

Implementation of kerberos

41900 - Fundamentals of Security



Authors:

David Lee – 11055579

Gerard McTaggart – 11849320

Yujian Zhuang – 11663236

Sasa Denda – 11000724

May 7, 2015

Table of Contents

[1.0 Document Management 2](#_Toc418768868)

[1.1 Revision History 2](#_Toc418768869)

[1.2 Intended Audience 2](#_Toc418768870)

[1.3 Reference Documents 2](#_Toc418768871)

[1.4 Glossary 2](#_Toc418768872)

# List of Tables

[Table 1: Revision History 2](#_Toc418768949)

[Table 2: Intended Audience 2](#_Toc418768950)

[Table 3: Reference Documents 2](#_Toc418768951)

[Table 4: Glossary 2](#_Toc418768952)

# List of Figures

# Document Management

## Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Description of Change | Author |
| 07/05/2015 | 1.0 | Initial template created | Sasa Denda |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table : Revision History

## Intended Audience

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Title | Action | Date Approved |
| Dr Richard Xu | Subject Coordinator | Sign-off |  |
| Bernard XXXX | Tutor | Sign-off |  |
| Security Group | Students | Review |  |

Table : Intended Audience

## Reference Documents

|  |  |  |
| --- | --- | --- |
| Ref. | Name | Description |
| R001 |  |  |
|  |  |  |

Table : Reference Documents

## Glossary

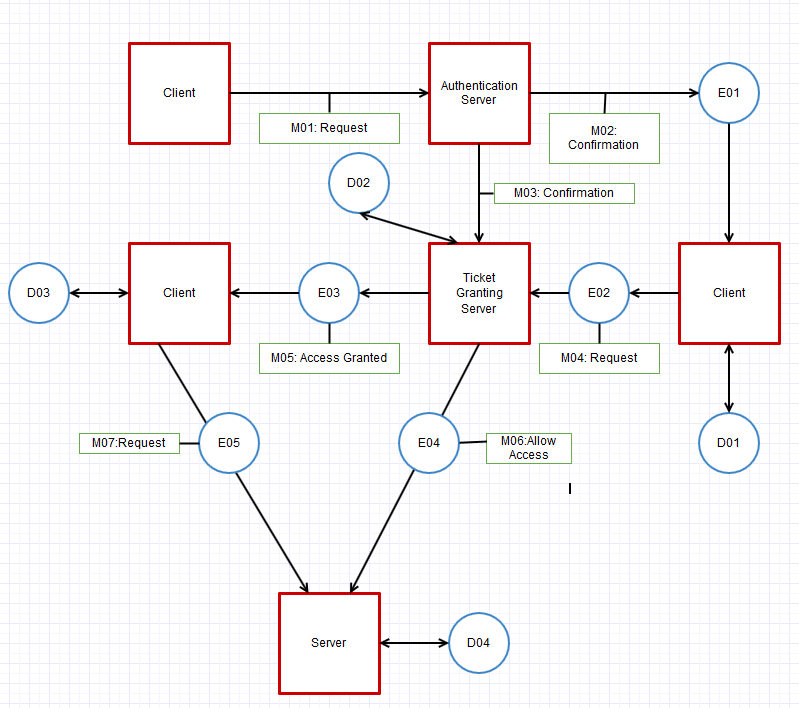
|  |  |
| --- | --- |
| Term | Description/Meaning |
|  |  |
|  |  |
|  |  |
|  |  |

Table : Glossary

# Introduction

This document outlines the design, implementation and execution of a symmetric encryption software program known as Kerberos. With the increased efficiency of communication through Information Technology infrastructure there is a coexistent need for the protection of these communication channels and thus begins the importance of encryption and decryption.

The generic high level outline of how the system works is as follows:



The diagrammatical representation has condensed each message, encryption and decryption component to save space, they are explained below.

Each Red box represents a different entity involved. As explained above the Client has the end goal of communicating with the server, however to do this they must first be authorised by the Authentication Server which does so by issuing a Ticket. The Ticket allows the Client to confirm with the Ticket Granting Server that connection between the Client and Server is allowed. The Ticket Granting Server then sends the key to the Client and the Server which allows for established communication between the two.

The details of each message component are explained below, followed by an explanation of what data each encryption and decryption algorithm utilise at the time they are utilised.

**Message Details**

|  |  |
| --- | --- |
| **Message Code** | **Message Contents** |
| M01 | This message consists of a simple request from the Client to the authentication server. The only data being read from this communication is the username and password being used. If the username and password are both valid then the Client is authenticated. |
| M02 | The second message is more |
| M03 |  |
| M04 |  |
| M05 |  |
| M06 |  |
| M07 |  |

**Encryption Details**