



360Security - software requirement specification srs

Software Engineering (Lovely Professional University)

Software Requirements Specification

For

360 Total Security

Prepared by Kinshuk kataria

Reg. Number: 11505869

Roll No. B39

K1512



L OVELY
P ROFESSIONAL
U NIVERSITY

Transforming Education Transforming India

Lovely Professional University

Table of Contents

1. Introduction.....	1
1.1 Purpose.....	1
1.2 Document Conventions.....	1
1.3 Intended Audience and Reading Suggestions.....	1
1.4 Definitions, acronyms, abbreviations.....	1
1.5 Scope))))))))))))))))))))))))))	3
2. Overall Description.....	3
2.1 Product Perspective.....	3
2.2 Product Features.....	4
2.3 User Classes and Characteristics.....	5
2.4 Operating Environment.....	5
2.5 Design and Implementation Constraints.....	5
2.6 Assumptions and Dependencies.....	7
3. Specific Requirements.....	7
3.1 Functional Requirement.....	7
3.2 Requirements of the bank computer for the ATM))))))))))))))))..	11
4. External Interface Requirements.....	13
4.1 User Interfaces.....	13
4.2 Hardware Interfaces.....	13
4.3 Software Interfaces.....	14
5. Other Nonfunctional Requirements.....	14
5.1 Performance Requirements.....	14
5.2 Safety Requirements.....	14
5.3 Security Requirements.....	14
5.4 Software Quality Attributes.....	15
6. Other Requirements.....	15

1. Introduction

1.1 Purpose

This document describes the software requirements and specification for an antivirus i.e. 360 Total Security.

1.2 Document Conventions: font: TNR 11

1.3 Intended Audience and Reading Suggestions (Intended audience is defined as the group of people for which a service or product is designed)

The document is intended for all the stakeholders i.e. customer and the developer (**designers, testers, maintainers**). The reader is assumed to have basic knowledge of Malwares, Computer worms and Trojans required. Knowledge and understanding of antivirus working is also required.

1.4 Definitions, abbreviations

1.4.1 Definitions

- **360 Total Security**

It is a free security protection against any virus, malware and computer worms. It is also designed to provide protection against internet theft and allows the user to boost up device speed and clear junk files at same time. It is available for various platforms like Windows, IOS and Android.

- **Antivirus**

Antivirus (or anti-virus) software is used to safeguard a computer from malware, including viruses, computer worms, and Trojan horses. Antivirus software may also remove or prevent spyware and adware, along with other forms of malicious programs.

- **Virus**

A piece of code which is capable of copying itself and typically has a detrimental effect, such as corrupting the system or destroying data.

- **Malware**

It is software which is specifically designed to disrupt, damage, or gain authorized access to a computer system.

- **Trojans**

It is a program designed to breach the security of a computer system while ostensibly performing some innocuous function.

- **User**

A person who uses or operates something. The person who works within the device based operating environment

- **Device**

A thing made or adapted for a particular purpose, especially a piece of mechanical or electronic equipment.

1.4.2 Abbreviations

Throughout this document the following abbreviations are used:

- k : is the maximum time for the software to be valid to use.
- m: is the maximum number of scans.
- n : is the minimum number of scans.
- t : is the total validity of the antivirus.

1.5 Project Scope

This is **computer software** used to prevent, detect and remove **malicious software**. Antivirus software was originally developed to detect and remove **computer viruses**, hence the name. However, with the proliferation of other kinds of **malware**, antivirus software started to provide protection from other computer threats.

Overall Description

1.5 Product Perspective

The 360 Total Security does not work independently. It works together with the system Kernel and the operating system installed in the device.

Communication interface: The 360 Total Security communicate with the service provider via a communication network.

Software interface: The software will run on any device based on Windows, Android and IOS

Hardware interface: The software will run on any device.

User interfaces

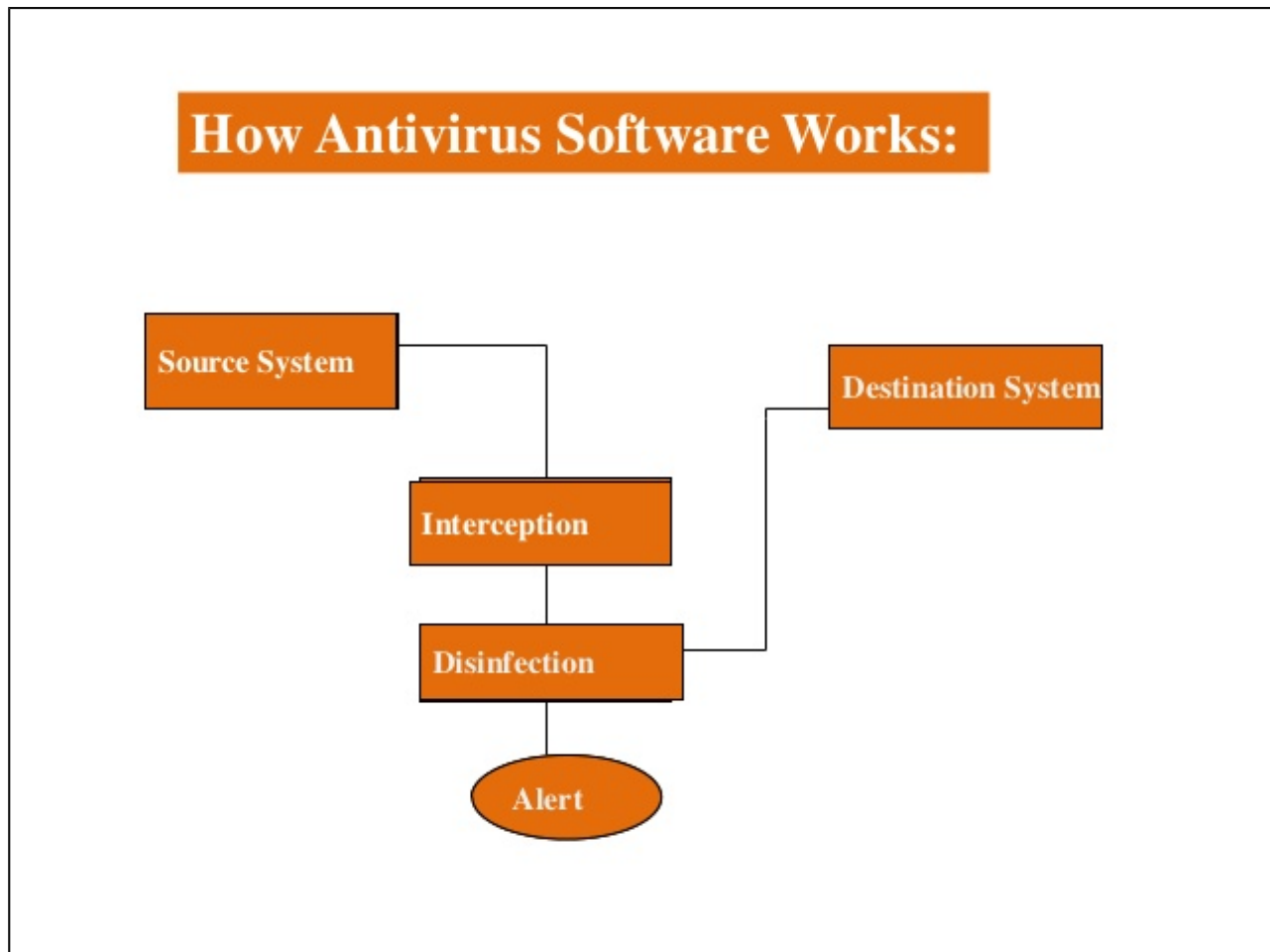
Customer: The customer user interface should be used, such that 99.9% of all new product users are able to remove and filter the threats without any assistance.

Software Security Personnel: Software security personnel are responsible for removing deposits and adding new updates. There should be a simple interface (e.g., a switch or button) that they can use to initialize the scan whenever they restock.

Maintainer: The maintainer is responsible for adding new updates to the softwares and servicing existing version of software. A maintainer should be possible to add a new update to the software within 1 week.

1.6 Product Features

The 360 Total Security provides real time protection every time. The software identifies a user by a software version and key. It collects information about a simple account registration details(e.g., deposit, withdrawal, transfer, bill payment), communicates the transaction information to the customer's bank, and dispenses cash to the customer. The banks provide their own software for their own computers. The bank software requires appropriate record keeping and security provisions. The software must handle concurrent accesses to the same account correctly.



1.7 User Classes and Characteristics

Characteristics: There are several users of the 360 Total Security:

Customers are simply members of the general public with no special training.

Software security personnel need have no special education or experience.

Maintainers must be experienced network administrators, to be able to get new updates to the software.

1.8 Operating Environment

The hardware, software and technology used should have following specifications:

- Ability to run the 360 Total securities.
- Ability to install all the files of the software.

- Touch screen for convenience or via mechanical keyboard.
- Keypad (in case touchpad fails)
- Continuous power supply
- Ability to connect to service provider.
- Ability to take input from user
- Ability to validate software

1.9 Design and Implementation Constraints

- Registration

Validate Antivirus:

- Validate for Software Expiration Date
- Validate that the software expiration date is later than today's date
- If software is expired, prompt error message "This version is expired"

Validate for Stolen software copy:

- Validate that the software is not stolen
- If the software is not genuine, prompt error message, "This version is already in use"

Validate for Expired Software:

- Validate that the software is not expired
- If software is expired, prompt error message, "This version is already expired"

Validate for Pirate Software:

- Validate that the software is not pirated version.
- If software is invalid, prompt error message "This is not a valid version"

Validate Serial Key:

- Validate that the serial key is not blank
- If serial key is blank, prompt error message "Please provide serial key"
- Validate that the password entered matches the password on file
- If password does not match, prompt error message "Invalid Serial Key"

Outdates Software Version:

- If number of consecutive unsuccessful logins exceeds three attempts, terminate software
- Maintain Consecutive Unsuccessful Login Counter
- Increment Login Counter
- For every consecutive Login attempt, increment logic counter by 1.
- Reset login counter to 0 after login is successful.
- Get validity information
- Run the software

2.6 Assumptions and Dependencies

- Hardware never fails
- Limited number of scans
- Custom Drive Scan.

2. Specific Requirements**2.1 Functional Requirements**

The functional requirements are organized in two sections First requirements of the software and second requirements of the device.

2.1.1 Requirements of the 360 Total Security

The requirements for 360 Total Security are organized in the following way General requirements, requirements for authorization, requirements for a validation.

General**Functional requirement 1:**

- **Description:** Initialize parameters t, k, m, n
- **Input:** 360 Total Security is initialized with t duration, k, m, n are entered
- **Processing:** Storing the parameters.
- **Output:** Parameters are set.

Functional requirement 2:

- **Description:** If no software in the device, the system should display initial display.

Functional requirement 3:

- **Description:** If the software is running out of validation, no extra features should be accepted. An error message is displayed.
- **Input:** Software is run.
- **Processing:** The requirements of software are less than t.
- **Output:** Display an error message. Terminate the run task.
- **Authorization:** The authorization starts after a user has run the software in the device

Functional requirement 4:

- **Description:** The software has to check if the entered key is valid serial key.
- **Input:** Customer runs the scan.
- **Processing:** Check if it is a valid software version. It will be valid if
 - The information on the software copy be read.
 - It is not expired.
- **Output:** Display error message and terminates the installation.

Functional requirement 5:

- **Description:** If it is valid, the software should read the serial number and linked address.
- **Input:** Valid version.
- **Processing:** Read the serial number.
- **Output:** Initiate authorization dialog







Functional requirement 6:

- **Description:** The serial number should be logged.
- **Input:** Serial number from dialog box.
- **Processing:** Log the number.
- **Output:** Update to log file.

Functional requirement 7:

- **Description Authorization dialog:** The user is requested to enter his serial key. The 360 Total Security verifies information and password with the service provider.
- **Input:** Password from user, serial key from the product.
- **Processing:** Send serial number and password to service provider, receive response from team.
- **Output:** Accept or reject authorization form .

Functional requirement 8:

- **Description:** Different negative answers from service provider for authorization dialog.
- **Input:** Response from team or authorization dialog:
 -  bad password  if the password was wrong.
 -  bad bank code  if the serial key is not supported by the service provider.
 -  bad account  if there are problems with the account.
- **Processing:** If the antivirus gets any of these messages from the bank computer, the software copy will be terminated and the user will get the relevant error message.
- **Output:** Installation will cancel and error message is displayed.

Functional requirement 9:

- **Description:** If password and serial number are ok, the authorization process is finished.
- **Input:** The software gets accept from the team for authorization process.
- **Processing:** Finishing authorization.
- **Output:** Start installing.

Functional requirement 10:

- **Description:** If a serial key entered more than three times in a row in a software and the password was wrong each time, a message will be displayed that the customer should call the team.
- **Input:** Entering a wrong serial key for the fourth time in succession
- **Processing:** Initiate authorization process Response from service provider is to keep the genuine software.
- **Output:** Display error message that the customer should call the service provider.

Functions: These are the requirements for the different functions the 360 Total Security should provide after authorization.

2.1.2 Requirements of the 360 Total security.

Authorization

The antivirus gets verified by its developer via internet from anywhere around the world.

Functional requirement 1:

- **Description:** The software provider checks if the antivirus has valid serial key. A serial key is valid if the software was issued by the developer's team themselves only.
- **Input:** Request from the software provider to verify software copy (Serial number and password.)
- **Processing:** Check if the software was issued by them only.
- **Output:** Valid or invalid serial key.

Functional requirement 2:

- **Description:** If it is not a valid serial key, the 360 Security will send a message to the main developer team.
- **Input:** Invalid serial key
- **Processing:** Process message
- **Output:** The software sends the message "Invalid Serial Key" to the Device.

Functional requirement 3:

- **Description:** The installed software checks if the Serial key is valid for a valid antivirus copy.
- **Input:** Request from the service provider to verify password.
- **Processing:** Check serial key of the customer.
- **Output:** Valid or invalid password.

Functional requirement 4:

- **Description:** If it is not a valid serial key, the service provider will send a message to the device.
- **Input:** Invalid password.
- **Processing:** Process message. Update count for invalid key for the account.
- **Output:** The bank computer sends the message "Invalid Serial Key" to the ATM.

Functional requirement 5:

- **Description:** If it is valid software and a valid serial key but there are problems with the account, the bank will send a message to the device that there are problems.
- **Input:** Valid version and serial key.
- **Processing:** Process message.
- **Output:** The service provider sends "Invalid Version" to the ATM.

Functional requirement 6:

- **Description:** If it is valid software with a valid key and there are no problems with the product the service provider will send a message to the team that everything is ok.
- **Input:** Valid product password and key.
- **Processing:** Process message.
- **Output:** Send "Verified" to the Device.

Functional requirement 7:

- **Description:** Update software after its version get expires.
- **Input:** Response from device about updating antivirus.
- **Processing:** Updates software.
- **Output:** Updated

Functional requirement 8:

- **Description:** Each software has a limit k for which it can protect the device from any external threats.
- **Input:** Request to process validation.
- **Processing:** Check if the validity of the software doesn't exceed k
- **Output:** If the validity exceeds the limit, the software will stop protecting device from threats. .

Functional requirement 9:

- **Description:** The 360 Total Security only provides security for their own computer and their own devices.

3. External Interface Requirements

3.1 User Interfaces

The user interface should be intuitive, such that 99.9% of all new users are able to understand the software working to scan any drive.

3.2 Hardware Interfaces

The hardware should have following specifications:

- Ability to read the hard drive and flash drives too.
- Ability to detect real time connected device.
- Touch screen for convenience.
- Keypad (in case touchpad fails)
- Continuous power supply
- Ability to connect to secured server.
- Ability to take instruction from user
- Ability to validate user

3.3 Software Interfaces

The software interfaces are specific to the target protection against any threats.

4. Other Nonfunctional Requirements

4.1 Performance Requirements

- It must be able to perform in adverse conditions like high/low ram usage etc.
- Good internet connection.
- Device should have enough ram.

4.2 Safety Requirements

- Do not lose the serial key.
- Must be registered with a provided serial key in the kit.
- Must have a registered E-mail linked to the software.
- There must be a registered phone number.
- Carefully select the installation option during installation.

4.3 Security Requirements

- Users accessibility is ensured in all the ways.
- Users are advised that antivirus should be genuine.
- Users are advised update the software as soon as the new update is available.
- Only one antivirus should be installed at a time in a single device.

4.4 Software Quality Attributes

Security

Performance

5.4.1 Availability: The Antivirus should have a real time protection and run behind every process.

5.4.2 Security: The antivirus should provide maximal security .In order to make that much more transparent there are the following requirements:

1. It must be impossible to plug into the network.

5.4.3 Maintainability: Only users are allowed to manipulate the working of antivirus.

6. Other Requirements

6.1 Data Base

The 360 Total Security must be able to access the data base in order to get regular updates to perform action against new threats which tends to affect the working of any device and all the last scan details.