ESET Endpoint Security

Security Target

Date: 2025-12-15

Created by

jtsec BEYOND IT SECURITY

CCGEN Create Common Criteria compliant documentation Simple and Easy

Changelog

Version	Date	Author	Comment
0.1	2023/09/11	ESET, spol. s r.o	First draft.
0.2	2025/10/01	ESET, spol. s r.o	References to document title modified to "ESET Endpoint Security - Security Target" to avoid the use of subsequent repeated term "Security" and enhance styling. Amended references to FPT_IDV_EXT. Modified SFR/Security Objective mapping and sufficiency rationale. Added descriptions for compilation flags in TOE Summary Description. Extended other descriptions in TOE Summary Description. Updated technical decisions Enhanced styling for some tables. Fixed typographic error in section related to timely security updates, clarified description related to public key in section related to timely security updates.
0.3	2025/12/15	ESET, spol. s r.o	Modified references to updated preparative guidance documentation (v0.3).

Table of contents

1 ST INTRODUCTION

1.1 ST REFERENCE

Title: ESET Endpoint Security - Security Target

Version: 0.3

Author: ESET, spol. s r.o

Evaluation Lab: jtsec Beyond IT Security

Date of publication: 2025-12-15

1.2 TOE REFERENCE

TOE Name: ESET Endpoint Security

TOE Developer: ESET, spol. s r.o

TOE Version: 12.1.2057.3

1.3 TOE OVERVIEW

1.3.1 INTRODUCTION

The TOE, ESET Endpoint Security 12.1.2057.3, is an endpoint protection solution that provides a variety of security features to protect their systems from a wide range of threats. ESET Endpoint Security is primarily designed for use on workstations in a business environment.

ESET Endpoint Security can be deployed as a standalone locally managed application or a remotely managed application.

1.3.2 TOE TYPE

The TOE is an application software which runs on a Windows platform that provides malware detection and mitigation in the system where it is installed.

1.3.3 TOE USAGE & MAJOR SECURITY FEATURES

The TOE is comprised of several security features. Below are identified the security features and which of them are considered TSF:

- **Cryptographic support**. The TOE exercises a set of cryptographic mechanisms intended to satisfy high-level security objectives such as confidentiality and integrity of the user data and the communications channels related to the TOE.
- **User data protection**. Refers to how the TOE limits its access to necessary hardware resources, information repositories and management or storage of sensitive data.
- **Security management**. The TOE uses mechanisms to allow a secure management of its functionalities. This protection is related to the restriction of using any default credentials and proper storage of configuration parameters.
- **Identification and Authentication**. This feature is intended to provide an authentication mechanism to the communication between the TOE and other entities.
- **Protection of the TSF**. The TOE includes several mechanisms to protect its critical components and functionalities, for example, incorporating memory anti-exploitation capabilities.
- **Trusted path/channel**. The product uses secure protocols and cryptographic mechanisms to establish secure and reliable communication channels so that sensitive information managed and transmitted is protected.

1.3.4 NON-TOE HARDWARE/SOFTWARE/FIRMWARE

As mentioned before, the TOE can be deployed in a standalone locally managed scenario or a remotely managed scenario. In this case, the evaluated configuration depicts the first case, a scenario where ESET Endpoint Security runs standalone and is managed locally in the platform where it is installed.

Therefore, the client-server architecture required for the remotely management scenario is discarded.

The main elements required by the TOE to operate are the following:

- **A general-purpose computer** with Windows 10 operating system featuring at least version 20H1 (19041) 64-bit.
  - **RAM**: 0.3 of free system memory.
  - **Hard Drive**: 1 GB of free disk space.
  - **Minimum display resolution**: 1024 x 768.
  - **Network requirements**: Internet connection for updates and licensing purposes.
- **ESET remote servers** for ESET Endpoint Security deployments to obtain updates and licensing purposes.

None of the above-mentioned elements are considered as part of the TOE ESET Endpoint Security, they are supporting elements.

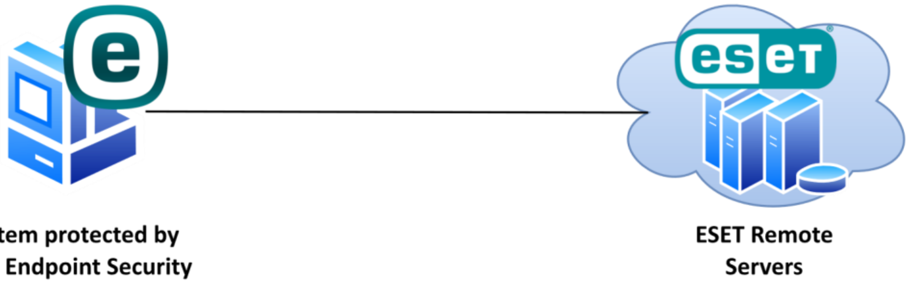


Figure 1 TOE deployment overview

1.3.5 NON-EVALUATED SECURITY FEATURES

As it was described in previous sections, the product is an antivirus software that is designed to provide detection, prevention and mitigation of malware threats.

The product offers the following capabilities:

- **Antivirus and Antimalware Protection**: ESET Endpoint Security employs advanced signature-based and heuristic detection techniques to identify and block known and unknown malware, including viruses, trojans, worms, and other malicious software.
- **Ransomware Protection**: The solution includes specialized features to protect against ransomware attacks, which are designed to encrypt data and demand a ransom for its release. ESET's anti-ransomware technology aims to detect and block such threats before they can cause data loss.
- **Firewall and Network Attack Protection**: The product includes a built-in firewall to monitor and control network traffic, preventing unauthorized access and blocking potential network-based attacks.
- **Web Filtering and Phishing Protection**: ESET Endpoint Security can filter web content and block access to malicious websites, protecting users from phishing attempts and other harmful online content.
- **Device Control**: The solution allows administrators to control and manage the devices that can connect to the endpoints, such as USB drives, external storage, and other peripherals. This helps prevent data leakage and the introduction of malicious software through unauthorized devices.
- **SSL/TLS Filtering**: ESET Endpoint Security can check for communication threats that use the SSL protocol. You can use various filtering modes to examine SSL-protected communication with trusted certificates, unknown certificates, or certificates that are excluded from SSL-protected communication checking.

- **Remote management**: Using the ESET PROTECT, it is possible to deploy ESET Endpoint Security, manage tasks, enforce security policies, monitor system status and respond to problems or threats on remote computers.

According to the specifications of the Protection Profile concerning the present Security Target, the features described in this section have not been considered within the scope of the Security Target. Therefore, these features will not be considered part of the evaluation as they are not considered part of the TOE.

Given the aforementioned rationale, the following modules are installed and operational given the evaluated configuration:

- Computer scan
- Protections:
  - Real-time file system protection
  - Document protection
  - Network access protection
  - Device control

On the other hand, the following modules are not installed or, otherwise, deactivated:

- Protections:
  - Email client protection
  - Web access protection
  - Secure browser
- Update mirror
- RMM support
- SSL/TLS Scanning
- Live Grid

1.4 TOE DESCRIPTION

1.4.1 TOE LOGICAL SCOPE

1.4.1.1 CRYPTOGRAPHIC SUPPORT

The TOE provides the possibility to configure a password to protect advanced setup configurations and prevent unauthorized uninstallation. This password is securely stored using platform-provided functionality and stored in the platform-provided registry.

The TOE does not implement or make direct use of asymmetric cryptographic key generation services. It invokes platform-functionality in order to establish trusted communication channels with the remote ESET update servers; therefore, keys required to implement these channels are implicitly generated by the platform itself. Same rationale applies to DRBG functionality, the TOE does not implement or directly employs DRBG services.

1.4.1.2 USER DATA PROTECTION

The TOE restricts its access to the platform's network connectivity resources. It also restricts its sensitive data access to system logs stored in the platform. Moreover, sensitive data generated and managed is stored using proper cryptographic mechanisms mentioned in the previous section.

In relation to the communications, the connections established by the TOE are limited to the ones related to update procedures.

1.4.1.3 SECURITY MANAGEMENT

The TOE does not use any default credentials, the advanced setup and uninstallation password is not set by default. While this password protection mechanism is not configured, the authentication mechanisms of the underlying platform are used to ensure only authorized users of that platform can gain access to the application critical configuration parameters or uninstall the TOE.

In relation to management capabilities, the TOE provides a way to install product and module updates, perform malware scans, activate/deactivate protection modules and configuration and enable/disable advance setup and uninstallation protection.

1.4.1.4 PRIVACY

The TOE does not explicitly request PII and users are not prompted to introduce PII; therefore, it does not transmit PII over the network.

1.4.1.5 PROTECTION OF THE TSF

Regarding the software updates, the TOE allows checking the installed version providing this information on the main interface of the TOE. Moreover, the TOE allows checking the updates manually with the aim of installing new available updates. The TOE also has a mechanism that allows installing software updates when available. The TOE takes the necessary steps to verify the integrity and authenticity of updates before installing them by checking their digital signature.

The TOE provides protection mechanisms to protect itself and prevent exploitation during its execution. These capabilities are compiled into the TOE and they assure a proper memory allocation management.

The TOE only uses documented platform APIs and a controlled set of third-party libraries to prevent the use of components that could present a privacy threat and ensure that technical vulnerabilities are appropriately addressed.

1.4.1.6 TRUSTED PATH/CHANNEL

During the operation state of the TOE, data is transmitted and received securely via HTTPS and TLSv1.2 when connections are established with the remote ESET update servers. Therefore, sensitive information related to product updates are encrypted and protected.

1.4.1.7 IDENTIFICATION AND AUTHENTICATION

The TOE establishes a communication with the remote ESET servers using the HTTPS protocol. This implies the use of the TLS security communication protocol, which is responsible for carrying out the authentication between the TOE itself and the remote ESET servers through the use of certificates.

The TOE uses X.509v3 certificates to authenticate the TLS connection with the remote ESET servers. The TOE validates the X.509 certificates using the certificate path validation algorithm and a local trust store.

1.4.2 TOE PHYSICAL SCOPE

The TOE is a software-only application running standalone on a Windows operating system platform, such platform is not considered part of the TOE.

- **Format**: *msi* format.
- **File name**: ees_nt64.msi
- **Delivery Method**: Downloadable from official ESET website.
- **TOE version**: 12.1.2057.3
- **SHA256 hash:** EC602625147A2B4B6845201D6632CB6F1D8F5C3753EE8696A96B1736D026B7A8

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

Item	Description	Version / Hash	Delivery Method	Format
ESET Endpoint Security Preparational Guidance for Common Criteria	Documents for the safe acceptance of the TOE and the installation and configuration process	0.3	Email on customer request	PDF

ESET Endpoint Security Operational Guidance for Common Criteria	Documents describing the safe use of the TOE.	0.2	Email on customer request	PDF
ESET Endpoint Security User Guide (eset_endpoint_security_12_enu.pdf)	Official guide available in ESET website.	REV. 10/1/2025 SHA 256 BC3A51157C0B271E000AFAC5CB9C46AE9257766E2B1CA77CBD0F76E43E42E51B	Online help portal: https://help.eset.com/ees/12/en-US/	Online PDF available for download

2 CONFORMANCE CLAIMS

This Security Target is compliant with Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.

This Security Target claims conformance with the following parts of Common Criteria:

- Conformance with [CC31R5P2] extended.
- Conformance with [CC31R5P3] extended.

The methodology to be used for the evaluation is described in the "Common Evaluation Methodology" of the Common Criteria standard of April 2017, version 3.1 revision 5 with an evaluation assurance level corresponding to the protection profile to which it claims conformance.

This Security Target claims exact conformance with the following protection profile:

- NIAP Protection Profile for Application Software version 1.4, dated 10 October 2021 with exact conformance.

2.1 CONFORMANCE CLAIM RATIONALE

The claimed Protection Profile [PPAPP-14] states the following:

"The requirements in this document apply to application software which runs on any type of platform. Some application types are covered by more specific PPs, which may be expressed as PP-Modules of this PP. Such applications are subject to the requirements of both this PP and the PP-Module that addresses their special functionality. PPs for some particularly specialized applications may not be expressed as PP-Modules at this time, though the requirements in this document should be seen as objectives for those highly specialized applications."

The TOE is a standalone application software which runs on a desktop/server Windows platform and is therefore considered to be aligned with the use cases and compliant targets of evaluation described in [PPAPP-14].

2.2 TECHNICAL DECISIONS

The following Technical Decisions for [PPAPP-14] have been considered for this evaluation:

TD#	Title	References	Applicable	Rationale
TD0945	Adding FIPS 186-5 in PP_APP_V1.4	FCS_CKM.1.1/AK FCS_COP.1.1/Sig	NO	SFRs is not claimed.
TD0931	Clarification when CTR_DRBG is Selected for FCS_RBG_EXT.2.2 in PP_APP_V1.4	FCS_RBG_EXT.2.2	NO	SFR is not claimed.
TD0893	Addition of Recommended Configuration Locations for Windows in FMT_MEC_EXT.1.1	FMT_MEC_EXT.1.1	NO	SFR claimed but changes in evaluation activity only affect .NET applications, which are not involved in this evaluation.
TD0865	Consistency of Cryptographic Key Sizes	FCS_STO_EXT.1.1, FCS_CKM.1.1/PBKDF, FCS_COP.1.1/SKC, FCS_CKM.1.1/SK	YES	Affects claimed SFRs referenced.
TD0844	Addition of Assurance Package for Flaw Remediation V1.0 Conformance Claim	Conformance Claims	NO	Changes for PP, does not impact ST.
TD0822	Correction to Windows Manifest File for FDP_DEC_EXT.1	FDP_DEC_EXT.1.1, FDP_DEC_EXT.1.2	NO	TOE is not a Windows Universal Application.

TD0815	Addition of Conditional TSS Activity for FPT_AEX_EXT.1.5	FPT_AEX_EXT.1.5	YES	Update test from evaluation activity.
TD0798	Static Memory Mapping Exceptions	FPT_AEX_EXT.1.1	NO	Affected assignment option is not defined by the author. Explicitly mapped addresses are not claimed.
TD0780	FIA_X509_EXT.1 Test 4 Clarification	FIA_X509_EXT.1.1	YES	Updates test from evaluation activity.
TD0756	Update for platform-provided full disk encryption	FDP_DAR_EXT.1	YES	Updates evaluation activity for claimed SFR.
TD0747	Configuration Storage Option for Android	FMT_MEC_EXT.1	NO	SFR claimed but changes in evaluation activity only affect products that relies on Android platforms which are not involved in this evaluation.
TD0743	FTP_DIT_EXT.1.1 Selection exclusivity	FTP_DIT_EXT.1.1	YES	Affects claimed SFRs, updates evaluation activity.
TD0736	Number of elements for iterations of FCS_HTTPS_EXT.1	FCS_HTTPS_EXT.1.3/Server	NO	SFR is not claimed.
TD0719	ECD for PP APP V1.3 and 1.4	Protection Profile	YES	Changes for PP, does not impact ST.
TD0717	Format changes for PP_APP_V1.4	FCS_CKM.1, FCS_CKM.2, FCS_CKM.1/AK, FCS_CKM.1/PBKDF, FCS_COP.1/Hash, FCS_COP.1/KeyedHash, FCS_COP.1/Sig, FCS_COP.1/SKC	YES	Affects claimed SFRs referenced. FCS_CKM.1 renamed to FCS_CKM_EXT.1.
TD0664	Testing activity for FPT_TUD_EXT.2.2	FPT_TUD_EXT.2.2	YES	Updates test from evaluation activity.
TD0650	Conformance claim sections updated to allow for MOD_VPNC_V2.3 and 2.4	Section 2	NO	Changes for PP, does not apply since PP-Module is not claimed.
TD0628	Addition of Container Image to Package Format	FPT_TUD_EXT.2.1	YES	SFR claimed, updates test from evaluation activity.

3 SECURITY PROBLEM DEFINITION

The security problem is described in terms of the threats that the TOE is expected to address, assumptions about the operational environment, and any organizational security policies that the TOE is expected to enforce.

3.1 THREATS TO SECURITY

This section identifies the threats against the TOE, as extracted from [PPAPP-14]. The threats are defined in terms of assets concerned, attackers and the adverse action that materializes the threat.

T.NETWORK_ATTACK: An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may engage in communications with the application software or alter communications between the application software and other endpoints in order to compromise it.

T.NETWORK_EAVESDROP: An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between the application and other endpoints.

T.LOCAL_ATTACK: An attacker can act through unprivileged software on the same computing platform on which the application executes. Attackers may provide maliciously formatted input to the application in the form of files or other local communications.

T.PHYSICAL_ACCESS: An attacker may try to access sensitive data at rest.

3.2 ASSUMPTIONS

The assumptions when using the TOE are the following, as extracted from [PPAPP-14]:

A.PLATFORM: The TOE relies upon a trustworthy computing platform with a reliable time clock for its execution. This includes the underlying platform and whatever runtime environment it provides to the TOE.

A.PROPER_USER: The user of the application software is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy.

A.PROPER_ADMIN: The administrator of the application software is not careless, willfully negligent or hostile, and administers the software in compliance with the applied enterprise security policy.

3.3 ORGANIZATIONAL SECURITY POLICIES

There are no Organizational Security Policies in [PPAPP-14].

4 SECURITY OBJECTIVES

4.1 SECURITY OBJECTIVES FOR THE TOE

O.INTEGRITY: Conformant TOEs ensure the integrity of their installation and update packages, and also leverage execution environment-based mitigations. Software is seldom, if ever, shipped without errors. The ability to deploy patches and updates to fielded software with integrity is critical to enterprise network security. Processor manufacturers, compiler developers, execution environment vendors, and operating system vendors have developed execution environment-based mitigations that increase the cost to attackers by adding complexity to the task of compromising systems. Application software can often take advantage of these mechanisms by using APIs provided by the runtime environment or by enabling the mechanism through compiler or linker options.

O.QUALITY: To ensure quality of implementation, conformant TOEs leverage services and APIs provided by the runtime environment rather than implementing their own versions of these services and APIs. This is especially important for cryptographic services and other complex operations such as file and media parsing. Leveraging this platform behavior relies upon using only documented and supported APIs.

O.MANAGEMENT: To facilitate management by users and the enterprise, conformant TOEs provide consistent and supported interfaces for their security-relevant configuration and maintenance. This includes the deployment of applications and application updates through the use of platform-supported deployment mechanisms and formats, as well as providing mechanisms for configuration. This also includes providing control to the user regarding disclosure of any PII.

O.PROTECTED_STORAGE: To address the issue of loss of confidentiality of user data in the event of loss of physical control of the storage medium, conformant TOEs will use data-at-rest protection. This involves encrypting data and keys stored by the TOE in order to prevent unauthorized access to this data. This also includes unnecessary network communications whose consequence may be the loss of data.

O.PROTECTED_COMMS: To address both passive (eavesdropping) and active (packet modification) network attack threats, conformant TOEs will use a trusted channel for sensitive data. Sensitive data includes cryptographic keys, passwords, and any other data specific to the application that should not be exposed outside of the application.

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

The following security objectives for the operational environment assist the TOE in correctly providing its security functionality.

OE.PLATFORM: The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying operating system and any discrete execution environment provided to the TOE.

OE.PROPER_USER: The user of the application software is not willfully negligent or hostile, and uses the software within compliance of the applied enterprise security policy.

OE.PROPER_ADMIN: The administrator of the application software is not careless, willfully negligent or hostile, and administers the software within compliance of the applied enterprise security policy.

4.3 SECURITY OBJECTIVES RATIONALE

This section describes how the assumptions, threats, and organizational security policies map to the security objectives.

Threat / Assumption / OSP	Security Objectives	Rationale
T.NETWORK_ATTACK	**O.PROTECTED_COMMS**	The threat **T.NETWORK_ATTACK** is countered by **O.PROTECTED_COMMS** as this provides for integrity of transmitted data.
	O.INTEGRITY	The threat **T.NETWORK_ATTACK** is countered by **O.INTEGRITY** as this provides for integrity of software that is installed onto the system from the network.
	O.MANAGEMENT	The threat **T.NETWORK_ATTACK** is countered by **O.MANAGEMENT** as this provides for the ability to configure the application to defend against network attack.
T.NETWORK_EAVESDROP	**O.PROTECTED_COMMS**	The threat **T.NETWORK_EAVESDROP** is countered by **O.PROTECTED_COMMS** as this provides for confidentiality of transmitted data.
	O.QUALITY	The objective **O.QUALITY** ensures use of mechanisms that provide protection against network-based attack.
	O.MANAGEMENT	The threat **T.NETWORK_EAVESDROP** is countered by **O.MANAGEMENT** as this provides for the ability to configure the application to protect the confidentiality of its transmitted data.
T.LOCAL_ATTACK	**O.QUALITY**	The objective **O.QUALITY** protects against the use of mechanisms that weaken the TOE with regard to attack by other software on the platform.

T.PHYSICAL_ACCESS	**O.PROTECTED_STORAGE**	The objective **O.PROTECTED_STORAGE** protects against unauthorized attempts to access physical storage used by the TOE.
A.PLATFORM	**OE.PLATFORM**	The operational environment objective **OE.PLATFORM** is realized through **A.PLATFORM**.
A.PROPER_USER	**OE.PROPER_USER**	The operational environment objective **OE.PROPER_USER** is realized through **A.PROPER_USER**.
A.PROPER_ADMIN	**OE.PROPER_ADMIN**	The operational environment objective **OE.PROPER_ADMIN** is realized through **A.PROPER_ADMIN**.

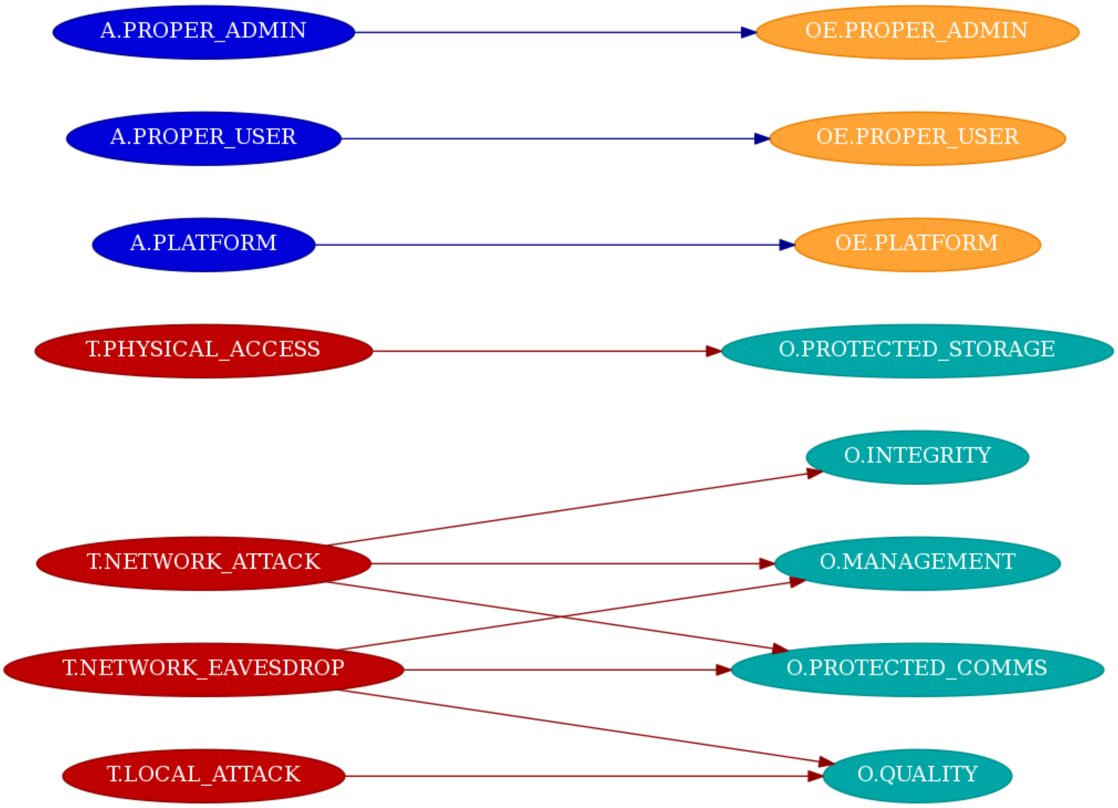


Figure 2 Mapping of Security Problem Definition to Security Objectives

5 EXTENDED COMPONENTS DEFINITION

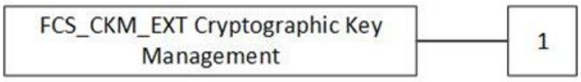
5.1 CLASS FCS: CRYPTOGRAPHIC SUPPORT

5.1.1 CRYPTOGRAPHIC KEY MANAGEMENT (FCS_CKM_EXT)

Family behavior

This family defines requirements for management of cryptographic keys that are not addressed by FCS_CKM in CC Part 2.

Component levelling



FCS_CKM_EXT.1 Cryptographic Key Generation Services, requires the TSF to specify whether asymmetric key generation is implemented by the TSF, invoked from the operational environment, or not used by the TOE.

Management: FCS_CKM_EXT.1

There are no management activities foreseen.

Audit: FCS_RBG_EXT.1

There are no auditable events foreseen.

FCS_CKM_EXT.1 Cryptographic Key Generation Services

Hierarchical to:

No other components.

Dependencies:

No dependencies.

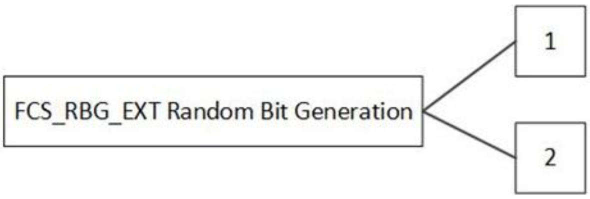
FCS_CKM_EXT.1.1 ***The application shall [selection: generate no asymmetric cryptographic keys, invoke platform-provided functionality for asymmetric key generation, implement asymmetric key generation].***

5.1.2 RANDOM BIT GENERATION (FCS_RBG_EXT)

Family behavior

This family defines requirements for the generation of random bits.

Component levelling



FCS_RBG_EXT.1 Random Bit Generation Services, requires the TSF to specify whether random bit generation is implemented by the TSF, invoked from the operational environment, or not used by the TOE.

FCS_RBG_EXT.2 Random Bit Generation from Application, specifies the mechanism by which the TSF generates random bits.

Management: FCS_RBG_EXT.1

There are no management activities foreseen.

Audit: FCS_RBG_EXT.1

There are no auditable events foreseen.

FCS_RBG_EXT.1: Random Bit Generation Services

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FCS_RBG_EXT.1.1: ***The application shall [selection: use no DRBG functionality, invoke platform-provided DRBG functionality, implement DRBG functionality] for its cryptographic operations.***

5.1.3 STORAGE OF CREDENTIALS (FCS_STO_EXT)

Family behavior

This family defines requirements for the secure storage of credential data.

Component levelling

FCS_STO_EXT Storage of Credentials
1

FCS_STO_EXT.1 Storage of Credentials, requires the application to define how to store credentials to non-volatile memory.

Management: FCS_STO_EXT.1

There are no management functions foreseen.

Audit: FCS_STO_EXT.1

There are no auditable events foreseen

FCS_STO_EXT.1: Storage of Credentials

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FCS_STO_EXT.1.1: ***The application shall [selection: not store any credentials, invoke the functionality provided by the platform to securely store [assignment: list of credentials], securely store [assignment: list of credentials] with platform provided [selection: [selection: AES-CBC (as defined in NIST SP 800-38A) mode, AES-GCM (as defined in NIST SP 800-38D) mode, AES-XTS (as defined in NIST SP 800-38E) mode] and cryptographic key size of 256-bits. PBKDF2 function that uses [selection: HMAC-SHA256, HMAC-SHA384, HMAC-SHA512] with [assignment: positive integer of 1,000 or more] iterations and output size of [assignment: positive integer of 256 or greater] bits that meet the following [NIST SP 800-132].] implement functionality to securely store [assignment: list of credentials] according to [selection: FCS_COP.1/SKC, FCS_CKM.1/PBKDF]] to non-volatile memory.***

5.2 CLASS FDP: USER DATA PROTECTION

5.2.1 ACCESS TO PLATFORM RESOURCES (FDP_DEC_EXT)

Family behavior

This family defines requirements for accessing platform resources.

Component levelling

FDP_DEC_EXT.1 Access to Platform Resources, requires the application to restrict access to hardware sources and sensitive information repositories.

Management: FDP_DEC_EXT.1

The following action could be considered for the management functions in FMT:

a) enable/disable the transmission of any information describing the system's hardware, software, or configuration.

Audit: FDP_DEC_EXT.1

There are no auditable events foreseen.

FDP_DEC_EXT.1: Access to Platform Resources

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FDP_DEC_EXT.1.1: ***The application shall restrict its access to [selection: no hardware resources, network connectivity, camera, microphone, location services, NFC, USB, Bluetooth, [assignment: list of additional hardware resources]]***

FDP_DEC_EXT.1.2: ***The application shall restrict its access to [selection: no sensitive information repositories, address book, calendar, call lists, system logs, [assignment: list of additional sensitive information repositories]]***

5.2.2 NETWORK COMMUNICATIONS (FDP_NET_EXT)

Family behavior

This family defines requirements for the TOE's use of network connectivity.

Component levelling

FDP_NET_EXT Network Communications
1

FDP_NET_EXT.1 Network Communications, identifies the purpose for each network interface used by the TOE and how that interface is invoked.

Management: FDP_NET_EXT.1

There are no management functions foreseen.

Audit: FDP_NET_EXT.1

There are no auditable events foreseen.

FDP_NET_EXT.1: Network Communications

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FDP_NET_EXT.1.1: ***The application shall restrict network communication to [selection: no network communication, user-initiated communication for, [assignment: list of functions for which the user can initiate network communication], respond to, [assignment: list of remotely initiated communication], [assignment: list of application-initiated network communication]].***

5.2.3 ENCRYPTION OF SENSITIVE APPLICATION DATA (FDP_DAR_EXT)

Family behavior

This family defines requirements for implementation of data-at-rest protection.

Component levelling

FDP_DAR_EXT Data at Rest Encryption
1

FDP_DAR_EXT.1 Encryption of Sensitive Application Data, requires the application to be able to protect all data with a chosen method of encryption.

Management: FDP_DAR_EXT.1

There are no management functions foreseen.

Audit: FDP_DAR_EXT.1

There are no auditable events foreseen.

FDP_DAR_EXT.1: Encryption Of Sensitive Application Data

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FDP_DAR_EXT.1.1: ***The application shall [selection: leverage platform-provided functionality to encrypt sensitive data, implement functionality to encrypt sensitive data as defined in the PPModule for File Encryption, protect sensitive data in accordance with FCS_STO_EXT.1, not store any sensitive data] in non-volatile memory.***

5.3 CLASS FMT: SECURITY MANAGEMENT

5.3.1 SUPPORTED CONFIGURATION MECHANISM (FMT_MEC_EXT)

Family behavior

This family defines requirements for the TOE’s use of mechanisms for the storage of configuration data.

Component levelling

FMT_MEC_EXT Supported Configuration Mechanism
1

FMT_MEC_EXT.1 Supported Configuration Mechanism, requires the application to store configuration data either through the use of an appropriate environmental mechanism or through its own file encryption capability.

Management: FMT_MEC_EXT.1

There are no management functions foreseen.

Audit: FMT_MEC_EXT.1

There are no auditable events foreseen.

FMT_MEC_EXT.1: Supported Configuration Mechanism

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FMT_MEC_EXT.1.1: ***The application shall [selection: invoke the mechanisms recommended by the platform vendor for storing and setting configuration options, implement functionality to encrypt and store configuration options as defined by FDP_PRT_EXT.1 in the PP-Module for File Encryption]***

5.3.2 SECURE BY DEFAULT CONFIGURATION (FMT_CFG_EXT)

Family behavior

This family defines requirements for authorization to manage the behavior of the application.

Component levelling

FMT_CFG_EXT.1 Secure by Default Configuration, requires the application to define how to set new credentials and protect the application from modification by unprivileged users.

Management: FMT_CFG_EXT.1

There are no management functions foreseen.

Audit: FMT_CFG_EXT.1

There are no auditable events foreseen.

FMT_CFG_EXT.1: Secure by Default Configuration

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FMT_CFG_EXT.1.1: ***The application shall provide only enough functionality to set new credentials when configured with default credentials or no credentials.***

FMT_CFG_EXT.1.2: ***The application shall be configured by default with file permissions which protect the application binaries and data files from modification by normal unprivileged users.***

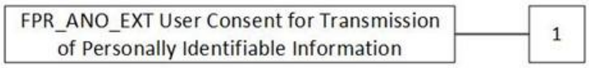
5.4 CLASS FPR: PRIVACY

5.4.1 USER CONSENT FOR TRANSMISSION OF PERSONALLY IDENTIFIABLE INFORMATION (FPR_ANO_EXT)

Family Behavior

This family defines requirements for anonymity that are not covered by the Part 2 family FPR_ANO.

Component Leveling


FPR_ANO_EXT User Consent for Transmission of Personally Identifiable Information
1

FPR_ANO_EXT.1 User Consent for Transmission of Personally Identifiable Information, requires the TSF to transmit personally identifiable information only with explicit approval.

Management: FPR_ANO_EXT.1

The following action could be considered for the management functions in FMT:

a) enable/disable the transmission of any PII.

Audit: FPR_ANO_EXT.1

There are no auditable events foreseen.

FPR_ANO_EXT.1: User Consent for Transmission of Personally Identifiable Information

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FPR_ANO_EXT.1.1 The application shall [selection: not transmit PII over a network, require user approval before executing [assignment: list of functions that transmit PII over a network]].

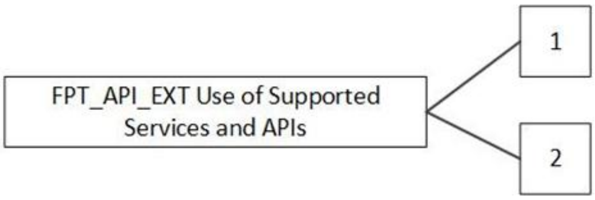
5.5 CLASS FPT: PROTECTION OF THE TSF

5.5.1 USE OF SUPPORTED SERVICES AND APIS (FPT_API_EXT)

Family behavior

This family defines requirements for specifying the environmental APIs used by the TOE.

Component levelling



FPT_API_EXT.1 Use of Supported Services and APIs, requires the application to use only documented platform APIs.

Management: FPT_API_EXT.1

There are no management functions foreseen.

Audit: FPT_API_EXT.1

There are no auditable events foreseen.

FPT_API_EXT.1: Use of Supported Services and APIs

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FPT_API_EXT.1.1: ***The application shall use only documented platform APIs.***

5.5.2 ANTI-EXPLOITATION CAPABILITIES (FPT_AEX_EXT)

Family behavior

This family defines requirements for protecting against common types of software exploitation techniques.

Component levelling

FPT_AEX_EXT Anti-Exploitation Capabilities
1

FPT_AEX_EXT.1 Anti-Exploitation Capabilities, requires the application to implement functionality that protects against common software exploits.

Management: FPT_AEX_EXT.1

There are no management functions foreseen.

Audit: FPT_AEX_EXT.1

There are no auditable events foreseen.

FPT_AEX_EXT.1: Anti-Exploitation Capabilities

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FPT_AEX_EXT.1.1: ***The application shall not request to map memory at an explicit address except for [assignment: list of explicit exceptions]***

FPT_AEX_EXT.1.2: ***The application shall [selection: not allocate any memory region with both write and execute permissions, allocate memory regions with write and execute permissions for only, [assignment: list of functions performing just-in-time compilation]]***

FPT_AEX_EXT.1.3: ***The application shall be compatible with security features provided by the platform vendor.***

FPT_AEX_EXT.1.4: ***The application shall not write user-modifiable files to directories that contain executable files unless explicitly directed by the user to do so.***

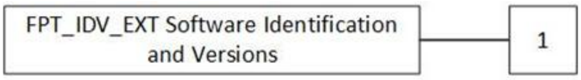
FPT_AEX_EXT.1.5: ***The application shall be built with stack-based buffer overflow protection enabled.***

5.5.3 SOFTWARE IDENTIFICATION AND VERSIONS (FPT_IDV_EXT)

Family behavior

This family defines requirements for how to use versioning.

Component levelling



FPT_IDV_EXT.1 Software Identification and Versions, requires the TSF to specify the versioning mechanism used.

Management: FPT_IDV_EXT.1

There are no management functions foreseen.

Audit: FPT_IDV_EXT.1

There are no auditable events foreseen.

FPT_IDV_EXT.1: Software Identification and Versions

Hierarchical to:

No other components.

Dependencies:

No dependencies.

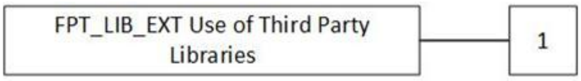
FPT_IDV_EXT.1.1: ***The application shall be versioned with [selection: SWID tags that comply with minimum requirements from ISO/IEC 19770-2:2015, [assignment: other version information]]***

5.5.4 USE OF THIRD PARTY LIBRARIES (FPT_LIB_EXT)

Family behavior

This family defines requirements for identification of any third-party libraries used by the TOE.

Component levelling



FPT_LIB_EXT.1 TSF Use of Third Party Libraries, requires the TOE to identify the third party libraries that it uses.

Management: FPT_LIB_EXT.1

There are no management functions foreseen.

Audit: FPT_LIB_EXT.1

There are no auditable events foreseen.

FPT_LIB_EXT.1: Use of Third Party Libraries

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FPT_LIB_EXT.1.1: ***The application shall be packaged with only [assignment: list of third-party libraries]***

5.5.5 INTEGRITY FOR INSTALLATION AND UPDATE (FPT_TUD_EXT)

Family behavior

This family defines requirements for applying updates to the TOE.

Component levelling

FPT_TUD_EXT Trusted Updates
1
2

FPT_TUD_EXT.1 Integrity for Installation and Update, requires the TSF to specify how updates to it are acquired and verified.

FPT_TUD_EXT.2 Integrity for Installation and Update, requires TOE updates to be packaged in a certain manner.

Management: FPT_TUD_EXT.1

There are no management functions foreseen.

Audit: FPT_TUD_EXT.1

There are no auditable events foreseen.

Management: FPT_TUD_EXT.2

There are no management functions foreseen.

Audit: FPT_TUD_EXT.2

There are no auditable events foreseen.

FPT_TUD_EXT.1: Integrity for Installation and Update

Hierarchical to:

No other components.

Dependencies:

FPT_IDV_EXT.1

FPT_TUD_EXT.1.1: ***The application shall [selection: provide the ability, leverage the platform] to check for updates and patches to the application software.***

FPT_TUD_EXT.1.2: ***The application shall [selection: provide the ability, leverage the platform] to query the current version of the application software.***

FPT_TUD_EXT.1.3: ***The application shall not download, modify, replace or update its own binary code.***

FPT_TUD_EXT.1.4: ***Application updates shall be digitally signed such that the application platform can cryptographically verify them prior to installation.***

FPT_TUD_EXT.1.5: ***The application is distributed [selection: with the platform OS, as an additional software package to the platform OS]***

FPT_TUD_EXT.2: Integrity for Installation and Update

Hierarchical to:

No other components.

Dependencies:

FPT_TUD_EXT.1

FPT_TUD_EXT.2.1: ***The application shall be distributed using the format of the platform-supported package manager.***

FPT_TUD_EXT.2.2: ***The application shall be packaged such that its removal results in the deletion of all traces of the application, with the exception of configuration settings, output files, and audit/log events.***

FPT_TUD_EXT.2.3: ***The application installation package shall be digitally signed such that its platform can cryptographically verify them prior to installation.***

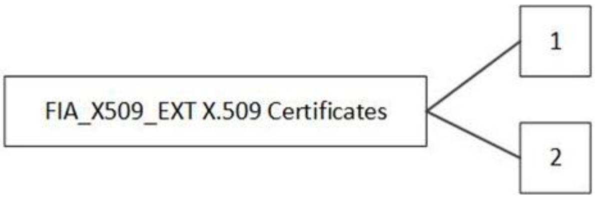
5.6 CLASS FIA: IDENTIFICATION AND AUTHENTICATION

5.6.1 X.509 CERTIFICATE AUTHENTICATION (FIA_X509_EXT)

Family behavior

This family defines requirements for the management and use of X.509 certificates.

Component levelling



FIA_X509_EXT.1 X.509 Certificate Validation, specifies the rules the TSF must follow to determine if an X.509 certificate is valid.

FIA_X509_EXT.2 X.509 Certificate Authentication, defines the TOE's usage of X.509 certificates and how it reacts to certificates that cannot be validated.

Management: FIA_X509_EXT.1

There are no management functions foreseen.

Audit: FIA_X509_EXT.1

There are no auditable events foreseen.

Management: FIA_X509_EXT.2

There are no management functions foreseen.

Audit: FIA_X509_EXT.2

The following action could be considered for the management functions in FMT:

a) configuration of TSF behavior in the event that certificate revocation status cannot be verified.

FIA_X509_EXT.1: X.509 Certificate Validation (Selection-based)

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FIA_X509_EXT.1.1: ***The application shall [selection: invoke platform-provided functionality, implement functionality] to validate certificates in accordance with the following rules: RFC 5280 certificate validation and certificate path validation. The certificate path must terminate with a trusted CA certificate. The application shall validate a certificate path by ensuring the presence of the basicConstraints extension and that the CA flag is set to TRUE for all CA certificates, and that any path constraints are met. The application shall validate that any CA certificate includes caSigning purpose in the key usage field The application shall validate the revocation status of the certificate using [selection: OCSP as specified in RFC 6960, CRL as specified in RFC 5280 Section 6.3, CRL as specified in RFC 8603, an OCSP TLS Status Request Extension (OCSP stapling) as specified in RFC 6066, OCSP TLS Multi- Certificate Status Request Extension (i.e., OCSP Multi-Stapling) as specified in RFC 6961] The application shall validate the extendedKeyUsage (EKU) field according to the following rules: Certificates used for trusted updates and executable code integrity verification shall have the Code Signing Purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field. Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the EKU field. Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the EKU field. S/MIME certificates presented for email encryption and signature shall have the Email Protection purpose (id-kp 4 with OID 1.3.6.1.5.5.7.3.4) in the EKU field. OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the EKU field. Server certificates presented for EST shall have the CMC Registration Authority (RA) purpose (id-kp-cmcRA with OID 1.3.6.1.5.5.7.3.28) in the EKU field.***

FIA_X509_EXT.1.2: ***The application shall treat a certificate as a CA certificate only if the basicConstraints extension is present and the CA flag is set to TRUE.***

FIA_X509_EXT.2: X.509 Certificate Authentication

Hierarchical to:

No other components.

Dependencies:

FIA_X509_EXT.1

[FTP_ITC.1 or FTP_TRP.1]

FIA_X509_EXT.2.1: ***The application shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [selection: HTTPS, TLS, DTLS, SSH, IPsec]***

FIA_X509_EXT.2.2: ***When the application cannot establish a connection to determine the validity of a certificate, the application shall [selection: allow the administrator to choose whether to accept the certificate in these cases, accept the certificate, not accept the certificate]***

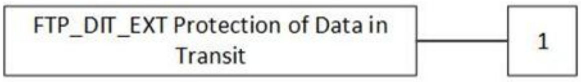
5.7 CLASS FTP: TRUSTED PATH/CHANNELS

5.7.1 PROTECTION OF DATA IN TRANSIT (FTP_DIT_EXT)

Family behavior

This family defines requirements for protecting data in transit.

Component levelling



FTP_DIT_EXT.1 Protection of Data in Transit, requires the TSF to specify what data is transmitted outside the TOE over a trusted channel, what protocol is used for data transmission, and whether the TSF implements this protocol or invokes an environmental interface to do so.

Management: FTP_DIT_EXT.1

There are no management functions foreseen.

Audit: FTP_DIT_EXT.1

There are no auditable events foreseen.

FTP_DIT_EXT.1: Protection of Data in Transit

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FTP_DIT_EXT.1.1: ***The application shall [selection: not transmit any[selection: data, sensitive data], encrypt all transmitted [selection: sensitive data, data] with [selection: HTTPS as a client in accordance with FCS_HTTPS_EXT.1/Client for [assignment: function(s)], HTTPS as a server in accordance with FCS_HTTPS_EXT.1/Server for [assignment: function(s)], HTTPS as a server using mutual authentication in accordance with FCS_HTTPS_EXT.2 for [assignment: function(s)], TLS as a server as defined in the Functional Package for TLS and also supports functionality for [selection: mutual authentication, none] for [assignment: function(s)], TLS as a client as defined in the Functional Package for TLS for [assignment: function(s)], DTLS as a server as defined in the Functional Package for TLS and also supports functionality for [selection: mutual authentication, none] for [assignment: function(s)], DTLS as a client as defined in the Functional Package for TLS for [assignment: function(s)], SSH as defined in the Functional Package for Secure Shell for [assignment: function(s)], IPsec as defined in the PP-Module for VPN Client for [assignment: function(s)]], invoke platform-provided functionality to encrypt all transmitted sensitive data with [selection: HTTPS, TLS, DTLS, SSH] for [assignment: function(s)], invoke platform-provided functionality to encrypt all transmitted data with [selection: HTTPS, TLS, DTLS, SSH] for [assignment: function(s)]] between itself and another trusted IT product.***

5.8 EXTENDED SARS DEFINITION

5.8.1 CLASS ALC: LIFE-CYCLE SUPPORT

Class extension according to Protection Profile for Application Software.

5.8.1.1 TIMELY SECURITY UPDATES (ALC_TSU_EXT)

Family objectives

Family created according to Protection Profile for Application Software.

Component levelling

ALC_TSU_EXT.1: Timely Security Updates

Hierarchical to:

No other components.

Dependencies:

No dependencies.

Developer action elements.

ALC_TSU_EXT.1.1D: ***The developer shall provide a description in the TSS of how timely security updates are made to the TOE.***

ALC_TSU_EXT.1.2D: ***The developer shall provide a description in the TSS of how users are notified when updates change security properties or the configuration of the product.***

Content and representation elements.

ALC_TSU_EXT.1.1C: ***The description shall include the process for creating and deploying security updates for the TOE software.***

ALC_TSU_EXT.1.2C: ***The description shall express the time window as the length of time, in days, between public disclosure of a vulnerability and the public availability of security updates to the TOE.***

ALC_TSU_EXT.1.3C: ***The description shall include the mechanisms publicly available for reporting security issues pertaining to the TOE.***

Evaluator action elements.

ALC_TSU_EXT.1.1E: ***The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.***

6 SECURITY REQUIREMENTS

This section defines the Security functional requirements (SFRs) and the Security assurance requirements (SARs) that fulfill the TOE. Assignment, selection, iteration and refinement operations have been made, adhering to the following conventions:

- Assignments. They appear between square brackets. The word “assignment” is maintained and the resolution is presented in ***boldface, italic and blue color.***

- Selections. They appear between square brackets. The word “selection” is maintained and the resolution is presented in ***boldface, italic and blue color.***

- Iterations. It includes “/” and an “identifier” following requirement identifier that allows to distinguish the iterations of the requirement. Example: FCS_COP.1/XXX.

- Refinements: the text where the refinement has been done is shown ***bold, italic, and light red color.*** Where part of the content of a SFR component has been removed, the removed text is shown in ~~***bold, italic, light red color and crossed out.***~~

6.1 SECURITY FUNCTIONAL REQUIREMENTS

None of the optional SFRs from Appendix A of [PPAPP-14] have been included in this Security Target.

The following selection-based requirements from Appendix B of [PPAPP-14] have been included in this Security Target: FPT_TUD_EXT.2, FIA_X509_EXT.1, FIA_X509_EXT.2.

The following selection-based requirements from Appendix B of [PPAPP-14] have not been included in this Security Target: FCS_RBG_EXT.2, FCS_HTTPS_EXT.1/Server, FCS_HTTPS_EXT.1/Client, FCS_HTTPS_EXT.2, FCS_COP.1/Sig, FCS_COP.1/KeyedHash, FCS_COP.1/Hash, FCS_COP.1/SKC, FCS_CKM.2, FCS_CKM.1/AK, FCS_CKM.1/PBKDF.

6.1.1 FCS: CRYPTOGRAPHIC SUPPORT

6.1.1.1 FCS_CKM_EXT.1: CRYPTOGRAPHIC KEY GENERATION SERVICES

FCS_CKM_EXT.1.1 The application shall ***[selection:***

- ***generate no asymmetric cryptographic keys***

].

6.1.1.2 FCS_RBG_EXT.1: RANDOM BIT GENERATION SERVICES

FCS_RBG_EXT.1.1 The application shall ***[selection:***

- ***use no DRBG functionality***

] for its cryptographic operations.

6.1.1.3 FCS_STO_EXT.1: STORAGE OF CREDENTIALS

FCS_STO_EXT.1.1 The application shall ***[selection:***

- ***invoke the functionality provided by the platform to securely store [assignment: advanced setup and uninstallation password]***

] to non-volatile memory.

6.1.2 FDP: USER DATA PROTECTION

6.1.2.1 FDP_DEC_EXT.1: ACCESS TO PLATFORM RESOURCES

FDP_DEC_EXT.1.1 The application shall restrict its access to ***[selection:***

- ***network connectivity***

].

FDP_DEC_EXT.1.2 The application shall restrict its access to ***[selection:***

- ***system logs***

].

6.1.2.2 FDP_NET_EXT.1: NETWORK COMMUNICATIONS

FDP_NET_EXT.1.1 The application shall restrict network communication to ***[selection:***

- ***[assignment: product and module updates]***

].

6.1.2.3 FDP_DAR_EXT.1: ENCRYPTION OF SENSITIVE APPLICATION DATA

FDP_DAR_EXT.1.1 The application shall ***[selection:***

- ***protect sensitive data in accordance with FCS_STO_EXT.1***

] in non-volatile memory.

6.1.3 FMT: SECURITY MANAGEMENT

6.1.3.1 FMT_MEC_EXT.1: SUPPORTED CONFIGURATION MECHANISM

FMT_MEC_EXT.1.1 The application shall ***[selection: invoke the mechanisms recommended by the platform vendor for storing and setting configuration options]***.

6.1.3.2 FMT_CFG_EXT.1: SECURE BY DEFAULT CONFIGURATION

FMT_CFG_EXT.1.1 The application shall provide only enough functionality to set new credentials when configured with default credentials or no credentials.

FMT_CFG_EXT.1.2 The application shall be configured by default with file permissions which protect the application binaries and data files from modification by normal unprivileged users.

6.1.3.3 FMT_SMF.1: SPECIFICATION OF MANAGEMENT FUNCTIONS

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions ***[selection:***

- ***[assignment: product and module updates, malware scan, protection modules activation/deactivation and configuration, enable/disable advanced setup and uninstallation protection]***

].

6.1.4 FPR: PRIVACY

6.1.4.1 FPR_ANO_EXT.1: USER CONSENT OF TRANSMISSION OF PERSONALLY IDENTIFIABLE INFORMATION

FPR_ANO_EXT.1.1 The application shall ***[selection:***

- ***not transmit PII over a network***

].

6.1.5 FPT: PROTECTION OF THE TSF

6.1.5.1 FPT_API_EXT.1: USE OF SUPPORTED SERVICES AND APIS

FPT_API_EXT.1.1 The application shall use only documented platform APIs.

6.1.5.2 FPT_AEX_EXT.1: ANTI-EXPLOITATION CAPABILITIES

FPT_AEX_EXT.1.1 The application shall not request to map memory at an explicit address except for ***[assignment: none]***.

FPT_AEX_EXT.1.2 The application shall ***[selection:***

- ***allocate memory regions with write and execute permissions for only [assignment: emulation during scanning]***

].

FPT_AEX_EXT.1.3 The application shall be compatible with security features provided by the platform vendor.

FPT_AEX_EXT.1.4 The application shall not write user-modifiable files to directories that contain executable files unless explicitly directed by the user to do so.

FPT_AEX_EXT.1.5 The application shall be built with stack-based buffer overflow protection enabled.

6.1.5.3 FPT_IDV_EXT.1: SOFTWARE IDENTIFICATION AND VERSIONS

FPT_IDV_EXT.1.1 The application shall be versioned with ***[selection: [assignment: major.minor.patch.differentiator methodology]]***.

6.1.5.4 FPT_LIB_EXT.1: USE OF THIRD PARTY LIBRARIES

FPT_LIB_EXT.1.1 The application shall be packaged with only ***[assignment: third-party libraries listed in Annex B]***.

6.1.5.5 FPT_TUD_EXT.1: INTEGRITY FOR INSTALLATION AND UPDATE

FPT_TUD_EXT.1.1 The application shall ***[selection: provide the ability]*** to check for updates and patches to the application software.

FPT_TUD_EXT.1.2 The application shall ***[selection: provide the ability]*** to query the current version of the application software.

FPT_TUD_EXT.1.3 The application shall not download, modify, replace or update its own binary code.

FPT_TUD_EXT.1.4 Application updates shall be digitally signed such that the application platform can cryptographically verify them prior to installation.

FPT_TUD_EXT.1.5 The application is distributed ***[selection: as an additional software package to the platform OS]***.

6.1.5.6 FPT_TUD_EXT.2: INTEGRITY FOR INSTALLATION AND UPDATE

FPT_TUD_EXT.2.1 The application shall be distributed using ***[selection: the format of the platform-supported package manager]***.

FPT_TUD_EXT.2.2 The application shall be packaged such that its removal results in the deletion of all traces of the application, with the exception of configuration settings, output files, and audit/log events.

FPT_TUD_EXT.2.3 The application installation package shall be digitally signed such that its platform can cryptographically verify them prior to installation.

6.1.6 FTP: TRUSTED PATH/CHANNELS

6.1.6.1 FTP_DIT_EXT.1: PROTECTION OF DATA IN TRANSIT

FTP_DIT_EXT.1.1 The application shall ***[selection:***

- ***invoke platform-provided functionality to encrypt all transmitted sensitive data with [selection: HTTPS]***

] between itself and another trusted IT product.

6.1.7 FIA: IDENTIFICATION AND AUTHENTICATION

6.1.7.1 FIA_X509_EXT.1: X.509 CERTIFICATE VALIDATION

FIA_X509_EXT.1.1 The application shall ***[selection: invoke platform-provided functionality]*** to validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certificate path validation.
- The certificate path must terminate with a trusted CA certificate.
- The application shall validate a certificate path by ensuring the presence of the basicConstraints extension and that the CA flag is set to TRUE for all CA certificates, and that any path constraints are met.
- The application shall validate that any CA certificate includes caSigning purpose in the key usage field
- The application shall validate the revocation status of the certificate using ***[selection: CRL as specified in RFC 5280 Section 6.3]***.
- The application shall validate the extendedKeyUsage (EKU) field according to the following rules:
    - Certificates used for trusted updates and executable code integrity verification shall have the Code Signing Purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.
    - Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the EKU field.
    - Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the EKU field.
    - S/MIME certificates presented for email encryption and signature shall have the Email Protection purpose (id-kp 4 with OID 1.3.6.1.5.5.7.3.4) in the EKU field.
    - OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the EKU field.
    - Server certificates presented for EST shall have the CMC Registration Authority (RA) purpose (id-kp-cmcRA with OID 1.3.6.1.5.5.7.3.28) in the EKU field.

FIA_X509_EXT.1.2 The application shall treat a certificate as a CA certificate only if the basicConstraints extension is present and the CA flag is set to TRUE.

6.1.7.2 FIA_X509_EXT.2: X.509 CERTIFICATE AUTHENTICATION

FIA_X509_EXT.2.1 The application shall use X.509v3 certificates as defined by RFC 5280 to support authentication for ***[selection: HTTPS]***.

FIA_X509_EXT.2.2 When the application cannot establish a connection to determine the validity of a certificate, the application shall ***[selection: accept the certificate]***.

6.2 SECURITY ASSURANCE REQUIREMENTS

The development and the evaluation of the TOE shall be done in accordance with the protection profile to which it claims conformance. The SARs selected are those of the application software protection profile this ST claims conformance. They provide the expected assurance for the evaluated TOE.

The following table shows the assurance requirements by reference the individual components in [CC31R5P3]

Assurance Class	Assurance Components
ASE: Security Target evaluation	ASE_INT.1: ST introduction ASE_CCL.1: Conformance claims ASE_SPD.1: Security problem definition ASE_OBJ.2: Security objectives ASE_ECD.1: Extended components definition ASE_REQ.2: Derived security requirements ASE_TSS.1: TOE summary specification
ALC: Life-cycle support	ALC_CMC.1: Labelling of the TOE ALC_CMS.1: TOE CM coverage ALC_TSU_EXT.1: Timely Security Updates
ADV: Development	ADV_FSP.1: Basic functional specification
AGD: Guidance documents	AGD_OPE.1: Operational user guidance AGD_PRE.1: Preparative procedures
ATE: Tests	ATE_IND.1: Independent testing - conformance
AVA: Vulnerability assessment	AVA_VAN.1: Vulnerability survey

Table 1 *Security Assurance Requirements*

6.3 SECURITY REQUIREMENTS RATIONALE

6.3.1 NECESSITY AND SUFFICIENCY ANALYSIS

SFR / TOE Security Objective	O.INTEGRITY	O.QUALITY	O.MANAGEMENT	O.PROTECTED_STORAGE	O.PROTECTED_COMMS
FCS_CKM_EXT.1		X			X
FCS_RBG_EXT.1		X		X	X
FCS_STO_EXT.1		X		X	
FDP_DEC_EXT.1	X				
FDP_NET_EXT.1					X
FDP_DAR_EXT.1		X		X	
FMT_MEC_EXT.1		X			
FMT_CFG_EXT.1	X				
FMT_SMF.1			X		
FPR_ANO_EXT.1			X		
FPT_API_EXT.1		X			
FPT_AEX_EXT.1	X				

SFR / TOE Security Objective	O.INTEGRITY	O.QUALITY	O.MANAGEMENT	O.PROTECTED_STORAGE	O.PROTECTED_COMMS
FPT_IDV_EXT.1			X		
FPT_LIB_EXT.1		X			
FPT_TUD_EXT.1	X		X		
FPT_TUD_EXT.2		X			
FTP_DIT_EXT.1		X			X
FIA_X509_EXT.1					X
FIA_X509_EXT.2					X

Table 2 SFRs / TOE Security Objectives coverage

6.3.2 SECURITY REQUIREMENT SUFFICIENCY

O.INTEGRITY:

The PP includes **FDP_DEC_EXT.1** to limit access to platform hardware resources, which limits the methods by which an attacker can attempt to compromise the integrity of the TOE.

The PP includes **FMT_CFG_EXT.1** for the TSF to limit unauthorized access to itself by preventing the use of default authentication credentials and by ensuring that the TOE uses appropriately restrictive platform permissions on its binaries and data.

The PP includes **FPT_AEX_EXT.1** to add complexity to the task of compromising systems by ensuring that application is compatible with security features provided by the platform vendor and that the application implements platform-provided anti-exploitations such as ASLR and stack overflow protection.

The PP includes **FPT_TUD_EXT.1** to ensure that the TOE can be patched and that any updates to the TOE have appropriate integrity protection.

O.QUALITY:

The PP supports this objective by allowing **FCS_CKM_EXT.1** to specify that the TSF may rely on platform-provided key generation services.

The PP supports this objective by allowing **FCS_RBG_EXT.1** to specify that the TSF may rely on platform-provided random bit generation services.

The PP supports this objective by allowing **FCS_STO_EXT.1** to specify that the TSF may rely on platform-provided credential storage services.

The PP supports this objective by allowing **FDP_DAR_EXT.1** to specify that the TSF may rely on platform-provided data-at-rest protection services.

The PP includes **FMT_MEC_EXT.1** to ensure that the TOE can use platform services to store and set configuration options.

The PP includes **FPT_API_EXT.1** to require the TOE to leverage platform functionality by using only documented and supported APIs.

The PP includes **FPT_LIB_EXT.1** to ensure that the TOE does not include any unnecessary or unexpected third-party libraries which could present a privacy threat or vulnerability.

The PP supports this objective by allowing **FTP_DIT_EXT.1** to specify that the TSF may rely on platform-provided services to implement trusted communications.

The PP includes **FPT_TUD_EXT.2** to specify that the TOE may leverage the platform-supported package manager for application distribution and leverages platform-provided mechanisms to remove all traces of itself when removed from the platform system.

O.MANAGEMENT:

The PP includes **FMT_SMF.1** to define the security-relevant management functions that are supported by the TOE.

The PP includes **FPR_ANO_EXT.1** to define how the TSF provides control to the user regarding the disclosure of any PII.

The PP includes **FPT_IDV_EXT.1** to provide a methodology for identifying the TOE versioning.

The PP includes **FPT_TUD_EXT.1** to define how updates to the TOE are deployed and verified.

O.PROTECTED_STORAGE:

The PP includes **FCS_RBG_EXT.1** to define whether random bit generation services are implemented by the TSF or the platform. Depending on how data at rest is protected, the TOE may rely on the use of a random bit generator to create keys that are subsequently used for data protection.

The PP includes **FCS_STO_EXT.1** to define the mechanism that the TSF uses or relies upon to protect stored credential data.

The PP includes **FDP_DAR_EXT.1** to define the mechanism that the TSF uses or relies upon to protect sensitive data at rest.

O.PROTECTED_COMMS:

The PP includes **FCS_CKM_EXT.1** to specify whether the TOE or the platform is responsible for generation of any asymmetric keys that may be used for establishing trusted communications.

The PP includes **FCS_RBG_EXT.1** to define whether the random bit generation services used in establishing trusted communications are implemented by the TSF or by the platform.

The PP includes **FDP_NET_EXT.1** to define the TOE's usage of network communications, which may include the transmission or receipt of data over a trusted channel.

The PP includes **FTP_DIT_EXT.1** to define the trusted channels used to protect data in transit, the data that is protected, and whether the trusted channels are implemented by the TSF or the platform.

The PP includes **FIA_X509_EXT.1** to define X.509 certificate validation activities in support of trusted communications.

The PP includes **FIA_X509_EXT.2** to define the trusted communications that X.509 certificate services support, as well as the extent to which trusted communications can be established when using a certificate with unknown validity.

6.3.3 SFR DEPENDENCY RATIONALE

6.3.3.1 TABLE OF SFR DEPENDENCIES

The following table lists the dependencies for each security functional requirement, indicating how they have been satisfied. The abbreviation "h.a." indicates that the dependency has been satisfied by a SFR that is hierarchically above the required dependency.

SFR	Required	Fulfilled	Missing
FCS_CKM_EXT.1	None	None	None
FCS_RBG_EXT.1	None	None	None
FCS_STO_EXT.1	None	None	None
FDP_DEC_EXT.1	None	None	None
FDP_NET_EXT.1	None	None	None
FDP_DAR_EXT.1	None	None	None
FMT_MEC_EXT.1	None	None	None
FMT_CFG_EXT.1	None	None	None
FMT_SMF.1	None	None	None
FPR_ANO_EXT.1	None	None	None
FPT_API_EXT.1	None	None	None
FPT_AEX_EXT.1	None	None	None
FPT_IDV_EXT.1	None	None	None
FPT_LIB_EXT.1	None	None	None
FPT_TUD_EXT.1	FPT_IDV_EXT.1	FPT_IDV_EXT.1	None
FPT_TUD_EXT.2	FPT_TUD_EXT.1	FPT_TUD_EXT.1	None
FTP_DIT_EXT.1	None	None	None
FIA_X509_EXT.1	None	None	None
FIA_X509_EXT.2	FIA_X509_EXT.1, [FTP_ITC.1 or FTP_TRP.1]	FIA_X509_EXT.1	[FTP_ITC.1 or FTP_TRP.1]

Table 3 SFR Dependencies

6.3.3.2 JUSTIFICATION FOR MISSING DEPENDENCIES

FIA_X509_EXT.2 dependency on [FTP_ITC.1 or FTP_TRP.1]

FTP_ITC.1 nor FTP_TRP.1 have not been included as it is not included in [PPAPP-14] to which the Security Target claims exact conformance.

6.3.4 SAR DEPENDENCY RATIONALE

6.3.4.1 TABLE OF SAR DEPENDENCIES

The following table lists the dependencies for each security assurance requirement, indicating how they have been satisfied. The abbreviation "h.a." indicates that the dependency has been satisfied by a SAR that is hierarchically above the required dependency.

SAR	Required	Fulfilled	Missing
ASE_CCL.1	ASE_INT.1, ASE_ECD.1, ASE_REQ.1	ASE_INT.1, ASE_ECD.1, ASE_REQ.1	None
ASE_ECD.1	None	None	None
ASE_INT.1	None	None	None
ASE_SPD.1	None	None	None
ASE_OBJ.2	ASE_SPD.1	ASE_SPD.1	None
ASE_REQ.2	ASE_OBJ.2, ASE_ECD.1	ASE_OBJ.2, ASE_ECD.1	None
ASE_TSS.1	ASE_INT.1, ASE_REQ.1, ADV_FSP.1	ASE_INT.1, ASE_REQ.2 (h.a. ASE_REQ.1), ADV_FSP.1	None
ALC_CMC.1	ALC_CMS.1	ALC_CMS.1	None
ALC_CMS.1	None	None	None
ADV_FSP.1	None	None	None
AGD_OPE.1	ADV_FSP.1	ADV_FSP.1	None
AGD_PRE.1	None	None	None
ATE_IND.1	ADV_FSP.1, AGD_OPE.1, AGD_PRE.1	ADV_FSP.1, AGD_OPE.1, AGD_PRE.1	None

AVA_VAN.1	ADV_FSP.1, AGD_OPE.1, AGD_PRE.1	ADV_FSP.1, AGD_OPE.1, AGD_PRE.1	None
ALC_TSU_EXT.1	None	None	None

Table 4 *SAR dependencies*

7 TOE SUMMARY SPECIFICATION

7.1 TOE SECURITY FUNCTIONALITY

7.1.1 CRYPTOGRAPHIC SUPPORT (FCS)

As declared in **FCS_CKM_EXT.1**, the TOE does not generate asymmetric cryptographic keys, it invokes the Windows platform in order to establish trusted communication channels; therefore, keys required to implement these channels are implicitly generated by the Windows platform itself, the TOE does not directly invoke asymmetric cryptographic keys generation services.

FCS_RBG_EXT.1 defines that the TOE does not use DRBG functionality, it invokes the Windows platform for encrypted storage of credentials and trusted communications. Therefore, the Windows platform itself is the one entity that calls on the DRBG services required.

As covered by **FCS_STO_EXT.1**, the TOE invokes platform functionality, in this case the Data Protection API (DPAPI), to securely store the advanced setup and uninstallation password managed by the TOE under the ESET related Windows Registry entries, the purpose of such password is to protect advanced setup configurations and prevent unauthorized uninstallation. The cryptography employed by the platform involves the use of SHA256 and AES-256-CBC. Other credentials are stored under the ESET related Windows Registry entries but these are not TOE related as they are related to the licensing required to obtain updates; these are “Password” and “LegacyPassword” in the ESET related Windows Registry entries.

7.1.2 USER DATA PROTECTION (FDP)

As addressed by **FDP_DEC_EXT.1**, the TOE restricts its access to the platform’s network connectivity hardware resource for the purposed defined in FDP_NET_EXT.1.

The only platform’s sensitive information that the TOE requires access to is the system logs, this repository is considered sensitive since it could include information that the enterprise or user environment may value as sensitive, for example, infrastructure information.

As defined by **FDP_NET_EXT.1**, the TOE restricts network communication to product and module updates and licensing. The following remote endpoints are involved:

Hostname	Description
update.gtm.eset.com	Module and detection engine updates
repository.gtm.eset.com	Product updates

In respect to sensitive data, the only case considered is the advanced setup and uninstallation password. The TOE stores this type of data in accordance with FCS_STO_EXT.1, this is addressed by **FDP_DAR_EXT.1**.

7.1.3 SECURITY MANAGEMENT (FMT)

In relation to **FMT_CFG_EXT.1**, when the TOE is installed, functionality is restricted based on the platform's access control this means that low privileged users log into the operating system are not able to change relevant configuration parameters (e.g.: deactivation of protection engines) or uninstall the product, providing a secure by default approach.

In addition to this, for further security, the TOE allows to configure an advanced setup and uninstallation password. Such password is not set by default on installation, administrators of the TOE are required to set it manually through the TOE interface Advanced Setup menu.

The TOE is automatically installed with the appropriate file permissions to prevent unauthorized access to the binaries, configuration settings, and data.

Following with the configuration of the TOE as addressed by **FMT_MEC_EXT.1**, parameters related to the different protection modules and behaviour of the TOE itself are stored using platform mechanisms, in this case the Windows Registry, under the ESET related Windows Registry entries (HKLM\SOFTWARE\ESET and HKCU\SOFTWARE\ESET). Among others, the parameters stored using platform mechanisms are those related to the detection engine (exclusions, malware scans...) and configuration of the protection modules, for example, detection response aggressiveness for malware detections, potentially unwanted or unsafe applications, suspicious applications, etc…. In addition, configuration parameters related to updates are also stored using platform mechanisms (e.g.: remote server address, enable/disable of automatic updates).

Moreover, other data required during the operational state of the TOE is managed under the %ProgramData%\ESET directory.

According to **FMT_SMF.1**, the TOE performs the following management functionality: product and module updates, malware scan, protection modules activation/deactivation and configuration and configuration of advanced setup and uninstallation protection.

7.1.4 PRIVACY (FPR)

The TOE does not specifically request any PII, the user is not prompted to introduce PII when the TOE is in the normal mode of operation; therefore, as addressed by **FPR_ANO_EXT.1**, it is considered that the TOE does not transmit PII over the network.

7.1.5 PROTECTION OF THE TSF (FPT)

As defined in **FPT_API_EXT.1**, the TOE only uses documented platform APIs, the complete list of APIs can be found in Annex A: Platform APIs.

The TOE is compiled with protection mechanisms to prevent attacks during its execution, this is addressed by **FPT_AEX_EXT.1**. The TOE supports address space layout randomization (ASLR) through the use of the following compilation flags:

- /HIGHENTROPYVA: Specifies whether the executable image supports high-entropy 64-bit address space layout randomization (ASLR).
- /DYNAMICBASE: Specifies whether to generate an executable image that can be randomly rebased at load time by using the address space layout randomization (ASLR) feature of Windows Operating System.

Moreover, the TOE does not request memory mapping to any explicit address. It also features the usage of DEP and GS compilation flags that prevent the allocation of memory pages with write and execute attributes simultaneously (following a W^X policy) and stack guards to increase protection against buffer overflow attacks. Write and execute allocations may be only carried out for a short period of time due to binary translation, as a consequence of emulation during scanning.

This W^X policy is also implemented by not writing user-modifiable files to directories that present executables files, preventing possible exploitation and privilege escalation attempts by attackers.

FPT_TUD_EXT.1 assures that the TOE provides mechanisms to query the current version and check for updates and patches. These functionalities are available to the user through the TOE intuitive interface. In order to preserve the integrity of the installation, the TOE does not modify its own binary code during the operational state of the TOE.

When executing an update process, the TOE contacts the ESET official repositories which are used as the source for the update files. These update packages are verified by the TOE by invoking platform-provided functionality prior to their installation using the digital signature that is incorporated. This signature, which uses SHA256 as digest algorithm and RSA as signature encryption algorithm according to the PKCS#1v1.5 signature scheme, is provided by an authorized source, in this case ESET. Such digital signature is supported by a certification path that involves Entrust Certification Authority, which is considered reputable and trustworthy.

Following with the integrity of the installation, the TOE is not bundled with the operating system, it is distributed through the ESET official webpage (eset.com) which provides the installation package. In relation to this, the application is packaged in a platform-supported format that allows to remove all traces when it is uninstalled or removed, as addressed by **FPT_TUD_EXT.2**.

As defined by **FPT_LIB_EXT.1**, the TOE only uses the list of third-party libraries declared in the present Security Target (Annex B: Third-party Libraries) to prevent the use of components that could present a privacy threat and ensure that technical vulnerabilities are correctly addressed.

In relation to **FPT_IDV_EXT.1**, ESET follows industry standards for product version numbering. The number version of the TOE (12.1.2057.3), from left to right, is composed of major version, minor version and build or patch number version separated by points. In addition to these three individual numbers, there is a fourth differentiator that indicates, for example, language version.

7.1.6 TRUSTED PATH/CHANNEL (FTP)

The TOE stablishes the following communication channels, as addressed by **FTP_DIT_EXT.1**:

- Communication channels established with the remote ESET servers with the objective to obtain updates.

The communication channel related to the remote ESET update servers is established by the TOE through the invoke of the platform-provided API in order to establish a secure connection. The communication channel features the usage of HTTPS and, therefore, TLS protocols. The TOE negotiates a TLSv1.2 connection using the cryptographic parameters provided by Windows and using the Windows Certificate Store as trust store to validate the certificate of the remote server.

7.1.7 IDENTIFICATION AND AUTHENTICATION (FIA)

The TOE performs certificate validation checking when establishing the following connections:

- The TOE to ESET remote update servers.

These connections involve the use of secure communication protocols, in this case, using the HTTPS protocol. This protocol implies the use of the TLS communication protocols, which provides the ability to authenticate the connection.

This authentication is performed by validating the certificate of the remote ESET servers invoking platform-provided functionality. These certificates follow the X.509v3 standard and validation algorithms as addressed by **FIA_X509_EXT.1** are considered. If for any reason it is not possible to determine the validity of a certificate, the certificate will be accepted and the connection is not established. This is addressed by **FIA_X509_EXT.2**.

The certificates are validated using the certificate path validation algorithm as defined in RFC 5280 and invokes-platform provided functionality to determine their trustworthiness using the Windows Certificate Store, ensuring that all certificate paths terminate with a trusted root CA certificate and that all CA certificates include the basicConstraints extension with the CA flag set to TRUE. Moreover, a Certificate Revocation List is used to validate the revocation status of the certificate. The certificate validation procedure will also ensure that the extendedKeyUsage field is properly set for all certificates depending on their intended usage.

The certificates of the remote ESET servers are issued and signed by a trustworthy and well-known CA. This CA is installed by default in the Windows Certificate store when the platform operating system is installed, therefore, further actions or configuration regarding this matter are not required.

The primary goal of path validation is to verify the binding between a subject distinguished name or a subject alternative name and subject public key, as represented in the target certificate, based on the public key of the trust anchor.

The certificate validation algorithm, as defined by [RFC-5280], takes the following nine inputs:

1. The certificate path to be evaluated.
2. The current date/time.
3. The list of certificate policy object identifiers (OIDs) acceptable to the relying party;

4. The trust anchor of the certificate path; and
5. Indicators whether the policy mapping is allowed and how, when, whether the any-policy OID is to be tolerated.
    5.1. initial-policy-mapping-inhibit, which indicates if policy mapping is allowed in the certification path.
    5.2. initial-explicit-policy, which indicates if the path must be valid for at least one of the certificate policies in the user-initial-policy-set.
    5.3. initial-any-policy-inhibit, which indicates whether the any-policy OID should be processed if it is included in a certificate.
    5.4. initial-permitted-subtrees, which indicates for each name type (e.g., X.500 distinguished names, email addresses, or IP addresses) a set of subtrees within which all subject names in every certificate in the certification path must fall.
    5.5. initial-excluded-subtrees, which indicates for each name type (e.g., X.500 distinguished names, email addresses, or IP addresses) a set of subtrees within which no subject name in any certificate in the certification path may fall.

To meet the goal, the path validation process verifies, among other things, that a prospective certification path (a sequence of n certificates) satisfies the following conditions:

a) for all x in {1, ..., n-1}, the subject of certificate x is the issuer of certificate x+1;
b) certificate 1 is issued by the trust anchor;
c) certificate n is the certificate to be validated (i.e., the target certificate); and
d) for all x in {1, ..., n}, the certificate was valid at the time in question.

7.2 TIMELY SECURITY UPDATES

This section covers the developer actions required by the component ALC_TSU_EXT.1.

ESET is a strong supporter of coordinated vulnerability disclosure process and publicly credits security vulnerability reporters for their efforts if they do not wish to remain anonymous.

ESET actively advocates for the coordinated vulnerability disclosure process and acknowledges security vulnerability reporters publicly for their contributions, if they prefer not to stay anonymous. The team of security specialists in ESET is dedicated to respond to potential security problems and making sure reports on such issues are handled properly.

The report policy to notify a hypothetical issue to ESET is the following:

- Users reach out via security@eset.com and send their reports and all related materials encrypted by ESET's active PGP public key and in English language. The PGP public key is available in the Report Policy section of the official ESET website related to the report of vulnerabilities.
- The content of the report shall follow the guidelines below:
    - Include organization and contact name of reporter.

- Include a clear description of the potential vulnerability. When assessing the vulnerability, use the latest version of CVSS - ESET will prioritize the response based on this CVSS score or vector string.
- Include all information needed to validate the potential vulnerability.
- Indicate ESET product and module version.
- Proof of concept – A description as detailed as possible, including screenshots and video (marked as private when uploaded to stream services).
- Include a log file from ESET SysInspector if possible.
- Include mitigation suggestions if possible.
- Include the impact that you expect the potential vulnerability has on users.

ESET requests the reporters to keep any communication regarding vulnerability confidential and inform about any disclosure plans and coordinate with the manufacturer.

An automatic reply is sent when report is successfully processed by ESET's system and within three working days a security specialist will send the reporter feedback via security@eset.com. Depending on the severity of the reported issue, it is included in the development roadmap for the product with a different level of priority. The target of ESET is to provide a fix for confirmed vulnerabilities within 90 calendar days of disclosure.

As a CVE Numbering Authority (CNA) for applicable vulnerabilities in ESET's products, ESET will reserve a CVE ID automatically.

When a security issue is addressed and a patch or hotfix is released, since the TOE allows to check the installed version and also allows checking the updates manually, users are able to install newer versions of the product. It is possible to enable automatic updates installation, moreover, before installing this type of updates, ESET Endpoint Security displays "Security Alert. Restart required." or "Security and stability update to newer version is prepared. Restart your computer for all changes to take effect".

8 ACRONYMS

The following table shows the acronyms used in this document.

Acronym	Meaning
PP	Protection Profile
CC	Common Criteria
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFi	TSF Interface
OSP	Organisational Security Policies
EAL	Evaluation Assurance Level
ST	Security Target
IT	Information Technology
RMM	Remote Monitoring and Management
CVE	Common Vulnerabilities and Exposures
CNA	CVE Numbering Authority
API	Application Programming Interface
DPAPI	Data Protection API
ASLR	Address Space Layout Randomization
DEP	Data Execution Prevention
GS	Guard Stack

Table 5 *Abbreviations*

9 GLOSSARY OF TERMS

Term	Meaning
Augmentation	Addition of one or more requirement(s) to a package
Evaluation Assurance Level	Set of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale, that form an assurance package
Operational Environment	Environment in which the TOE is operated
Protection Profile	Implementation-independent statement of security needs for a TOE type
Security Target	Implementation-dependent statement of security needs for a specific identified TOE
Target Of Evaluation	Set of software, firmware and/or hardware possibly accompanied by guidance

Table 6 *Glossary of terms*

10 DOCUMENT REFERENCES

The following table shows the acronyms used in this document.

Reference	Document
[CC31R5P1]	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, Part 1: Introduction and general model
[CC31R5P2]	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, Part 2: Security functional components
[CC31R5P3]	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, Part 3: Security assurance components
[CEM31R5P3]	Common Criteria Evaluation methodology, Version 3.1, Revision 5
[PPAPP-14]	Protection Profile for Application Software, Version 1.4, 2021-10-07
[RFC-5280]	RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (https://datatracker.ietf.org/doc/html/rfc5280)

Table 7 List of document references

11 ANNEX A: PLATFORM APIS

AccessCheck,AccessibleObjectFromWindow,AcquireSRWLockExclusive,AcquireSRWLockShared,AddAccessAllowedAce,AddAccessAllowedAceEx,AddFontMemResourceEx,AdjustTokenPrivileges,AdjustWindowRectEx,AllocConsole,AllocateAndInitializeSid,AllowSetForegroundWindow,AnimateWindow,AppendMenuW,AreFileApisANSI,AttachConsole,AttachThreadInput,AuthzAccessCheck,AuthzFreeContext,AuthzFreeResourceManager,AuthzInitializeContextFromSid,AuthzInitializeResourceManager,BCryptCloseAlgorithmProvider,BCryptCreateHash,BCryptDecrypt,BCryptDestroyHash,BCryptDestroyKey,BCryptFinishHash,BCryptGenerateSymmetricKey,BCryptGetProperty,BCryptHashData,BCryptImportKeyPair,BCryptOpenAlgorithmProvider,BCryptVerifySignature,Beep,BeginBufferedPaint,BeginDeferWindowPos,BeginPaint,BitBlt,CLSIDFromString,CM_Disable_DevNode,CM_Enable_DevNode,CM_Get_DevNode_PropertyW,CM_Query_And_Remove_SubTreeW,CM_Reenumerate_DevNode,CallNextHookEx,CallWindowProcW,CancelIoEx,CancelMibChangeNotify2,CancelThreadpoolIo,CertAddCertificateContextToStore,CertAddEncodedCertificateToStore,CertCloseStore,CertCompareCertificateName,CertComparePublicKeyInfo,CertControlStore,CertCreateCertificateContext,CertDeleteCertificateFromStore,CertDuplicateCertificateContext,CertEnumCRLsInStore,CertEnumCertificatesInStore,CertFindCertificateInStore,CertFreeCertificateChain,CertFreeCertificateContext,CertGetCertificateChain,CertGetCertificateContextProperty,CertGetNameStringW,CertNameToStrW,CertOpenStore,CertSetCertificateContextProperty,CertVerifyCertificateChainPolicy,ChangeServiceConfig2W,ChangeServiceConfigW,ChangeTimerQueueTimer,CharNextW,CharUpperBuffW,CharUpperW,CheckDlgButton,CheckMenuItem,CheckMenuRadioItem,CheckRemoteDebuggerPresent,CheckTokenMembership,ClientToScreen,CloseClipboard,CloseEventLog,CloseHandle,ClosePrinter,CloseServiceHandle,CloseThreadpool,CloseThreadpoolCleanupGroup,CloseThreadpoolCleanupGroupMembers,CloseThreadpoolIo,CloseThreadpoolTimer,CloseThreadpoolWait,CloseThreadpoolWork,CloseTrace,CmRegisterCallback,CmUnRegisterCallback,CoAddRefServerProcess,CoCreateGuid,CoCreateInstance,CoFreeUnusedLibraries,CoGetApartmentType,CoGetObjectContext,CoInitialize,CoInitializeEx,CoInitializeSecurity,CoRegisterClassObject,CoRegisterMessageFilter,CoReleaseServerProcess,CoRevokeClassObject,CoSetProxyBlanket,CoTaskMemAlloc,CoTaskMemFree,CoTaskMemRealloc,CoUninitialize,CombineRgn,CommDlgExtendedError,CompareFileTime,CompareStringEx,CompareStringW,ConnectNamedPipe,ControlService,ControlTraceW,ConvertSecurityDescriptorToStringSecurityDescriptorW,ConvertSidToStringSidW,ConvertStringSecurityDescriptorToSecurityDescriptorW,ConvertStringSidToSidW,ConvertThreadToFiber,CopyFileW,CopyRect,CopySid,CountClipboardFormats,CreateBitmap,CreateBrushIndirect,CreateCaret,CreateCompatibleBitmap,CreateCompatibleDC,CreateCursor,CreateDIBPatternBrushPt,CreateDIBSection,CreateDialogIndirectParamW,CreateDirectoryW,CreateEnvironmentBlock,CreateEventA,CreateEventExW,CreateEventW,CreateFiberEx,CreateFileA,CreateFileMappingA,CreateFileMappingW,CreateFileW,CreateFontA,CreateFontIndirectW,CreateHardLinkW,CreateHatchBrush,CreateICW,CreateILockBytesOnHGlobal,CreateIconFromResourceEx,CreateIconIndirect,CreateIoCompletionPort,CreateMenu,CreateMutexA,CreateMutexW,CreateNamedPipeW,CreatePatternBrush,CreatePen,CreatePipe,CreatePopupMenu,CreateProcessA,CreateProcessAsUserW,CreateProcessW,CreateRectRgn,CreateRectRgnIndirect,CreateRemoteThread,CreateSemaphoreExW,CreateSemaphoreW,CreateServiceW,CreateSolidBrush,CreateStdAccessibleObject,CreateSymbolicLinkW,CreateThread,CreateThreadpool,CreateThreadpoolCleanupGroup,CreateThreadpoolIo,CreateThreadpoolTimer,CreateThreadpoolWait,CreateThreadpoolWork,CreateTimerQueue,CreateTimerQueueTimer,CreateToolhelp32Snapshot,CreateTransaction,CreateWellKnownSid,CreateWindowExA,CreateWindowExW,CryptAcquire

ContextA,CryptAcquireContextW,CryptCATAdminAcquireContext,CryptCATAdminAcquireContext2,CryptCATAdminAddCatalog,CryptCATAdminCalcHashFromFileHandle,CryptCATAdminEnumCatalogFromHash,CryptCATAdminReleaseCatalogContext,CryptCATAdminReleaseContext,CryptCATAdminRemoveCatalog,CryptCATCatalogInfoFromContext,CryptCreateHash,CryptDecodeObject,CryptDecodeObjectEx,CryptDecrypt,CryptDestroyHash,CryptDestroyKey,CryptEncodeObject,CryptEncrypt,CryptExportKey,CryptExportPublicKeyInfo,CryptFindOIDInfo,CryptGenKey,CryptGenRandom,CryptGetHashParam,CryptGetProvParam,CryptGetUserKey,CryptHashCertificate,CryptHashData,CryptImportKey,CryptImportPublicKeyInfo,CryptMemFree,CryptMsgClose,CryptMsgGetParam,CryptMsgOpenToDecode,CryptMsgUpdate,CryptProtectData,CryptProtectMemory,CryptQueryObject,CryptReleaseContext,CryptRetrieveObjectByUrlW,CryptStringToBinaryA,CryptUnprotectData,CryptUnprotectMemory,CryptVerifyCertificateSignatureEx,CryptVerifySignatureW,DPtoLP,DbgPrint,DefWindowProcA,DefWindowProcW,DeferWindowPos,DeleteCriticalSection,DeleteDC,DeleteFiber,DeleteFileA,DeleteFileW,DeleteMenu,DeleteObject,DeleteService,DeleteTimerQueueTimer,DeregisterEventSource,DestroyCaret,DestroyEnvironmentBlock,DestroyIcon,DestroyMenu,DestroyPrivateObjectSecurity,DestroyWindow,DeviceIoControl,DialogBoxIndirectParamW,DisableThreadLibraryCalls,DisconnectNamedPipe,DispatchMessageA,DoDragDrop,DosDateTimeToFileTime,DragQueryFileW,DrawEdge,DrawFocusRect,DrawFrameControl,DrawIconEx,DrawTextA,DrawTextExW,DrawTextW,DsGetDcNameW,DsRoleFreeMemory,DsRoleGetPrimaryDomainInformation,DuplicateHandle,DuplicateToken,DuplicateTokenEx,Ellipse,EmptyClipboard,EnableMenuItem,EnableTrace,EnableTraceEx,EnableTraceEx2,EnableWindow,EndBufferedPaint,EndDeferWindowPos,EndDialog,EndDoc,EndPage,EndPaint,EnterCriticalSection,EnumChildWindows,EnumClipboardFormats,EnumDesktopWindows,EnumFontFamiliesExA,EnumFontFamiliesExW,EnumProcessModules,EnumProcesses,EnumServicesStatusExW,EnumServicesStatusW,EnumSystemLocalesW,EnumThreadWindows,EnumUILanguagesW,EnumerateTraceGuidsEx,EqualRect,EqualSid,Escape,EtwActivityIdControl,EtwRegister,EtwUnregister,EtwWriteTransfer,EventActivityIdControl,EventRegister,EventUnregister,EventWrite,EventWriteTransfer,ExAcquireFastMutex,ExAcquireFastMutexUnsafe,ExAcquireResourceExclusiveLite,ExAcquireResourceSharedLite,ExAllocatePoolWithTag,ExAllocateTimer,ExCreateCallback,ExDeleteNPagedLookasideList,ExDeletePagedLookasideList,ExDeleteResourceLite,ExDeleteTimer,ExFreePool,ExFreePoolWithTag,ExGetPreviousMode,ExInitializeNPagedLookasideList,ExInitializePagedLookasideList,ExInitializeResourceLite,ExInterlockedInsertHeadList,ExInterlockedInsertTailList,ExInterlockedRemoveHeadList,ExQueryDepthSList,ExQueueWorkItem,ExRegisterCallback,ExReleaseFastMutex,ExReleaseFastMutexUnsafe,ExReleaseResourceLite,ExSetTimer,ExUnregisterCallback,ExUuidCreate,ExcludeClipRect,ExitProcess,ExitThread,ExitWindowsEx,ExpInterlockedPopEntrySList,ExpInterlockedPushEntrySList,ExpandEnvironmentStringsA,ExpandEnvironmentStringsForUserW,ExpandEnvironmentStringsW,ExtTextOutW,ExtractIconExW,FileTimeToLocalFileTime,FileTimeToSystemTime,FillRect,FilterInstanceFindClose,FilterInstanceFindFirst,FilterInstanceFindNext,FilterVolumeFindClose,FilterVolumeFindFirst,FilterVolumeFindNext,FindClose,FindCloseChangeNotification,FindFirstChangeNotificationW,FindFirstFileExA,FindFirstFileExW,FindFirstFileW,FindFirstVolumeW,FindNextChangeNotification,FindNextFileA,FindNextFileW,FindNextVolumeW,FindResourceA,FindResourceExW,FindResourceW,FindVolumeClose,FindWindowA,FindWindowExW,FindWindowW,FlsAlloc,FlsFree,FlsGetValue,FlsSetValue,FltAllocateContext,FltAllocateDeferredIoWorkItem,FltCancelFileOpen,FltCancellableWaitForMultipleObjects,FltClose,FltCompletePendedPostOperation,FltCreateFile,FltDeleteStreamHandleContext,FltDeleteVolumeContext,FltDeviceIoControlFile,FltFreeDeferredIoWorkItem,FltFreeExtraCreateParameter,FltFsControlFile,FltGetDestinationFileNameInformation,FltGetDeviceObject,FltGetDiskDeviceObject,FltGetFileNameInformation,FltGetFileSy stemType,FltGetFilterFromInstance,FltGetRequestorProcess,FltGetRequestorProcessId,FltGetRoutineAddress,FltGetStreamContext,FltGetStreamHandleContext,FltGetVolumeContext,FltGetVolumeFromFileObject,FltGetVolumeFromInstance,FltGetVolumeFromName,FltGetVolumeInstanceFromName,FltGetVolumeName,FltGetVolumeProperties,FltIsDirectory,FltIsEcpAcknowledged,FltObjectDereference,FltObjectReference,FltParseFileNameInformation,FltQueryInformationFile,FltQueryVolumeInformation,FltQueueDeferredIoWorkItem,FltReferenceContext,FltRegisterFilter,FltReissueSynchronousIo,FltReleaseContext,FltSetCallbackDataDirty,FltSetEcpListIntoCallbackData,FltSetStreamContext,FltSetStreamHandleContext,FltSetVolumeContext,FltStartFiltering,FltSupportsStreamHandleContexts,FltUnregisterFilter,FlushFileBuffers,FlushInstructionCache,FlushProcessWriteBuffers,FlushViewOfFile,FormatMessageA,FormatMessageW,FrameRect,FreeConsole,FreeEnvironmentStringsW,FreeLibrary,FreeLibraryAndExitThread,FreeLibraryWhenCallbackReturns,FreeMibTable,FreeResource,FreeSid,FwpmBfeStateGet0,FwpmBfeStateSubscribeChanges0,FwpmBfeStateUnsubscribeChanges0,FwpmCalloutAdd0,FwpmCalloutDeleteByKey0,FwpmCalloutGetByKey0,FwpmEngineClose0,FwpmEngineOpen0,FwpmFilterAdd0,FwpmFilterCreateEnumHandle0,FwpmFilterDeleteByKey0,FwpmFilterDestroyEnumHandle0,FwpmFilterEnum0,FwpmFilterGetByKey0,FwpmFilterGetSecurityInfoByKey0,FwpmFilterSetSecurityInfoByKey0,FwpmFilterSubscribeChanges0,FwpmFilterUnsubscribeChanges0,FwpmFreeMemory0,FwpmLayerCreateEnumHandle0,FwpmLayerDestroyEnumHandle0,FwpmLayerEnum0,FwpmProviderAdd0,FwpmProviderDeleteByKey0,FwpmProviderGetByKey0,FwpmSubLayerAdd0,FwpmSubLayerDeleteByKey0,FwpmSubLayerGetByKey0,FwpmTransactionAbort0,FwpmTransactionBegin0,FwpmTransactionCommit0,FwpsAllocateNetBufferAndNetBufferList0,FwpsCalloutRegister0,FwpsCalloutUnregisterById0,FwpsCloneStreamData0,FwpsCompleteOperation0,FwpsConstructIpHeaderForTransportPacket0,FwpsCopyStreamDataToBuffer0,FwpsDereferenceNetBufferList0,FwpsDiscardClonedStreamData0,FwpsFlowAbort0,FwpsFlowAssociateContext0,FwpsFlowRemoveContext0,FwpsFreeNetBufferList0,FwpsInjectTransportReceiveAsync0,FwpsInjectTransportSendAsync0,FwpsInjectTransportSendAsync1,FwpsInjectionHandleCreate0,FwpsInjectionHandleDestroy0,FwpsPendOperation0,FwpsQueryPacketInjectionState0,FwpsReferenceNetBufferList0,FwpsStreamInjectAsync0,GdipAddPathBezier,GdipAddPathLine,GdipAlloc,GdipCloneBrush,GdipCloneImage,GdipClosePathFigure,GdipCreateBitmapFromScan0,GdipCreateBitmapFromStream,GdipCreateFromHDC,GdipCreateHBITMAPFromBitmap,GdipCreateImageAttributes,GdipCreateLineBrushI,GdipCreateMatrix,GdipCreatePath,GdipCreatePen1,GdipCreateSolidFill,GdipDeleteBrush,GdipDeleteGraphics,GdipDeleteMatrix,GdipDeletePath,GdipDeletePen,GdipDisposeImage,GdipDisposeImageAttributes,GdipDrawEllipseI,GdipDrawImageRectRectI,GdipFillEllipseI,GdipFillPath,GdipFree,GdipGetImageEncoders,GdipGetImageEncodersSize,GdipGetImageGraphicsContext,GdipGetImageHeight,GdipGetImagePixelFormat,GdipGetImageWidth,GdipSaveImageToStream,GdipScaleMatrix,GdipSetImageAttributesWrapMode,GdipSetInterpolationMode,GdipSetSmoothingMode,GdipStartPathFigure,GdipTransformPath,GdipTranslateMatrix,GdiplusShutdown,GdiplusStartup,GetACP,GetAce,GetAclInformation,GetActiveProcessorCount,GetActiveWindow,GetAdaptersAddresses,GetAsyncKeyState,GetBitmapBits,GetBufferedPaintBits,GetCPInfo,GetCapture,GetCaretBlinkTime,GetClassInfoExA,GetClassInfoExW,GetClassInfoW,GetClassLongPtrA,GetClassLongPtrW,GetClassNameW,GetClientRect,GetClipBox,GetClipRgn,GetClipboardData,GetClipboardSequenceNumber,GetCommandLineA,GetCommandLineW,GetComputerNameA,GetComputerNameExW,GetComputerNameW,GetConsoleCP,GetConsoleMode,GetConsoleOutputCP,GetConsoleScreenBufferInfo,GetConsoleWindow,GetCurrencyFormatW,GetCurrentObject,GetCurrentProcess,GetCurrentProcessId,GetCurrentProcessorNumber,GetCurrentThread,GetCurrentThreadId,GetCursorPos,GetDC,GetDCPenColor,GetDIBits,GetDateFormatW,GetDesktopWindow,GetDeviceCaps

,GetDiskFreeSpaceA,GetDiskFreeSpaceExW,GetDiskFreeSpaceW,GetDlgCtrlID,GetDlgItem,GetDllDirectoryW,GetDoubleClickTime,GetDriveTypeW,GetEnvironmentStringsW,GetEnvironmentVariableA,GetEnvironmentVariableW,GetExitCodeProcess,GetExitCodeThread,GetExtendedTcpTable,GetExtendedUdpTable,GetFileAttributesA,GetFileAttributesExW,GetFileAttributesW,GetFileInformationByHandle,GetFileInformationByHandleEx,GetFileSecurityW,GetFileSize,GetFileSizeEx,GetFileTime,GetFileType,GetFileVersionInfoExW,GetFileVersionInfoSizeExW,GetFileVersionInfoSizeW,GetFileVersionInfoW,GetFinalPathNameByHandleW,GetFocus,GetForegroundWindow,GetFullPathNameA,GetFullPathNameW,GetGeoInfoW,GetGlyphOutlineW,GetIconInfo,GetIpNetTable,GetIpNetTable2,GetKernelObjectSecurity,GetKerningPairsA,GetKeyState,GetKeyboardLayout,GetLastActivePopup,GetLastError,GetLengthSid,GetLocalTime,GetLocaleInfoA,GetLocaleInfoEx,GetLocaleInfoW,GetLogicalDriveStringsW,GetLogicalDrives,GetLogicalProcessorInformation,GetLongPathNameW,GetMapMode,GetMappedFileNameW,GetMenu,GetMenuCheckMarkDimensions,GetMenuItemCount,GetMenuItemID,GetMenuItemInfoW,GetMenuState,GetMenuStringW,GetMessageA,GetMessagePos,GetMessageTime,GetModuleFileNameA,GetModuleFileNameExW,GetModuleFileNameW,GetModuleHandleA,GetModuleHandleExW,GetModuleHandleW,GetModuleInformation,GetNamedSecurityInfoW,GetNativeSystemInfo,GetNextDlgTabItem,GetNumaHighestNodeNumber,GetNumberFormatW,GetNumberOfConsoleInputEvents,GetOEMCP,GetObjectA,GetObjectW,GetOpenFileNameW,GetOverlappedResult,GetPackageFullName,GetParent,GetPixel,GetPrivateProfileIntW,GetPrivateProfileStringW,GetProcAddress,GetProcessAffinityMask,GetProcessDefaultLayout,GetProcessHeap,GetProcessId,GetProcessImageFileNameW,GetProcessInformation,GetProcessTimes,GetPropW,GetQueueStatus,GetQueuedCompletionStatus,GetSaveFileNameW,GetScrollInfo,GetScrollPos,GetSecurityDescriptorDacl,GetSecurityDescriptorGroup,GetSecurityDescriptorOwner,GetShellWindow,GetShortPathNameW,GetSidIdentifierAuthority,GetSidLengthRequired,GetSidSubAuthority,GetSidSubAuthorityCount,GetStartupInfoW,GetStdHandle,GetStockObject,GetStringTypeA,GetStringTypeW,GetSubMenu,GetSysColor,GetSysColorBrush,GetSystemDefaultLocaleName,GetSystemDefaultUILanguage,GetSystemDirectoryW,GetSystemInfo,GetSystemMenu,GetSystemMetrics,GetSystemPowerStatus,GetSystemTime,GetSystemTimeAsFileTime,GetSystemWindowsDirectoryW,GetSystemWow64DirectoryW,GetTempFileNameA,GetTempFileNameW,GetTempPathA,GetTempPathW,GetTextAlign,GetTextColor,GetTextExtentExPointW,GetTextExtentPoint32A,GetTextExtentPoint32W,GetTextMetricsA,GetTextMetricsW,GetThreadContext,GetThreadDesktop,GetThreadId,GetThreadLocale,GetThreadPriority,GetThreadTimes,GetTickCount,GetTickCount64,GetTimeFormatW,GetTimeZoneInformation,GetTokenInformation,GetTopWindow,GetTraceEnableFlags,GetTraceEnableLevel,GetTraceLoggerHandle,GetUpdateRect,GetUserDefaultLCID,GetUserDefaultUILanguage,GetUserGeoID,GetUserNameA,GetUserNameExW,GetUserNameW,GetVersion,GetVersionExA,GetVersionExW,GetViewportExtEx,GetVolumeInformationW,GetVolumeNameForVolumeMountPointW,GetVolumePathNameW,GetVolumePathNamesForVolumeNameW,GetWindow,GetWindowContextHelpId,GetWindowDC,GetWindowExtEx,GetWindowLongA,GetWindowLongPtrA,GetWindowLongPtrW,GetWindowLongW,GetWindowOrgEx,GetWindowPlacement,GetWindowRect,GetWindowTextLengthW,GetWindowTextW,GetWindowThreadProcessId,GetWindowsDirectoryW,GlobalAddAtomW,GlobalAlloc,GlobalDeleteAtom,GlobalFindAtomW,GlobalFlags,GlobalFree,GlobalHandle,GlobalLock,GlobalMemoryStatus,GlobalMemoryStatusEx,GlobalReAlloc,GlobalSize,GlobalUnlock,GrayStringW,HeapAlloc,HeapCompact,HeapCreate,HeapDestroy,HeapFree,HeapQueryInformation,HeapReAlloc,HeapSetInformation,HeapSize,HeapValidate,HeapWalk,HttpOpenRequestA,HttpOpenRequestW,HttpQueryInfoA,HttpSendRequestA,HttpSendRequestW,IIDFromString,ImageList_Add,ImageList_Create,ImageList_Destroy,ImageList_DrawEx,ImageList_GetIconSize,I mageList_GetImageInfo,ImageList_ReplaceIcon,ImmAssociateContextEx,ImmGetCompositionStringW,ImmGetContext,ImmIsIME,ImmNotifyIME,ImmReleaseContext,ImmSetCandidateWindow,ImpersonateLoggedOnUser,ImpersonateSelf,InflateRect,InitOnceBeginInitialize,InitOnceComplete,InitOnceExecuteOnce,InitializeAcl,InitializeConditionVariable,InitializeCriticalSection,InitializeCriticalSectionAndSpinCount,InitializeCriticalSectionEx,InitializeProcThreadAttributeList,InitializeSListHead,InitializeSRWLock,InitializeSecurityDescriptor,InitializeSid,InitiateShutdownW,InsertMenuItemW,InsertMenuW,InterlockedFlushSList,InterlockedPopEntrySList,InterlockedPushEntrySList,InternetCloseHandle,InternetCombineUrlA,InternetConnectA,InternetConnectW,InternetErrorDlg,InternetGetLastResponseInfoA,InternetInitializeAutoProxyDll,InternetOpenA,InternetOpenUrlW,InternetOpenW,InternetQueryOptionA,InternetReadFile,InternetSetOptionA,InternetSetOptionW,IntersectClipRect,IntersectRect,InvalidateRect,InvertRect,IoAllocateMdl,IoAllocateWorkItem,IoAttachDeviceToDeviceStack,IoAttachDeviceToDeviceStackSafe,IoBuildDeviceIoControlRequest,IoBuildSynchronousFsdRequest,IoCreateDevice,IoCreateFileSpecifyDeviceObjectHint,IoCreateSymbolicLink,IoCsqInitialize,IoCsqInsertIrp,IoCsqRemoveNextIrp,IoDeleteDevice,IoDeleteSymbolicLink,IoDetachDevice,IoEnumerateDeviceObjectList,IoFreeMdl,IoFreeWorkItem,IoGetAttachedDeviceReference,IoGetCurrentProcess,IoGetDeviceInterfaces,IoGetDeviceObjectPointer,IoGetDeviceProperty,IoGetDevicePropertyData,IoGetInitialStack,IoGetRelatedDeviceObject,IoGetRequestorProcess,IoGetRequestorProcessId,IoGetStackLimits,IoGetTopLevelIrp,IoInitializeWorkItem,IoIs32bitProcess,IoIsWdmVersionAvailable,IoOpenDeviceRegistryKey,IoQueryFileDosDeviceName,IoQueryFileInformation,IoQueueWorkItem,IoQueueWorkItemEx,IoRegisterDeviceInterface,IoSetDeviceInterfaceState,IoSizeofWorkItem,IoThreadToProcess,IoUninitializeWorkItem,IoWMIRegistrationControl,IofCallDriver,IofCompleteRequest,IsBadReadPtr,IsBadStringPtrA,IsChild,IsClipboardFormatAvailable,IsDebuggerPresent,IsDialogMessageW,IsDlgButtonChecked,IsIconic,IsMenu,IsProcessorFeaturePresent,IsTextUnicode,IsThreadpoolTimerSet,IsTokenRestricted,IsUserAnAdmin,IsValidCodePage,IsValidLocale,IsValidSecurityDescriptor,IsValidSid,IsWellKnownSid,IsWindow,IsWindowEnabled,IsWindowUnicode,IsWindowVisible,IsWow64Process,IsWow64Process2,IsZoomed,KeAcquireGuardedMutex,KeAcquireGuardedMutexUnsafe,KeAcquireInStackQueuedSpinLock,KeAcquireSpinLockAtDpcLevel,KeAcquireSpinLockRaiseToDpc,KeBugCheckEx,KeCancelTimer,KeClearEvent,KeDelayExecutionThread,KeEnterCriticalRegion,KeEnterGuardedRegion,KeExpandKernelStackAndCallout,KeExpandKernelStackAndCalloutEx,KeFlushQueuedDpcs,KeGetCurrentIrql,KeGetCurrentThread,KeInitializeDpc,KeInitializeEvent,KeInitializeGuardedMutex,KeInitializeMutex,KeInitializeSemaphore,KeInitializeSpinLock,KeInitializeTimer,KeInsertQueueDpc,KeLeaveCriticalRegion,KeLeaveGuardedRegion,KeQueryPerformanceCounter,KeQueryPriorityThread,KeQuerySystemTime,KeQueryTimeIncrement,KeReadStateEvent,KeReleaseGuardedMutex,KeReleaseGuardedMutexUnsafe,KeReleaseInStackQueuedSpinLock,KeReleaseMutex,KeReleaseSemaphore,KeReleaseSpinLock,KeReleaseSpinLockFromDpcLevel,KeResetEvent,KeSetEvent,KeSetKernelStackSwapEnable,KeSetTimer,KeStackAttachProcess,KeUnstackDetachProcess,KeWaitForMultipleObjects,KeWaitForSingleObject,KillTimer,LCIDToLocaleName,LCMapStringEx,LCMapStringW,LPtoDP,LeaveCriticalSection,LineTo,LoadAcceleratorsW,LoadBitmapW,LoadCursorA,LoadCursorFromFileA,LoadCursorW,LoadIconW,LoadImageW,LoadLibraryA,LoadLibraryExA,LoadLibraryExW,LoadLibraryW,LoadResource,LoadStringW,LoadUserProfileW,LocalAlloc,LocalFileTimeToFileTime,LocalFree,LocalReAlloc,LocaleNameToLCID,LockFile,LockFileEx,LockResource,LogonUserW,LookupAccountNameW,LookupAccountSidLocalA,LookupAccountSidLocalW,LookupAccountSidW,LookupPrivilegeDisplayNameW,LookupPrivilegeNameW,LookupPrivilegeValueW,LresultFromObject,LsaEnumerateLogonSessions,LsaFreeReturnBuffer,LsaGetLogonSessionData,LsaNtStatusToWinError,MakeAbsoluteSD,MapGenericMask,MapViewOfFile,MapViewOfFileEx,M apWindowPoints,MessageBeep,MessageBoxW,MmBuildMdlForNonPagedPool,MmGetPhysicalAddress,MmGetSystemRoutineAddress,MmIsAddressValid,MmLockPagableDataSection,MmMapIoSpace,MmMapLockedPagesSpecifyCache,MmProbeAndLockPages,MmUnlockPagableImageSection,MmUnlockPages,MmUnmapIoSpace,MmUnmapLockedPages,ModifyMenuW,Module32FirstW,Module32NextW,MonitorFromWindow,MoveFileExW,MoveFileW,MoveToEx,MoveWindow,MsgWaitForMultipleObjects,MsgWaitForMultipleObjectsEx,MsiCloseHandle,MsiDatabaseOpenViewW,MsiEnumFeaturesW,MsiEnumRelatedProductsW,MsiOpenDatabaseW,MsiQueryFeatureStateW,MsiRecordDataSize,MsiRecordGetFieldCount,MsiRecordGetStringW,MsiRecordIsNull,MsiViewExecute,MsiViewFetch,MsiViewGetColumnInfo,MulDiv,MultiByteToWideChar,NCryptCreatePersistedKey,NCryptDecrypt,NCryptDeleteKey,NCryptEncrypt,NCryptFinalizeKey,NCryptFreeObject,NCryptOpenKey,NCryptOpenStorageProvider,NCryptSetProperty,NdisAdvanceNetBufferDataStart,NdisAdvanceNetBufferListDataStart,NdisAllocateCloneNetBufferList,NdisAllocateCloneOidRequest,NdisAllocateGenericObject,NdisAllocateMdl,NdisAllocateMemoryWithTagPriority,NdisAllocateNetBuffer,NdisAllocateNetBufferList,NdisAllocateNetBufferListPool,NdisAllocateNetBufferPool,NdisCopyReceiveNetBufferListInfo,NdisDeregisterDeviceEx,NdisFCancelOidRequest,NdisFCancelSendNetBufferLists,NdisFDeregisterFilterDriver,NdisFDevicePnPEventNotify,NdisFIndicateReceiveNetBufferLists,NdisFIndicateStatus,NdisFNetPnPEvent,NdisFOidRequest,NdisFOidRequestComplete,NdisFPauseComplete,NdisFRegisterFilterDriver,NdisFReturnNetBufferLists,NdisFSendNetBufferLists,NdisFSendNetBufferListsComplete,NdisFSetAttributes,NdisFreeCloneNetBufferList,NdisFreeCloneOidRequest,NdisFreeGenericObject,NdisFreeMdl,NdisFreeMemory,NdisFreeNetBuffer,NdisFreeNetBufferList,NdisFreeNetBufferListPool,NdisFreeNetBufferPool,NdisGeneratePartialCancelId,NdisGetDataBuffer,NdisGetDeviceReservedExtension,NdisGetRoutineAddress,NdisGetVersion,NdisRegisterDeviceEx,NdisRetreatNetBufferDataStart,NdisRetreatNetBufferListDataStart,NdisSetEvent,NetApiBufferFree,NetGetAnyDCName,NetGetDCName,NetScheduleJobEnum,NetUserChangePassword,NetUserGetInfo,NetUserModalsGet,NotifyIpInterfaceChange,NotifyServiceStatusChangeW,NotifyWinEvent,NtClose,NtCreateFile,NtCreateKey,NtDeleteKey,NtDeleteValueKey,NtEnumerateKey,NtEnumerateValueKey,NtMapViewOfSection,NtOpenFile,NtOpenKey,NtOpenSection,NtQueryInformationFile,NtQueryInformationProcess,NtQueryInformationThread,NtQueryKey,NtQueryObject,NtQuerySystemInformation,NtQueryValueKey,NtQueryVirtualMemory,NtQueryVolumeInformationFile,NtSetSecurityObject,NtSetValueKey,ObOpenObjectByPointer,ObQueryNameString,ObReferenceObjectByHandle,ObReferenceObjectByPointer,ObRegisterCallbacks,ObUnRegisterCallbacks,ObfReferenceObject,OffsetRect,OffsetViewportOrgEx,OleFlushClipboard,OleInitialize,OleIsCurrentClipboard,OleRun,OleUIBusyW,OleUninitialize,OpenClipboard,OpenEventLogW,OpenEventW,OpenFileById,OpenFileMappingW,OpenMutexW,OpenProcess,OpenProcessToken,OpenSCManagerW,OpenServiceW,OpenThread,OpenThreadToken,OpenTraceW,OutputDebugStringA,OutputDebugStringW,PatBlt,PathAddBackslashW,PathAddExtensionW,PathAppendW,PathCombineW,PathFileExistsW,PathIsDirectoryW,PathRemoveBackslashW,PathRemoveFileSpecW,PathStripPathW,PathStripToRootW,PeekMessageA,PeekMessageW,PeekNamedPipe,PoCallDriver,PoStartNextPowerIrp,PostMessageA,PostQueuedCompletionStatus,PostQuitMessage,PostThreadMessageW,PrintDlgW,ProbeForRead,ProbeForWrite,Process32FirstW,Process32NextW,ProcessIdToSessionId,ProcessTrace,PropVariantClear,PsCreateSystemThread,PsDereferencePrimaryToken,PsGetCurrentProcessId,PsGetCurrentThreadId,PsGetProcessCreateTimeQuadPart,PsGetProcessId,PsGetProcessStartKey,PsGetThreadId,PsGetVersion,PsIsThreadTerminating,PsLookupProcessByProcessId,PsLookupThreadByThreadId,PsReferencePrimaryToken,PsRemoveCreateThreadNotifyRoutine,PsRemoveLoadImageNotifyRoutine,PsSetCreateProcessNotifyRoutine,PsSetCreateProcessNotifyRoutineEx,PsSetCreateProcessNotifyRou tineEx2,PsSetCreateThreadNotifyRoutine,PsSetCreateThreadNotifyRoutineEx,PsSetLoadImageNotifyRoutine,PsSetLoadImageNotifyRoutineEx,PsTerminateSystemThread,PtInRect,PtVisible,QueryActCtxW,QueryAllTracesW,QueryDepthSList,QueryDosDeviceW,QueryFullProcessImageNameW,QueryPerformanceCounter,QueryPerformanceFrequency,QueryServiceConfig2W,QueryServiceConfigW,QueryServiceStatus,QueryServiceStatusEx,QueryUnbiasedInterruptTime,QueryWorkingSet,QueueUserAPC,QueueUserWorkItem,RaiseException,ReadEventLogW,ReadFile,ReadProcessMemory,RealChildWindowFromPoint,RectVisible,Rectangle,RedrawWindow,RegCloseKey,RegConnectRegistryW,RegCreateKeyExA,RegCreateKeyExW,RegCreateKeyTransactedW,RegDeleteKeyExW,RegDeleteKeyValueW,RegDeleteKeyW,RegDeleteTreeW,RegDeleteValueA,RegDeleteValueW,RegEnumKeyExA,RegEnumKeyExW,RegEnumKeyW,RegEnumValueA,RegEnumValueW,RegGetKeySecurity,RegGetValueA,RegGetValueW,RegLoadKeyW,RegNotifyChangeKeyValue,RegOpenCurrentUser,RegOpenKeyExA,RegOpenKeyExW,RegQueryInfoKeyW,RegQueryValueExA,RegQueryValueExW,RegQueryValueW,RegSaveKeyW,RegSetKeySecurity,RegSetKeyValueW,RegSetValueExA,RegSetValueExW,RegUnLoadKeyW,RegisterClassA,RegisterClassExA,RegisterClassExW,RegisterClassW,RegisterClipboardFormatW,RegisterDragDrop,RegisterEventSourceA,RegisterEventSourceW,RegisterServiceCtrlHandlerW,RegisterTraceGuidsW,RegisterWaitForSingleObject,RegisterWindowMessageA,RegisterWindowMessageW,ReleaseCapture,ReleaseDC,ReleaseMutex,ReleaseSRWLockExclusive,ReleaseSRWLockShared,ReleaseSemaphore,ReleaseStgMedium,RemoveDirectoryW,RemoveFontMemResourceEx,RemoveMenu,RemovePropW,ReportEventA,ReportEventW,ResetEvent,ResolveIpNetEntry2,RestoreDC,ResumeThread,RevertToSelf,RevokeDragDrop,RoundRect,RpcStringFreeW,RtlAbsoluteToSelfRelativeSD,RtlAddAccessAllowedAce,RtlAddFunctionTable,RtlAllocateAndInitializeSid,RtlAnsiStringToUnicodeString,RtlAppendUnicodeStringToString,RtlAppendUnicodeToString,RtlCaptureContext,RtlCaptureStackBackTrace,RtlCompareMemory,RtlCompareUnicodeString,RtlConvertSidToUnicodeString,RtlCopySid,RtlCopyUnicodeString,RtlCreateAcl,RtlCreateSecurityDescriptor,RtlDeleteElementGenericTable,RtlDeleteElementGenericTableAvl,RtlDeleteFunctionTable,RtlEnumerateGenericTable,RtlEnumerateGenericTableAvl,RtlEnumerateGenericTableWithoutSplaying,RtlEnumerateGenericTableWithoutSplayingAvl,RtlEqualSid,RtlEqualUnicodeString,RtlFreeAnsiString,RtlFreeUnicodeString,RtlGUIDFromString,RtlGetDaclSecurityDescriptor,RtlGetElementGenericTableAvl,RtlGetGroupSecurityDescriptor,RtlGetOwnerSecurityDescriptor,RtlGetSaclSecurityDescriptor,RtlGetVersion,RtlHashUnicodeString,RtlInitAnsiString,RtlInitUnicodeString,RtlInitializeGenericTable,RtlInitializeGenericTableAvl,RtlInsertElementGenericTable,RtlInsertElementGenericTableAvl,RtlInt64ToUnicodeString,RtlLengthSecurityDescriptor,RtlLengthSid,RtlLookupElementGenericTable,RtlLookupElementGenericTableAvl,RtlLookupFunctionEntry,RtlNtStatusToDosError,RtlNumberGenericTableElementsAvl,RtlPcToFileHeader,RtlPrefixUnicodeString,RtlQueryRegistryValues,RtlRandomEx,RtlSetDaclSecurityDescriptor,RtlSetOwnerSecurityDescriptor,RtlStringFromGUID,RtlSubAuthorityCountSid,RtlSubAuthoritySid,RtlUnicodeStringToAnsiString,RtlUnwind,RtlUnwindEx,RtlUpcaseUnicodeChar,RtlValidSecurityDescriptor,RtlValidSid,RtlVerifyVersionInfo,RtlVirtualUnwind,RtlVolumeDeviceToDosName,SHBrowseForFolderW,SHCreateItemFromParsingName,SHDeleteKeyW,SHGetFileInfoW,SHGetFolderPathW,SHGetMalloc,SHGetPathFromIDListW,SHGetSpecialFolderLocation,SHGetSpecialFolderPathA,SHGetSpecialFolderPathW,SHStrDupW,SLGetWindowsInformationDWORD,SafeArrayGetLBound,SafeArrayGetUBound,SafeArrayGetVartype,SaveDC,ScaleViewportExtEx,ScaleWindowExtEx,ScreenToClient,ScrollWindowEx,SeCaptureSubjectContext,SeLockSubjectContext,SeQueryInformationToken,SeReleaseSubjectContext,SeTokenIsAdmin,SeUnlockSubjectContext,SearchPathA,SelectClipRgn,SelectObject,SendDlgItemMessageA,SendMessageA,SendMessageTimeoutA,SendMessageTimeoutW,SendMessageW,SetActiveWindow,SetBitmapBits,SetBkColor,SetBkMode

,SetBrushOrgEx,SetCapture,SetCaretPos,SetClipboardData,SetConsoleCtrlHandler,SetConsoleMode,SetCursor,SetCursorPos,SetDCBrushColor,SetDCPenColor,SetDIBits,SetDllDirectoryW,SetEndOfFile,SetEntriesInAclW,SetEnvironmentVariableA,SetEnvironmentVariableW,SetErrorMode,SetEvent,SetFileAttributesW,SetFileInformationByHandle,SetFilePointer,SetFilePointerEx,SetFileSecurityW,SetFileTime,SetFocus,SetForegroundWindow,SetHandleInformation,SetKernelObjectSecurity,SetLastError,SetLayout,SetLocalTime,SetMapMode,SetMenu,SetMenuDefaultItem,SetMenuItemBitmaps,SetMenuItemInfoW,SetNamedPipeHandleState,SetNamedSecurityInfoA,SetNamedSecurityInfoW,SetPixel,SetPriorityClass,SetProcessAffinityMask,SetProcessDefaultLayout,SetPropW,SetRect,SetRectEmpty,SetScrollInfo,SetSecurityDescriptorDacl,SetSecurityDescriptorGroup,SetSecurityDescriptorOwner,SetSecurityDescriptorSacl,SetSecurityInfo,SetServiceStatus,SetStdHandle,SetStretchBltMode,SetTextAlign,SetTextColor,SetThreadAffinityMask,SetThreadContext,SetThreadLocale,SetThreadPriority,SetThreadStackGuarantee,SetThreadToken,SetThreadpoolThreadMaximum,SetThreadpoolThreadMinimum,SetThreadpoolTimer,SetThreadpoolWait,SetTimer,SetTokenInformation,SetUnhandledExceptionFilter,SetViewportExtEx,SetViewportOrgEx,SetWindowContextHelpId,SetWindowExtEx,SetWindowLongA,SetWindowLongPtrA,SetWindowLongPtrW,SetWindowLongW,SetWindowOrgEx,SetWindowPlacement,SetWindowPos,SetWindowTextW,SetWindowsHookExW,SetupDiDestroyDeviceInfoList,SetupDiEnumDeviceInfo,SetupDiGetActualSectionToInstallW,SetupDiGetClassDevsW,SetupDiGetDeviceInstanceIdW,SetupDiGetDeviceRegistryPropertyW,SfcIsFileProtected,ShellExecuteExA,ShellExecuteExW,ShellExecuteW,Shell_NotifyIconW,ShowWindow,SignalObjectAndWait,SizeofResource,Sleep,SleepConditionVariableCS,SleepConditionVariableSRW,SleepEx,StartDocA,StartPage,StartServiceCtrlDispatcherW,StartServiceW,StartThreadpoolIo,StartTraceW,StgCreateDocfile,StgCreateDocfileOnILockBytes,StgOpenStorageEx,StrStrIW,StretchBlt,StretchDIBits,StringFromGUID2,StringFromIID,SubmitThreadpoolWork,SuspendThread,SwitchToFiber,SwitchToThread,SysAllocString,SysAllocStringByteLen,SysAllocStringLen,SysFreeString,SysStringByteLen,SysStringLen,SystemParametersInfoA,SystemParametersInfoW,SystemTimeToFileTime,SystemTimeToTzSpecificLocalTime,TabbedTextOutW,TdhGetProperty,TdhGetPropertySize,TerminateProcess,TerminateThread,TextOutA,TextOutW,Thread32First,Thread32Next,TlsAlloc,TlsFree,TlsGetValue,TlsSetValue,TraceEvent,TraceMessage,TraceMessageVa,TrackPopupMenu,TrackPopupMenuEx,TranslateAcceleratorW,TranslateMessage,TryAcquireSRWLockExclusive,TryEnterCriticalSection,TzSpecificLocalTimeToSystemTime,UnhandledExceptionFilter,UnhookWindowsHookEx,UnionRect,UnloadUserProfile,UnlockFile,UnlockFileEx,UnmapViewOfFile,UnregisterClassA,UnregisterClassW,UnregisterTraceGuids,UnregisterWait,UnregisterWaitEx,UpdateProcThreadAttribute,UpdateWindow,UuidCreate,UuidFromStringW,UuidToStringW,ValidateRect,VariantChangeType,VariantClear,VariantInit,VerQueryValueW,VerSetConditionMask,VerifyVersionInfoW,VirtualAlloc,VirtualAllocEx,VirtualFree,VirtualFreeEx,VirtualProtect,VirtualProtectEx,VirtualQuery,VirtualQueryEx,WNetAddConnection2W,WNetCancelConnection2W,WNetCancelConnectionW,WSAAddressToStringA,WSACleanup,WSACloseEvent,WSAConnect,WSACreateEvent,WSAEnumNetworkEvents,WSAEventSelect,WSAGetOverlappedResult,WSAIoctl,WSARecv,WSARecvFrom,WSAResetEvent,WSASend,WSASetEvent,WSASocketA,WSAStartup,WSAStringToAddressA,WSAWaitForMultipleEvents,WSCDeinstallProvider,WSCEnumProtocols,WSCGetProviderPath,WSCInstallProvider,WSCSetApplicationCategory,WSCWriteProviderOrder,WTHelperGetProvCertFromChain,WTHelperGetProvSignerFromChain,WTHelperProvDataFromStateData,WTSCloseServer,WTSEnumerateProcessesW,WTSEnumerateSessionsW,WTSFreeMemory,WTSGetActiveConsoleSessionId,WTSOpenServerExW,WTSQuerySessionInformationW,WTSQueryUserToken,WaitForMultipleObjects,WaitForMultipleObjectsEx,WaitForSingleObject,WaitForSingleObjectEx,WaitForThreadpoolIoCallbacks,WaitForThreadpoolTimerCallbacks, WaitForThreadpoolWorkCallbacks,WaitMessage,WaitNamedPipeW,WakeAllConditionVariable,WakeConditionVariable,WideCharToMultiByte,WinHelpW,WinHttpAddRequestHeaders,WinHttpCloseHandle,WinHttpConnect,WinHttpCrackUrl,WinHttpGetDefaultProxyConfiguration,WinHttpGetIEProxyConfigForCurrentUser,WinHttpGetProxyForUrl,WinHttpOpen,WinHttpOpenRequest,WinHttpQueryAuthSchemes,WinHttpQueryDataAvailable,WinHttpQueryHeaders,WinHttpReadData,WinHttpReceiveResponse,WinHttpSendRequest,WinHttpSetCredentials,WinHttpSetOption,WinHttpSetTimeouts,WinVerifyTrust,WindowFromPoint,WindowsCreateStringReference,Wow64DisableWow64FsRedirection,Wow64GetThreadContext,Wow64RevertWow64FsRedirection,Wow64SetThreadContext,WriteClassStg,WriteFile,WritePrivateProfileStringW,WriteProcessMemory,WscRegisterForChanges,WscUnRegisterChanges,ZwClose,ZwCreateFile,ZwCreateKey,ZwDeleteKey,ZwDeleteValueKey,ZwDeviceIoControlFile,ZwDuplicateObject,ZwDuplicateToken,ZwEnumerateKey,ZwEnumerateValueKey,ZwFsControlFile,ZwOpenFile,ZwOpenKey,ZwOpenProcess,ZwOpenProcessTokenEx,ZwOpenSection,ZwOpenSymbolicLinkObject,ZwOpenThreadTokenEx,ZwQueryDirectoryFile,ZwQueryInformationFile,ZwQueryInformationToken,ZwQueryKey,ZwQueryObject,ZwQuerySecurityObject,ZwQuerySymbolicLinkObject,ZwQueryValueKey,ZwQueryVirtualMemory,ZwQueryVolumeInformationFile,ZwReadFile,ZwSetInformationFile,ZwSetInformationThread,ZwSetInformationToken,ZwSetSecurityObject,ZwSetValueKey,ZwTerminateProcess,ZwWriteFile,abort,asctime_s,atan,atoi,atol,bsearch,bsearch_s,btowc,calloc,ceil,ceilf,copysign,copysignf,cos,cosf,cosh,exit,exp,expm1,fclose,feof,ferror,fflush,fgetc,fgetpos,fgets,fgetwc,floor,floorf,fmod,fopen,fputc,fputs,fputwc,fread,free,freopen_s,frexp,fseek,fsetpos,ftell,fwrite,getenv,getenv_s,gethostbyaddr,getservbyport,htons,inet_addr,isalnum,isalpha,isdigit,islower,isprint,ispunct,isspace,isupper,iswalnum,iswalpha,iswdigit,iswspace,iswxdigit,isxdigit,keybd_event,ldexp,ldiv,localeconv,log,log1p,log2,logf,lstrcmpA,lstrcmpW,lstrcmpiA,lstrcmpiW,lstrcpyW,lstrcpynW,lstrlenW,malloc,mbstowcs,mbtowc,memchr,memcmp,memcpy,memcpy_s,memmove,memmove_s,memset,pow,powf,qsort,qsort_s,rand,rand_s,realloc,setlocale,setvbuf,signal,sin,sinf,sinh,sqrt,sqrtf,srand,strcat_s,strchr,strcmp,strcpy_s,strcspn,strerror,strftime,strncat,strncmp,strncpy,strncpy_s,strnlen,strpbrk,strrchr,strspn,strstr,strtod,strtof,strtok,strtol,strtoll,strtoul,swprintf_s,tan,timeGetDevCaps,timeGetTime,tolower,toupper,towlower,towupper,ungetc,ungetwc,vswprintf_s,wcscat_s,wcschr,wcscmp,wcscoll,wcscpy_s,wcscspn,wcsftime,wcsncmp,wcsncpy,wcsncpy_s,wcsnlen,wcspbrk,wcsrchr,wcsspn,wcsstr,wcstod,wcstof,wcstok_s,wcstol,wcstoll,wcstombs,wcstoul,wcstoull,wmemcpy_s,wsprintfW

12 ANNEX B: THIRD-PARTY LIBRARIES

- AppRemoverAPI 4.3.94.1 opswat
- LZMA SDK 24.09
- MAPIStubLibrary 2025.4.3
- OpswatOESIS WinSDK 4.3.4591.0
- Sciter ESET 11.0.60.0
- boost 1.87.0
- curl 8.12.0
- gRPC-Gateway 2.26.1
- google-protobuf 21.12
- googleapis 2025.2.10

- googletest 2025.2.10
- grpc 1.59.1
- imgui 1.91.3-docking
- miniz 3.0.2
- poco 1.14.1
- pugixml 1.15
- qr-code-generator 1.8.0
- sqlite 3.49.0
- wix_toolset 3.14.1.8722
- zlib 1.3.1
- Visual Studio v14.44.35211.0
- Microsoft Windows Performance Recorder v6.3.9600.17736