

Berner Fachhochschule  
Hochschule für Technik und Informatik HTI

# Pflichtenheft Version 08.06.2004

## Diplomarbeit I00 (2004)

# MuSeGa



## Mobile User Secure Gateway

Experte: Andreas Dürsteler (Swisscom)  
Betreuer: Hansjürg Wenger (HTI)  
Gerhard Hassenstein (HTI)  
Diplomand: Lukas Reusser (Swisscom)

# Abstract

Dieses Pflichtenheft beschreibt die Diplomarbeit „MuSeGa – Mobile User Secure Gateway“. Ziel von MuSeGa ist es, den momentan eingesetzten Bluesocket Gateway, der die Verbindung zwischen Wireless-LAN und HTI-Intranet sicher stellt, zu ersetzen und dessen Funktionalität mit höherer Performance zu übernehmen.

MuSeGa setzt auf High-End PC Hardware auf, läuft unter Linux und basiert vollkommen auf OpenSource. Dadurch werden die Kosten sehr tief gehalten.

## Versionskontrolle

Version	Datum	Kommentar	Genehmigt
0.1	29.04.2004	Erster Draft	
0.3	02.05.2004	Erste komplette Version	
0.4	06.05.2004	Mit Anpassungen nach erster Besprechung	
0.5	07.05.2004	Mit Anpassungen nach zweiter Besprechung	
0.6	17.05.2004	Zeitplan Grobübersicht hinzugefügt	
0.7	01.06.2004	Ergänzungen von Hansjürg Wenger eingefügt	
0.8	01.06.2004	Anpassungen aus Besprechung	
0.9	08.06.2004	Punkt 2.2.2 angepasst	Alle

Genehmigt durch:

Experte: Andreas Dürsteler

Betreuer: Hansjürg Wenger

Betreuer: Gerhard Hassenstein

Diplomand: Lukas Reusser



# Inhaltsverzeichnis

- 1 Allgemeines..... 5
  - 1.1 Sinn und Zweck..... 5
  - 1.2 Leserkreis..... 5
  - 1.3 Umfang..... 5
  - 1.4 Anwendungsgebiet..... 5
- 2 Anforderungen an MuSeGa..... 5
  - 2.1 Technische Anforderungen (Überblick)..... 5
  - 2.2 Technische Anforderungen (Details)..... 6
    - 2.2.1 Benutzerauthentifikation via RADIUS..... 6
    - 2.2.2 Stateful Firewall..... 7
    - 2.2.3 VLAN Unterstützung..... 7
    - 2.2.4 Administration via cmd und Web-GUI..... 8
    - 2.2.5 NAT/NAPT..... 8
    - 2.2.6 DHCP Server..... 8
    - 2.2.7 DNS Forwarding..... 8
    - 2.2.8 Statistik..... 8
    - 2.2.9 PPTP Endpunkt..... 8
    - 2.2.10 SMTP Catch & Forward..... 9
    - 2.2.11 Bandbreiten Management..... 9
    - 2.2.12 IDS..... 9
    - 2.2.13 IPSec Endpunkt..... 9
  - 2.3 Allgemeine Anforderungen..... 9
    - 2.3.1 Evaluierung des Betriebssystems und der Komponenten..... 9
    - 2.3.2 Verwendete Komponenten..... 9
    - 2.3.3 Dimensionierung..... 10
    - 2.3.4 Verwendungsrechte von MuSeGa..... 10
    - 2.3.5 Sprachen..... 10
- 3 Hardware..... 10
  - 3.1 Hardware für Entwicklung und Tests..... 10
    - 3.1.1 Liste benötigter Hardware..... 10
  - 3.2 MuSeGa-Box..... 10
    - 3.2.1 MuSeGa-Box Hardware Details..... 11
- 4 Projektorganisation..... 11
  - 4.1 Projektmitarbeiter..... 11
  - 4.2 Betreuer..... 11
  - 4.3 Experte..... 11
  - 4.4 Arbeitszeiten und Wochenstunden..... 11
  - 4.5 Sitzungen mit Betreuern..... 12
- 5 Vorgehensmodell..... 12
- 6 Zeitplanung..... 12
  - 6.1 Arbeitsplan..... 13
  - 6.2 Zeitplan..... 13
    - 6.2.1 Meilensteine..... 13
  - 6.3 Zeitplan Grobübersicht..... 13



7 Dokumentation..... 13

- 7.1 Journal..... 13
- 7.2 Sitzungsprotokolle..... 13
- 7.3 Projektdokumentation..... 13
  - 7.3.1 Installationshandbuch..... 14
  - 7.3.2 Betriebshandbuch..... 14
  - 7.3.3 Technische Dokumentation..... 14
  - 7.3.4 Dokumentenablage..... 14
- 7.4 Testprotokolle..... 14
  - 7.4.1 Performance..... 14
  - 7.4.2 Bandbreitenmanagement..... 14
- 7.5 Code..... 14
- 7.6 Dokumentenübersicht..... 14
- 7.7 Sprachen..... 14

8 Ergebnisse..... 15

- 8.1 MuSeGa-Box..... 15
- 8.2 Sourcecode..... 15
- 8.3 Dokumentation..... 15

9 Beurteilung und Bewertung..... 15

10 Glossar..... 16

11 Quellen..... 16



## 1 Allgemeines

### 1.1 Sinn und Zweck

Die Aufgabe dieses Pflichtenheftes ist es, die Anforderungen an die Diplomarbeit und das resultierende Endprodukt zu spezifizieren. Die Kriterien wurden mit den Betreuern definiert. Aus dem Pflichtenheft sind die Aufgaben und die Rahmenbedingungen zur Durchführung der Arbeit ersichtlich.

### 1.2 Leserkreis

Dieses Pflichtenheft richtet sich an die Betreuer und den Experten. Um das Pflichtenheft verstehen zu können, sind Grundkenntnisse aus dem Bereich IT-Security unabdingbar.

### 1.3 Umfang

Das Pflichtenheft spezifiziert die Funktionen und Eigenschaften von MuSeGa, wie sie im Rahmen der Diplomarbeit realisierbar erscheinen. MuSeGa soll wenn möglich so aufgebaut werden, dass später weitere Funktionalitäten hinzugefügt werden können.

### 1.4 Anwendungsgebiet

Die Hochschule für Technik und Informatik (HTI) Bern stellt ihren Studenten, Mitarbeitern und Dozenten einen Wireless-Zugang zu ihrem Netzwerk zur Verfügung. Um den Zugangsschutz zu gewährleisten, wird momentan eine Lösung von Bluesocket (<http://www.bluesocket.com/>) eingesetzt. Diese Bluesocket-Box stösst aber schon bald an ihre Leistungsgrenze, da das Wireless-Netzwerk in naher Zukunft auf den neuen 54Mbit Standard (IEEE 802.11g) umgerüstet wird. Leistungsstärkere Lösungen von Bluesocket oder auch von anderen Herstellern haben sofort hohe Kosten zur Folge und hier kommt diese Diplomarbeit ins Spiel. Mit leistungsstarker PC-Hardware und Opensource-Software soll eine eigene Lösung für den gesicherten Zugang zum Hochschulnetz entwickelt werden.

## 2 Anforderungen an MuSeGa

Ziel der Arbeit ist es, einen funktionierenden Gateway abzugeben, der den zur Zeit eingesetzten „Bluesocket“ ersetzen, und in Sachen Performance überbieten kann. Welche Funktionen dieser Gateway genau bieten muss, wird im Abschnitt „*Technische Anforderungen*“ genau definiert.

### 2.1 Technische Anforderungen (Überblick)

Die Funktionen von MuSeGa werden nach drei Prioritäten geordnet. Priorität 1 bedeutet, dass diese Funktion auf jeden Fall implementiert sein muss. Priorität 2 steht für wünschenswerte Funktionen mit höherer Priorität. Priorität 3 und höher stellt Wunschfunktionen mit niedriger Priorität dar.



Kapitel	Funktion	Beschreibung	Priorität
2.2.1	Benutzerauthentifikation via RADIUS	MuSeGa soll die Benutzer via RADIUS Server authentifizieren können.	1
2.2.2	Stateful Firewall	MuSeGa soll über einen internen „Stateful Firewall“ verfügen, der standardmässig SWITCHMobile Verbindungen zulässt	1
2.2.3	VLAN Unterstützung	MuSeGa soll auch virtuelle Interfaces (VLANs) unterstützen	1
2.2.4	Admin via cmd und Web-GUI	MuSeGa soll via Commandline und via Web-GUI konfiguriert werden können	1
2.2.5	NAT/NAPT	MuSeGa soll Network Address Translation (NAT) und Network Address Port Translation (NAPT) unterstützen	1
2.2.6	DHCP Server	MuSeGa muss die Funktionalität eines DHCP Servers aufweisen	1
2.2.7	DNS Forwarding	MuSeGa muss als DNS Forwarder konfiguriert werden können	1
2.2.8	Statistik	Es sollen verschiedene Statistiken vom Gateway abgefragt werden können.	2
2.2.9	PPTP Endpunkt	MuSeGa soll auch als VPN Endpunkt (PPTP) eingesetzt werden können	2
2.2.10	SMTP Catch & Forward	MuSeGa soll SMTP Verbindungen abfangen können und sie an einen internen Mailserver weiterleiten können.	3
2.2.11	Bandbreiten Management	MuSeGa soll verschiedenen Diensten und Benutzern unterschiedliche Bandbreiten zuteilen können	3
2.2.12	IDS	MuSeGa soll zusätzlich noch ein integriertes Intrusion Detection System (IDS) haben	4
2.2.13	IPSec Endpunkt	Es wäre toll wenn MuSeGa als VPN Concentrator analog dem Cisco VPN Concentrator eingesetzt werden könnte	5

## 2.2 Technische Anforderungen (Details)

### 2.2.1 Benutzerauthentifikation via RADIUS

Einer der wichtigsten Punkte dieser Arbeit ist die starke Benutzerauthentifikation. Der Gateway muss also RADIUS (Remote Authentication Dial-in User Service) unterstützen, da an der HTI „single-sign-on“ Authentisierung auf Basis eines RADIUS Servers angestrebt wird. Es sollen möglichst alle gängigen RADIUS Server



(freeradius.org) unterstützt werden, sicherlich aber jenes Modell, welches an der HTI verwendet wird ([MS IAS/RADIUS Server](#)). An anderen RADIUS Server Implementationen sind gegebenenfalls Anpassungen nötig. Wenn also ein Client eine Verbindung mit dem internen Netzwerk herstellen will, kommt er vorerst nur bis zum MuSeGa. Handelt es sich um http Verkehr, wird der Client auf das Login-Screen des MuSeGa umgeleitet. Diese Verbindung ist mittels TLS verschlüsselt. Dort gibt der Benutzer seinen Namen und sein Passwort ein und diese Informationen werden anschliessend zum RADIUS Server übertragen. Falls eine positive Antwort vom Server zurückkommt, wird der Benutzer einer lokalen Gruppe zugewiesen und somit erbt er deren Rechte. Je nach Gruppenzugehörigkeit kann der Benutzer nun auf das interne Netzwerk, auf das Internet oder auf weitere Dienste zugreifen. Um dieses Konzept zu realisieren werden mindestens drei Gruppen benötigt. Diese sind die folgenden:

Gruppenname	Beschreibung
Not authorized	Nicht autorisierter Benutzer. Zum Beispiel nur SWITCHMobile Zugriff erlaubt
Guest	Gastbenutzer: Zum Beispiel nur Zugriff aufs Internet und auf spezielle Dienste möglich
Authorized	Autorisierter Benutzer. Zum Beispiel Zugriff auf interne Terminal- und Fileserver, Internet und vieles mehr.

Die Unterstützung lokaler Benutzer wäre wünschenswert, da sich so Administratoren auch noch einloggen können wenn der RADIUS Server einmal nicht zur Verfügung steht.

### 2.2.2 Stateful Firewall

MuSeGa muss „stateful packet filtering“ unterstützen. Das heisst, er kann feststellen welche eingehenden Netzwerkpakete zu welcher ausgehenden Verbindung gehört und umgekehrt. Dank diesem Feature können sehr viel sauberere und sicherere Firewallregeln definiert werden. Der Funktionsumfang des „Stateful Firewalls“ ist abhängig vom verwendeten Betriebssystem, da MuSeGa auf die Betriebssystem internen Firewallfunktionen zurückgreifen will. Da das verwendete Betriebssystem zu diesem Zeitpunkt aber noch nicht einwandfrei feststeht, ist der genaue Funktionsumfang des „Stateful Firewalls“ auch noch nicht genau gegeben. Es wird kein perfekter „Firewall-Regeln-Compiler“ mit Optimierungen erwartet, da dies alleine schon eine sehr anspruchsvolle Arbeit wäre. Weiter ist der Administrator der die Regeln via Web-GUI konfiguriert selber für fehlerhafte Konfigurationen verantwortlich und er muss diese auch selber korrigieren.

Defaultmässig soll der Firewall Zugang zu den VPN-Knoten des SWITCHMobile Netzwerkes gemäss folgenden Anforderungen ermöglichen:

<http://www.switch.ch/mobile/concept.txt>

### 2.2.3 VLAN Unterstützung

MuSeGa muss VLANs (Virtuelle LANs) unterstützen. Dadurch können dann auf einem physikalischen Netzwerkinterface mehrere, getrennte LANs angesprochen werden. Unterstützt werden VLANs nach IEEE 802.1Q, sofern das verwendete Betriebssystem von MuSeGa und die verwendeten Netzwerkkarten dies unterstützen. Es muss möglich sein, unterschiedlichen Benutzergruppen verschiedene VLANs zuzuteilen.



### 2.2.4 Administration via cmd und Web-GUI

MuSeGa muss bequem via Web-Interface administriert werden können. Parallel dazu sollten die gängigsten Konfigurationsschritte von MuSeGa aber auch via Kommandozeile (via SSH) administrierbar sein. Es wird kaum möglich sein die ganze Funktionalität des GUIs mit der Kommandozeile abzubilden. Das GUI ist also einer der Hauptpunkte bei der Erstellung von MuSeGa. Was genau damit administriert werden kann, beschränkt sich auf die Funktionalität von MuSeGa selber. Dies bedeutet es können alle gängigen Funktionen der einzelnen Module damit konfiguriert werden. Es kann aber kaum der volle Funktionsumfang eines Moduls abgedeckt werden.

### 2.2.5 NAT/NAPT

MuSeGa muss NAT (Network Address Translation) und NAPT (Network Address Port Translation) unterstützen. Dafür wird die vom Betriebssystem mitgelieferte NAT/NAPT Funktionalität inklusive allfälliger Limitierungen bezüglich VPN verwendet und so auch nur diese unterstützt. Im Falle von IPsec muss die Problematik NAPT/ESP durch NAT-Traversal vom Client gelöst werden.

### 2.2.6 DHCP Server

MuSeGa muss über die gängigsten Funktionen eines DHCP Servers verfügen, damit er den Clients die für die Kommunikation benötigten IP-Adressen zuteilen kann. Er muss mindestens in der Lage sein, dem Client:

- IP-Adresse
- Netzmaske
- Broadcast Adresse
- Default Gateway
- DNS-Server

Nach Möglichkeit wird der DHCP Server von [ISC](#) verwendet.

### 2.2.7 DNS Forwarding

MuSeGa muss in der Lage sein, von den Clients eintreffende DNS Querys an einen vorkonfigurierten, internen DNS Server weiterzuleiten. Unterstützt wird der UDP Port 53.

### 2.2.8 Statistik

Anhand der Statistik muss ersichtlich sein, wie viele Benutzer online sind und wieviel Bandbreite sie total in Anspruch nehmen. Die Statistik soll über das Web-GUI erreichbar sein. Wenn noch genügend Zeit zur Verfügung steht, können weitere Statistiken implementiert werden.

### 2.2.9 PPTP Endpunkt

MuSeGa soll als PPTP Endpunkt eingesetzt werden können. Das heisst die Benutzer bauen einen verschlüsselten PPTP Tunnel zum MuSeGa auf und können dann je nach ihren Benutzerrechten auf verschiedene weitere Dienste und Netze zugreifen. Unterstützt werden sollen die PPTP Clients von MS Windows 2000/XP/2003 sowie gängige Implementationen unter Linux. PPTP ist lange nicht so sicher wie IPsec, jedoch immer noch um einiges besser als die WEP-Verschlüsselung.



### 2.2.10 SMTP Catch & Forward

Die meisten Clients die sich beim MuSeGa anmelden, werden ihren eigenen Server für ausgehende Mails konfiguriert haben. Damit nun diese Clients ihre Konfiguration nicht dauern anpassen müssen, soll MuSeGa ausgehende Verbindungen auf Port 25 (SMTP) abfangen und an einen vorkonfigurierten, internen Mailserver der HTI weiterleiten. Dieser liefert dann die Mails an den zuständigen Server im Internet weiter.

### 2.2.11 Bandbreiten Management

Es muss möglich sein, unterschiedlichen Benutzergruppen und Diensten verschiedene Bandbreiten zuzuteilen. Dabei kann jeweils nur die Geschwindigkeit des „ausgehenden Verkehrs“ kontrolliert werden. Die genaue Funktionalität des Bandbreitenmanagements steht noch nicht fest, da sie wiederum abhängig vom verwendeten Betriebssystem ist.

### 2.2.12 IDS

Das IDS muss im Stande sein den unverschlüsselten Netzwerkverkehr zu überwachen, welcher direkt durch den Gateway fließt. Was überwacht werden kann ist abhängig vom verwendeten IDS. Mit grossen Wahrscheinlichkeit wird Snort zum Einsatz kommen. Die Konfiguration eines IDS ist sehr kompliziert und darum werden nur sehr grundlegende Konfigurationsschritte durch das Web-GUI und die Kommandozeile abgedeckt. Die vollumfängliche Konfiguration müsste man weiterhin direkt im IDS Konfigurationsfile vornehmen.

### 2.2.13 IPSec Endpunkt

MuSeGa muss als VPN Endpunkt (VPN Concentrator) eingesetzt werden können. Das heisst die Benutzer bauen einen verschlüsselten VPN Tunnel zum MuSeGa auf und können dann je nach ihren Benutzerrechten auf verschiedene weitere Dienste und Netze zugreifen. Unterstützt werden soll die IPSec Implementation von Cisco (Cisco IPSec Client und Cisco VPN Concentrator) mit der an der HTI verwendeten Konfiguration.

## 2.3 Allgemeine Anforderungen

### 2.3.1 Evaluierung des Betriebssystems und der Komponenten

Eine der Hauptarbeiten an MuSeGa besteht darin, zu Evaluieren welches Betriebssystem und welche Komponenten (Softwarepakete) sich am besten für den Einsatz im Mobile User Secure Gateway eignen. Dieser Punkt wird einige Zeit in Anspruch nehmen. Fest steht bis jetzt nur, dass es sich um eine UNIX/Linux-Art handeln wird. Bei der Evaluierung werden also verschiedene Kombinationen von Betriebssystemen und Softwarepaketen getestet und einander gegenübergestellt. Anhand noch zu definierenden Kriterien wird dann entschieden, welche Kombination sich am besten eignet. Die ganze Evaluierung wird mit Begründungen dokumentiert.

### 2.3.2 Verwendete Komponenten

MuSeGa soll möglichst aus Standardkomponenten entstehen. Dies bringt den Vorteil, dass man bequem die Updates der Software-Maintainer einspielen kann und nicht



selber Patches erstellen muss. Weiter soll MuSeGa vollkommen aus OpenSource aufgebaut werden.

### 2.3.3 Dimensionierung

Es wird angestrebt, dass MuSeGa >100 gleichzeitige Benutzer unterstützen kann.

### 2.3.4 Verwendungsrechte von MuSeGa

Der selbst geschriebene Code von MuSeGa wird unter der [GPL](#) (GNU General Public License) entwickelt. Die Rechte an MuSeGa bleiben beim Diplomanden und der HTI.

### 2.3.5 Sprachen

Sämtliche Benutzerschnittstellen sind in englischer Sprache. Bei der Entwicklung soll aber darauf geachtet werden, dass auch weitere Sprachen möglichst problemlos implementiert werden könnten.

## 3 Hardware

### 3.1 Hardware für Entwicklung und Tests

Für die Entwicklung und Tests muss von der Hochschule diverse Hardware zur Verfügung gestellt werden.

#### 3.1.1 Liste benötigter Hardware

Was	Details	Wofür	Wann
MuSeGa-Box	PC (i386) neuerer Generation mit mehreren Netzwerkkarten (>=100MBit)	Entwicklung, Tests	immer
Test Client	PC (i386) neuerer Generation mit >=100MBit Interface (Standard HTI PC)	Tests	immer
Netzwerkzugang	Zugriff auf die restliche Netzwerk Infrastruktur der Hochschule, RADIUS Server, VPN Concentrator, etc..	Entwicklung, Tests	immer
PC-Raum	>= 25 schnelle Rechner	Performance Tests	Testphase
101 Studenten	>=101 Studenten mit ihren Notebooks/PCs wären wünschenswert	Performance-, Stabilitäts-Test	Testphase, Endphase

### 3.2 MuSeGa-Box

Spätestens wenn die Performance-Tests anstehen, sollte die endgültige MuSeGa Hardware bereitstehen. Die folgende Tabelle kann als Wunschliste angesehen werden. Es muss also von der HTI nicht genau die hier aufgeführte Hardware zur Verfügung gestellt werden.



### 3.2.1 MuSeGa-Box Hardware Details

Was	Details
Gehäuse	ca. 2-4 HE Rackmount Gehäuse mit redundanten Netzteilen
Mainboard	Server Chipset Mainboard, mit mindestens 2 CPU Slots
Prozessoren	Mindestens 2 CPUs, (Intel Xeon MP, AMD Opteron)
Speicher	>=2GB
Festplatten	4x 72GB Ultra320 SCSI (15k rpm) für RAID5 mit Hotspare: Netto 140GB
Netzwerkkarten	Mindestens 2x Gigabit Ethernet (ev. mit Hardwarverschlüsselung) 1x 100MB Management-Interface (Administration, Backup, etc.)
RAID Controller	Ultra320 SCSI RAID Controller (RAID 0,1,5,10)
Grafikkarte	Onboard oder low-end Grafikkarte
DVD Laufwerk	Standard IDE DVD Laufwerk

## 4 Projektorganisation

### 4.1 Projektmitarbeiter

Name	Email	Telefon
Lukas Reusser	i00reuss @ hti.bfh.ch	+41 79 305 91 71

### 4.2 Betreuer

Name	Email	Telefon
Hansjürg Wenger	hansjuerg.wenger @ bfh.ch	+41 31 33 55 222
Gerhard Hassenstein	gerhard.hassenstein @ bfh.ch	+41 31 33 55 248

### 4.3 Experte

Name	Email	Telefon
Andreas Duersteler	andreas.duersteler @ swisscom.com	+41 31 342 63 14

### 4.4 Arbeitszeiten und Wochenstunden

Bis Mitte Juli haben wir noch normal Schule. Während dieser Zeit werden 10 Stunden pro Woche in die Diplomarbeit investiert. Danach ist die Schule abgeschlossen und es werden 16 Stunden pro Woche sein. Während einigen Wochen (Ferien, Prüfungen, Zertifizierungen) werden aber aus Zeitgründen weniger, oder gar keine Stunden in die Diplomarbeit investiert. Die komplette Liste aller Kalenderwochen mit den entsprechenden Wochenstunden und Begründungen befinden sich hier:

[http://musega.ch/docs/verteilung\\_wochenstunden.pdf](http://musega.ch/docs/verteilung_wochenstunden.pdf)



Die Arbeit wird meistens Freitags (09h00 – 12h00, 13h00 – 18h00) und am Wochenende stattfinden.

### 4.5 Sitzungen mit Betreuern

Alle zwei bis drei Wochen findet eine Sitzung mit den Betreuern statt um den Projektstand zu Besprechen. Dauer jeweils ca. 30-60 Minuten.

## 5 Vorgehensmodell

Während dem Projekt orientiert man sich an folgendem Vorgehensmodell:

Projektphase	Inhalt	Resultat
Initialisierung	<ul style="list-style-type: none"> <li>- Aufnahme der Problemstellung</li> <li>- Einarbeiten in Problematik</li> <li>- Definition des Vorgehens und der Ziele</li> <li>- Aufstellen der anstehenden Tätigkeiten</li> <li>- Aufwandabschätzung, Zeitplan</li> </ul>	Pflichtenheft Arbeitsplan Zeitplan
Analyse & Design	<ul style="list-style-type: none"> <li>- Eingehende Studie der Fachgebiete</li> <li>- Geforderte Funktionen analysieren und mögliche Implementationen abklären. Diese dann eventuell testen.</li> <li>- Konfigfiles, Datenbankstrukturen festlegen</li> <li>- User Interfaces definieren (Masken, Syntax, ..)</li> </ul>	Analyse Dokumente Design Dokumente
Realisierung & Tests	<ul style="list-style-type: none"> <li>- Erstellen der MuSeGa Software</li> <li>- Diverse Tests durchführen</li> <li>- Dokumentation erstellen</li> </ul>	Quellcode Installationshandbuch Betriebshandbuch Technische Dokumentation Testprotokolle
Abschluss	<ul style="list-style-type: none"> <li>- Alles abschliessen, überprüfen</li> <li>- Schlussbericht</li> </ul>	Schlussbericht

## 6 Zeitplanung

Für die ganze Diplomarbeit sind ca. 400 Mannstunden eingeplant. Wie diese Zahl zustande kommt, kann folgender Tabelle entnommen werden:

[http://musega.ch/docs/verteilung\\_wochenstunden.pdf](http://musega.ch/docs/verteilung_wochenstunden.pdf)



### 6.1 Arbeitsplan

Im Arbeitsplan wurden grob alle anstehenden Tätigkeiten zusammengefasst und mit einer Aufwandabschätzung versehen. Zu diesem Zeitpunkt ist es natürlich nicht ganz einfach einen genauen Arbeitsplan zu erstellen. Darum muss er im Verlauf des Projektes ziemlich sicher noch angepasst werden. Die aktuelle Version des Arbeitsplanes ist jeweils unter <http://musega.ch> zu finden.

Setzt man nun den Arbeitsplan in einen Zeitmasstab, erhält man den groben Zeitplan.

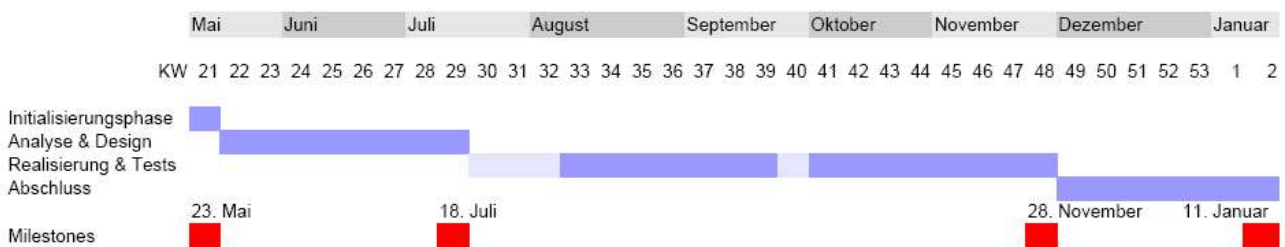
### 6.2 Zeitplan

Im Zeitplan sind grob alle anfallenden Tätigkeiten in ihrer zeitlichen Abfolge grafisch dargestellt. Da der Zeitplan abhängig vom Arbeitsplan ist, wird auch dieser im Verlauf des Projekts ziemlich sicher noch angepasst werden müssen. Der aktuelle Zeitplan steht auf der Projekthomepage <http://musega.ch> zur Verfügung.

#### 6.2.1 Meilensteine

Meilensteine sind aus dem Zeitplan ersichtlich.

### 6.3 Zeitplan Grobüberblick



## 7 Dokumentation

### 7.1 Journal

Es soll ein Arbeitsjournal geführt werden, wo alle Tätigkeiten eingetragen werden. Zusätzlich soll noch die dafür aufgewendete Zeit rapportiert werden. Das Journal ist jederzeit unter <http://musega.ch> abrufbar.

### 7.2 Sitzungsprotokolle

Nach jeder Sitzung soll ein Protokoll erstellt werden, welches kurz die wichtigsten besprochenen Themen und Entscheidungen der Sitzung festhält. Alle Sitzungsprotokolle sind unter <http://musega.ch> verfügbar.

### 7.3 Projektdokumentation

Zur Projektdokumentation zählen folgende Dokumente:



### 7.3.1 Installationshandbuch

Im Installationshandbuch wird erläutert wie man vorgehen muss, um MuSeGa in seinem vollen Funktionsumfang auf einem System zu installieren. Das Handbuch richtet sich an erfahrene Systemadministratoren.

### 7.3.2 Betriebshandbuch

Das Betriebshandbuch beschreibt im wesentlichen wie man via Web-GUI und Kommandozeile vorgehen muss, um MuSeGa korrekt zu konfigurieren. Das Betriebshandbuch richtet sich an erfahrene Systemadministratoren.

### 7.3.3 Technische Dokumentation

In der technischen Dokumentation wird hauptsächlich darauf eingegangen, wie das Web-GUI und die Kommandozeile mit der Konfiguration der einzelnen Komponenten zusammenhängt. Sie wird wenn möglich kurz gehalten, da die technische Funktion bereits aus dem dokumentierten Sourcecode ersichtlich sein sollte. Weiter enthält sie aber noch eine genaue Beschreibung des ganzen Systems. Dazu gehörten die Hauptkomponenten der Hardware, verwendetes Betriebssystem mit Version, Kernelversion sowie eine Liste aller verwendeter Software mit ihrer Versionsnummer. Die technische Dokumentation richtet sich an erfahrene Systemadministratoren.

### 7.3.4 Dokumentenablage

Die aktuelle Dokumentation ist jeweils unter <http://musega.ch> verfügbar.

## 7.4 Testprotokolle

### 7.4.1 Performance

Die Performance von MuSeGa muss getestet und in Testprotokollen festgehalten werden. Wie genau diese Test aussehen werden wird erst später bestimmt.

### 7.4.2 Bandbreitenmanagement

Falls die optionale Funktion „Bandbreitenmanagement“ implementiert wird, muss deren Funktion durch Messungen ausgewiesen und in Testprotokollen festgehalten werden. Wie genau diese Test aussehen werden wird erst später bestimmt.

## 7.5 Code

Der geschriebene Sourcecode wird „inline“ ausreichend kommentiert, so dass keine weitere Dokumentation für den Code nötig ist. Je nach Programmiersprache kann dann aus dem Sourcecode eine Dokumentation in HTML erstellt werden.

## 7.6 Dokumentenübersicht

Es soll ein Dokument erstellt werden, in dem alle erstellten Dokumente mit ihren aktuellen Versionen aufgelistet sind.

## 7.7 Sprachen

Das Journal, die Sitzungsprotokolle sowie die gesamte Projektdokumentation wird in



deutscher Sprache geschrieben. Der Sourcecode wird in englisch kommentiert. Ebenfalls werden alle Benutzerschnittstellen in englischer Sprache sein.

## 8 Ergebnisse

### 8.1 MuSeGa-Box

Schlussendlich wird eine wie oben spezifizierte Lösung als Gesamtpaket erwartet. In welchem Umfang die gesteckten Ziele zu erreichen sind, ist aufgrund der bevorstehenden Analyse- und Evaluationsphase noch nicht ganz klar. Die abgelieferte „MuSeGa-Box“ soll aber wenn möglich nach dem Einbau ins Rack und kurzer Konfiguration, ihren Dienst als „Bluesocket“ Ersatz aufnehmen können.

### 8.2 Sourcecode

Der geschriebene Quellcode ist für Betreuer und Experte in vollem Umfang verfügbar.

### 8.3 Dokumentation

Siehe 7 Dokumentation

## 9 Beurteilung und Bewertung

Die Bewertungsliste wurde mit den Betreuern wie folgt festgelegt:

	Arbeitsschritt	Gewicht
Vorbereitungsphase	Aufbau und Vollständigkeit des Pflichtenheftes	3
Durchführung	Arbeits- und Zeitplanung	2
	Kreativität, Initiative, Selbständigkeit	3
	Wahl und Anwendung der (Arbeits-)Methodik	3
	Implementation, Programmierstil	3
	Systemtest (Verfahren, Durchführung, Bericht)	2
	Kommunikation mit Experten und Betreuer	1
Ergebnis	Übereinstimmung Endprodukt/Pflichtenheft	5
	Allgemeiner Eindruck aus der Besichtigung	1
Projektbericht	Inhalt korrekt, vollständig, verständlich	3
	Sprache, Stil, Übersichtlichkeit	1
	Klare, aussagekräftige Zusammenfassung	1



## 10 Glossar

Der Glossar wird aufgrund der einfacheren Erweiterung in einem separaten Dokument geführt. Er ist unter <http://musega.ch> zu finden.

## 11 Quellen

- Informatik Projektentwicklung von Carl August Zehnder (2. Auflage 1991)  
ISBN 3 7281 1761 7
- HTA-BE Website: Beurteilung der Diplomarbeit (02.05.2004)  
<http://www.hta-be.bfh.ch/~wwwinfo/di/beurteilung/beurt.php3>
- HTA-BE Website: Ausschreibung Mobile User Secure Gateway (02.05.2004)  
<http://www.hta-be.bfh.ch/~wwwinfo/di/04/WirelessSecureGateway.shtml>
- SWITCHMobile Konzept (01.06.2004)  
<http://www.switch.ch/mobile/concept.txt>