Software Requirements Specification

For

BitVise

(An XTS-AES Based Disk Encryption Privacy Solution)

Version 1.0

**NC Myra Khalid**

**NC Usama Ahmad**

**PC Laraib Zahid**

Department of CSE, Military College of Signals, NUST

8th Nov 2016

Table of Contents

[1. Introduction 1](#_Toc431286499)

[1.1 Purpose 1](#_Toc431286500)

[1.2 Document Conventions 1](#_Toc431286501)

[1.3 Intended Audience and Reading Suggestions 2](#_Toc431286502)

[1.4 Project Scope 2](#_Toc431286503)

[1.5 References 3](#_Toc431286504)

[2. Overall Description 3](#_Toc431286505)

[2.1 Product Perspective 3](#_Toc431286506)

[2.2 Product Features 3](#_Toc431286507)

[2.3 User Classes and Characteristics 5](#_Toc431286508)

[2.4 Operating Environment 5](#_Toc431286509)

[2.5 Design and Implementation Constraints 5](#_Toc431286510)

[2.6 User Guide 5](#_Toc431286511)

[3. External Interface Requirements 6](#_Toc431286512)

[3.1 User Interfaces 6](#_Toc431286511)

[3.2 Hardware Interfaces 6](#_Toc431286511)

[3.3 Software Interfaces 6](#_Toc431286511)

[3.4 Communication Interfaces 6](#_Toc431286511)

[4. System Features 7](#_Toc431286512)

[4.1 Video Input..... 8](#_Toc431286513)

[4.2 Divide into Frames 9](#_Toc431286514)

[4.3 Compare Frames 9](#_Toc431286515)

[4.4 Convert to Text 10](#_Toc431286516)

[4.5 Segmentation of text 11](#_Toc431286517)

[4.6 Convert text to Speech 12](#_Toc431286518)

[5. Other Nonfunctional Requirements 13](#_Toc431286519)

[5.1 Performance Requirements 13](#_Toc431286520)

[5.2 Safety Requirements 13](#_Toc431286521)

[5.3 Hardware Requirements 13](#_Toc431286522)

[5.4 Software Quality Attributes 13](#_Toc431286523)

[5.5 Usability 13](#_Toc431286524)

[5.6 Maintainability 13](#_Toc431286525)

[Appendix A: GLossary 14](#_Toc431286526)

[Appendix B: Issue List 14](#_Toc431286527)

[Appendix C: Project Proposal 14](#_Toc431286528)

# **Introduction**

The aim of this document is to present Software Requirements Specification (SRS) of An XTS-AES Based Disk Encryption Privacy Solution by defining the problem statement in detail.

## **1.1 Purpose**

This document will further explain the purpose and features of the BitVise. Encryption software will provide the security services by encrypting physical hard disk. Purpose of BitVise is to protect the confidentiality of hard disks. Encryption will be based on implementation of XTS-AES implementation system. Government sensitive data holds top priority in sensitive organization therefore secure storage is as important as secure data transfer. Application will be responsible to encrypt data and ensure that data is not accessible to unauthorized personnel. Interactive interface will be provided to ensure ease of usage to system users. Software will be compatible with minimum hardware present at the government organization.

This document is intended for stakeholders, developers and support team at organization. Document will outline the features and requirements of BitVise and will act as software validation document for the prospective client.

## **1.2 Document Conventions**

* Priority of requirements is stated to be same when this document is being written.
* This document is based on requirements from NESCOM and also fulfills requirements of CSE Dept. regarding FYP.
* Context and flow diagrams are based on UML standards.
* Heading are prioritized in a numbered fashion.

## **1.3 Intended Audience and Reading Suggestions**

### **Reading suggestions:**

### **Intended audience:**

* **Project Supervisor (Lec. Waseem Iqbal)**

This document will assist in supervision and guiding the team. Further, document will act as reference to ensure completion of all requirements and proper implementation.

* **Developers (Project group):**

For project development team, this document will provide the guideline for development of BitVise software covering all the requirements of user and developing right product.

* **Testers (Project group, NESCOM Team)**

This document will help quality assurance team to form correct test cases for testing and evaluating whether all requirements have been fulfilled.

* **Users (NESCOM Team)**

Document will help team at NESCOM to evaluate the project and deploy it on their systems. It will also be helpful to know flow of program and familiarize them to the environment.

* **Project Evaluation Team (MCS NUST, NESCOM Team)**

It will help the evaluation team to evaluate the progress of FYP project. The document will provide the evaluators with the scope, requirements and details of the software to be developed. It will also be used as basis for the evaluation of the implementation of the project.

* **(More to be added if req )fips pkcs5 test vectors pehla vala ,**

## **Project Scope**

The BitVise includes disk encryption solution for Windows OS using XTS-AES implementation.

* Non System Partition Encryption.
* Encryption of volume of hard drive using XTS-AES algorithm
* Mounting volume using file container
* Key authentication mechanism using PKSC 5 and Password based Cryptology

(RSA CS5 standard)

* Recovery using recovery Key
* Desktop application using GTK+

Focus of the project will be providing standard performance in terms of encryption/decryption time involved. Providing Desktop application with user friendly Interface. Implementation will be in C language specifically according to requirements of NESCOM.

## 1.5 References (HARVARD REF )

* **NIST Standard : Encryption of Storage Devices** http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-111.pdf
* **(more to be added here)pkcs5**

# **Overall Description**

## **Product Perspective**

BitVise is new project built for sensitive organizations to provide security services to hard disks within the windows systems. Other products available in market are all being in news for possible breach or backdoor. It is built for organizations who do not want to use third party tools due to danger of sensitive data being leaked and possible backdoors.

## **Product Features**

The main features of BitVise are highlighted below:

* Volume encryption through XTS-AES algorithm.
* Desktop Application for user interaction.
* Volume structure and Files Hidden
* Mounting volume using file container
* Recovery key option in case of forgetting password
* (more to add)

## **User Classes and Characteristics**

Defining system users of the BitVise software.

#### **UCC-1 Government Employees (NESCOM)**

Employees will be general users who have system with them for encryption purposes. They will be interacting with desktop application.

#### **UCC-2 Developers (NESCOM ,Project group)**

BitVise software and source code will be provided to them for future upgrades that are required to be made.

#### **UCC-3 Software Testers (NESCOM and Project group)**

Software will be used for Beta testing by our project group and testers present with NESCOM.

## **Operating Environment**

This included all the specifics required for software to be build.

### **Hardware**

* 1 SATA Hard Disk Drive

### **Software**

* Windows 10 Operating System
* Visual Studio 2015

## **Design and Implementation Constraints**

This section covers limitation and requirements for software to work

* BitVise will only cover encryption of volume (Logical drives) at the moment.
* Non-system partitions will be considered for encryption only.
* (to be added)

## **User Documentation**

User manuals will be provided which will take users step by step to complete encryption process using BitVise. A tutorial will provide a quick start, a walk-thru of major system features, and further reference source for the complete system features.

Further, instructions will be given according to the particular user i.e. Government employees, NESCOM developers etc.

**Assumptions and Dependencies**

# **External Interfaces Requirements**

## **User Interfaces**

(t

## **Hardware Interfaces**

(to be added)

## **Software Interfaces**

(to be added)

# **4. System Features**

Section includes System features of BitVise describing use cases and features.

BitVise will work in offline mode

1. Partition encrypt

Encrypting data without affecting contents .

Inaccessable data

1. file contaier

**4.1 AES-XTS Encryption**

Software provide encryption using storage devices standard of AES-XTS standards.

**Functional Requirements**

**REQ-1**

Reading Sectors

Writing Sectors

**4.2 Implementation of File Container**

Driver Implementation

**4.3 GUI Using GTK+**

**4.4 Key Authentication Mechanism**

1. Video Input
2. Divide into Frames
3. Compare Frames
4. Convert to text
5. Segmentation of Text
6. Convert Text to speech

Use case diagram of the system given in figure 4.1



**Fig 4.1: Use Case Diagram**

## Video Input

|  |
| --- |
| **Use Case Requirement:** The camera mounted on the ring will capture the video in real time. This video will be used for further conversion of text into speech. |
| **Use Case Paths**   * Normal: * Video sent for processing. * Exceptional: * Beep Sound is produced |
| Normal Path: Video sent for processing |
| **Externals**   * Data Cable |
| **Preconditions**   * The camera captures the video in real time. |
| **Interactions**   * The captured video is sent to the system for processing. |
| **Post conditions**   * Captured video is divided into frames |
| **Categorization**   * **Frequency**: High * **Criticality**: High * **Probability of Defects**: Medium * **Risk**: High |
| Exceptional Path: Beep Sound is produced |
| **Externals**   * Speakers |
| **Preconditions**   * The camera is not aligned with the text while video is being captured. |
| **Interactions**  An error signal is sent to the system |
| **Post conditions**   * The beep sound is produced through the speakers of the computer. |
| **Categorization**   * **Frequency**: High * **Criticality**: High * **Probability of Defects**: Low * **Risk**: High |

**5. Other Nonfunctional Requirements**

https://en.wikipedia.org/wiki/List\_of\_system\_quality\_attributes

## **(for NF)**

## **Performance Requirements**

BitVise is expected to be according to standards and will have encryption rate of 1GB/minute rate of encryption. Memory used for encryption will be (memory used by file container).

## **Safety Requirements**

## The use of the software product has no harm whatsoever. If application is abruptly terminated, then data will remain in RAM unsecure and can be leaked. Therefore, its advised to shutdown computer in case of accidental termination.

## **Security Requirements**

BitVise require password to encrypt Volume data. Due to security reasons, there is no way to get the key once forgotten and data can be accessed only through recovery key as a result. In case both keys are lost, then data recovery is not possible (Usama that liner about data loss).

There are no specific security requirements for the application as there is no communication with other nodes or over internet.

## **Software Quality Attributes**

## **Usability**

Whole encryption process will run smoothly and user interaction will be complexity free. Graphical Interface visually appealing and easy for the user to navigate.

**Data** [**Integrity**](https://en.wikipedia.org/wiki/Data_corruption)

Data will not be affected by encryption process and will not be corrupted or any change made to its contents.

## **Scalability**

BitVise works for one user at a time as it’s a desktop application and would not let multiple access to hard drive.

## **Confidentiality**

BitVise will keep data confidential . Data will not be stored or sent anywhere. Encrypted data and passwords will not be stored in readable form.

**S**[**tandards Compliance**](https://en.wikipedia.org/wiki/Standardization)

BitVise will be according to standards of NIST and will be following standard encryption standards for storage devices

https://en.wikipedia.org/wiki/List\_of\_system\_quality\_attributes