in **CON.3**, the TOE shall not allow to access assets from the remote network if the authorization request sent by user (**CON.4**) is not accepted by the configured administrator user.
CON.6	The TOE shall close the connection with the remote network assets after 1 hour.
CON.7	The TOE shall allow administrators the addition, edition and removal of source IP addresses to a permanent blacklist, denying connections from these source IPs to the TOE.

6 Acronyms

The following table shows the acronyms used in this document.

Acronym	Meaning
AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CCN	Centro Criptológico Nacional
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
ENS	Esquema Nacional de Seguridad
GCM	Galois/Counter Mode
HMAC	Hash-based Message Authentication Code
IP	Internet Protocol
MSI	Microsoft Installer
mTLS	Mutual Transport Layer Security
OS	Operating System
PKCS	Public-Key Cryptography Standards
PQC	Post-Quantum Cryptography
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language
ST	Security Target
STIC	Seguridad de las Tecnologías de la Información y la Comunicación
TOE	Target Of Evaluation
TS	Timestamp

Table 1 Abbreviations

7 Document references

The following table shows the documents referenced in this document.

Reference	Document
CCN-STIC-2001	Definición de la Certificación Nacional Esencial de Seguridad (LINCE), marzo 2022 version 2.0 (National Essential Security Certification Definition, March 2022 version 2.0).
CCN-STIC-2002	Metodología de Evaluación para la Certificación Nacional Esencial de Seguridad (LINCE), marzo 2022 version 2.0 (Evaluation Methodology for National Essential Security Certification, March 2022 version 2.0).
CCN-STIC-2003	Plantilla para la Declaración de Seguridad de la Certificación Nacional Esencial de Seguridad (LINCE), marzo 2022 version 2.0 (Security Target template for National Essential Security Certification, March 2022 version 2.0).

Table 2 List of document references

8 Annex

8.1 Third party libraries used by the TOE

Library Name	Version
BouncyCastle.Cryptography	2.6.1
Newtonsoft.Json	13.0.3
log4net	3.1.0