Konzeptbericht (Applikationsentwicklung)

Auftraggeber	Beat Walter
Projektleiter	Agash Thamotharampillai
Autor	Agash Thamotharampillai, Marc Trittibach, Jonathan Camenzind
Klassifizierung	Intern
Status	In Arbeit

Änderungsverzeichnis

Datum	Version	Änderung	Autor
04.03.2014	0.1	Dokument wurde erstellt.	Jonathan Camenzind
11.03.2014	0.2	Use-Case Diagramm erstellt, Klassendiagramme und Systemdiagramme erstellt.	Agash Thamo.
18.03.2014	0.3	Korrekturen und Ergänzungen gemäss Email vom Auftraggeber	Agash Thamo., Marc Trittibach

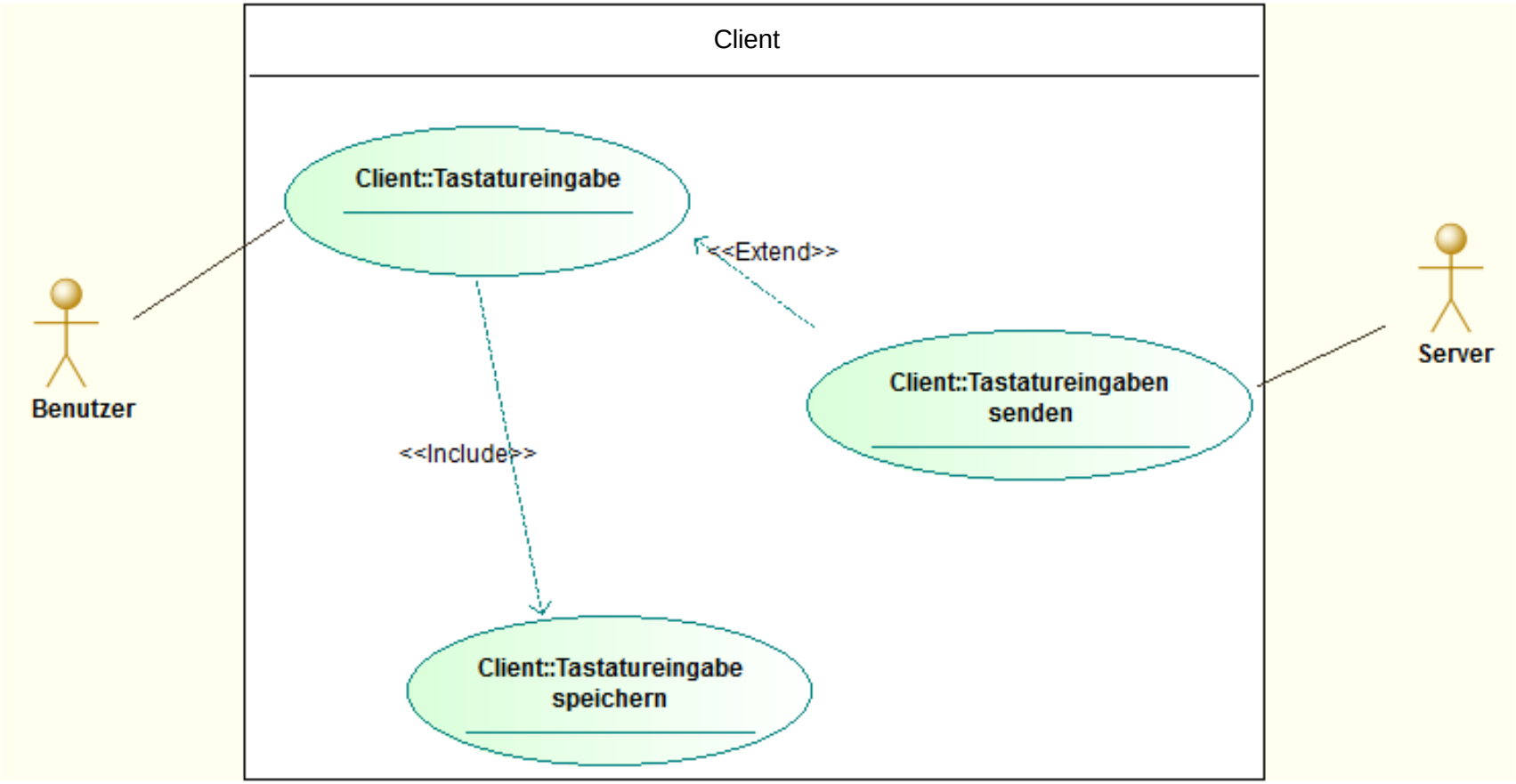
Inhaltsverzeichnis

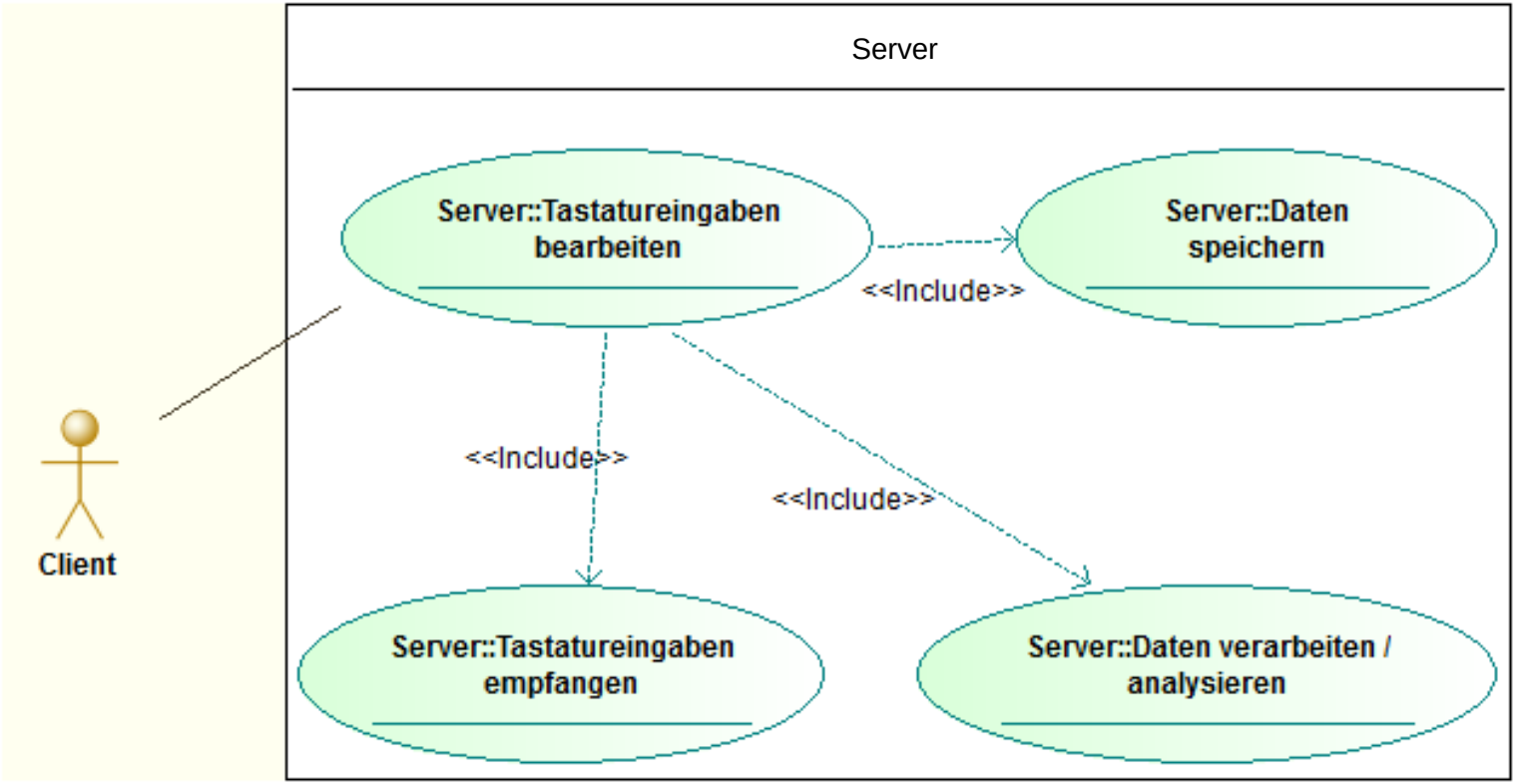
1 Zusammenfassung

Dieses Dokument beschreibt die technischen Anforderungen für den Rahmen des Schulprojekts zu realisierenden Keylogger.

2 Systemanforderungen

2.1 Übersicht Anwendungsfälle




Server
Server::Tastatureingaben bearbeiten
Server::Daten speichern
<<Include>>
<<Include>>
<<Include>>
Client
Server::Tastatureingaben empfangen
Server::Daten verarbeiten / analysieren

Anwendungsfall Client::Tastatureingabe

Anwendungsfall Client::Tasteneingabe	
Kurzbeschreibung	Der Benutzer auf dem Clientcomputer macht eine Eingabe auf der Tastatur.
Akteure	Der Benutzer auf dem Computer wo der Keylogger-Client ausgeführt wird.
Vorbedingungen	Damit dieser Anwendungsfall geschehen kann, muss die der Keylogger-Client auf dem Computer ausgeführt werden.
Ablauf	1. Der Benutzer befindet sich in einer Applikation auf dem Computer (Windows selbst oder irgendwas sonst) 2. Der Benutzer tätigt in dieser Applikation eine Tasteneingabe
Resultat	Die eingegebene Taste wird temporär Zwischengespeichert und bei Gelegenheit an den Server gesendet
Ausnahmen	Solange der Keylogger auf dem Client ausgeführt wird sollten keine Ausnahmen möglich sein. Falls keine Verbindung zum Server existiert werden die Daten temporär abgespeichert und bei Verbindung mit dem Server an den Server gesendet.

Anwendungsfall Server::Tastatureingaben bearbeiten

Anwendungsfall Server:: Tastatureingaben Einsehen	
Kurzbeschreibung	Der Benutzer auf dem Servercomputer liest die an den Server gesendeten und ausgewerteten Daten aus.
Akteure	Der Benutzer auf dem Computer wo der Keylogger-Server ausgeführt wird.
Vorbedingungen	Der Server hat bereits Daten erhalten und ausgewertet.
Ablauf	1. Der Benutzer navigiert zum Dateipfad, wo die Auswertungsdatei existiert. 2. Der Benutzer öffnet die Datei und sieht die Daten an.
Resultat	Der Benutzer kennt die Tasteneingaben (Welche Taste, welches Programm, welche Zeit, welcher Client)
Ausnahmen	Es sind noch keine Daten auf dem Server vorhanden. Ergo: Die Datei ist leer.

2.2 Product Backlog

Verbindung herstellen

- Als **Client**
- Möchte ich **automatisch eine Verbindung zum Server herstellen**
- Damit ich **Daten an den Server schicken** kann

Priorität: Hoch

Keyboard-Inputs lesen

- Als **Client**
- Möchte ich **die Tasteneingaben des Benutzers einlesen und speichern**
- Damit ich **die Daten für spätere Auswertungen zur Verfügung habe**

Priorität: Sehr Hoch

Gespeicherte Daten senden

- Als **Client**
- Möchte ich **die gesammelten Daten zum Server schicken**
- Damit diese **auf dem Server ausgewertet/verarbeitet werden können**

Priorität: Normal

Empfangene Daten verarbeiten

- Als **Server**
- Möchte ich **die empfangenen Daten analysieren**
- Damit ich **Keywörter, meist genutzten Wörter und diverse andere Daten erkennen** kann

Priorität: Niedrig

3 Benutzerschnittstelle

3.1 Client

Der Client besitzt an sich keine Schnittstelle, über welcher der Benutzer eventuelle Bedienelemente steuern könnte. Einzig die Konfiguration des Clients kann man mittels XML-Files verändern.

3.2 Server

Der Server bietet, wie auch der Client, keine „richtige“ Schnittstelle. Die Informationen werden in Files gespeichert, diese sind die Schnittstelle zwischen dem Benutzer und dem Server. Ebenfalls, lässt sich der Server über XML-Files konfigurieren.

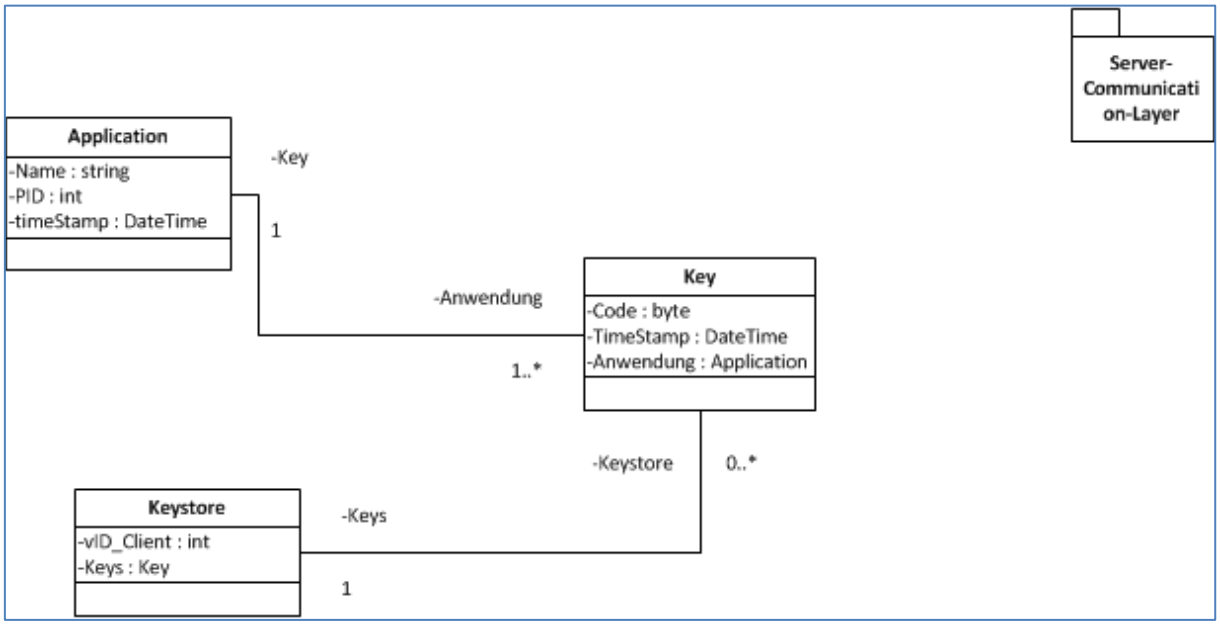
4 Systemarchitektur

4.1 Subsysteme

4.2 Gliederung der Lösung

4.2.1 Klassendiagramme

4.2.1.1 Client



Application

Die „Application“ Klasse enthält Informationen über ein bestimmtes Programm z.B. Internet Explorer. Erfasst werden dabei die Bezeichnung des Programms, die Prozess ID und ein timestamp wann das Fenster den Fokus bekommen hat.

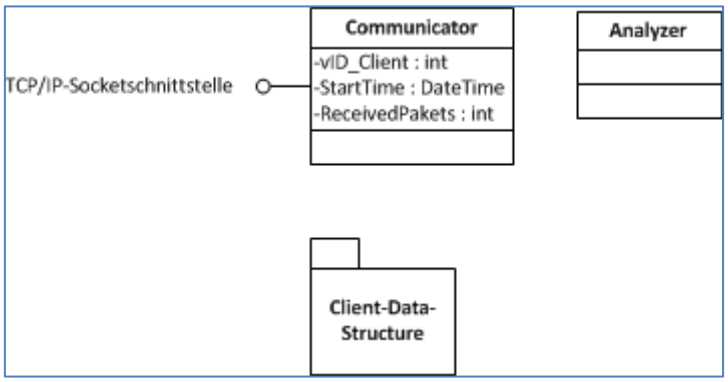
Key

Die „Key“ Klasse enthält die Information über eine Taste welche vom Client gedrückt wurde. Erfasst wird dabei der ASCII Code des Keys, ein Timestamp wann die Taste gedrückt wurde und eine Referenz zu einer Applikation in welcher die Taste gedrückt wurde.

Keystore

Der „Keystore“ stellt den Zwischenspeicher dar, welcher die Keys enthält bevor diese über das Netzwerk zum Server gesendet werden. Zusätzlich wird als ID die MAC Adresse des Clients mitgesendet.

4.2.1.2 Server



Communicator

Die Klasse „Communicator“ stellt eine Verbindung zu einem spezifischen Client dar. Dabei wird die MAC Adresse, die Startzeit der Verbindung und die Anzahl erhaltener Pakete gespeichert.

Analyzer

Der Analyzer hat die Aufgabe, die von den Clients erhaltenen Informationen zu analysieren und auszuwerten.

4.3 Schnittstellen

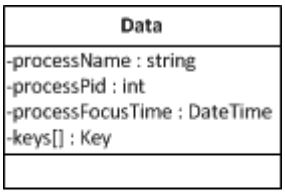
Unser Projekt beinhaltet bloss eine Schnittstelle. Diese ist eine Netzwerkschnittstelle, die wir über die Funktionalität von C#.Net entwickeln.
Der Namespace für diese Funktionalitäten lautet wie folgt:

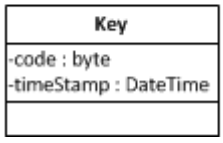
- System.Net.Sockets

Die Verbindung vom Client zum Server wird über TCP/IP errichtet. Der Server sowie der Client hören auf alle verfügbaren IP-Adressen des Computers.

4.3.1 Meldungstypen

Es wird nur einen Meldungstypen geben, dieser ist wie folgt aufgebaut:





Gesendet werden die „Data“-Objekte, das Key-Model wurde hier nur zwecks Informationsgehalts hinzugefügt.

5 Qualitätssicherung

Blackbox – Systemtests

Nr.	User Story	Beschreibung	Soll
1	Keyboard Inputs Lesen	Der Benutzer gibt auf dem Client Computer **eine** Tasteneingabe ein. Es besteht keine Verbindung zum Server.	Die Tasteneingabe wird auf dem Client temporär zwischengespeichert.
2	Keyboard Inputs lesen	Der Benutzer gibt auf dem Client Computer **mehrere** (> 1KB) Tasteneingaben ein. Es besteht keine Verbindung zum Server.	Alle Tasteneingaben werden auf dem Client zwischengespeichert.
3	Keyboard Inputs lesen	Der Benutzer gibt auf dem Client Computer **eine** Tasteneingabe ein. Es besteht eine Verbindung zum Server.	Die Tasteneingabe wird auf dem Client zwischengespeichert. Nach dem Senden ist der temporäre Speicher wieder leer.
4	Keyboard Inputs lesen	Der Benutzer gibt auf dem Client Computer **mehrere** (> 1KB) Tasteneingaben ein. Es besteht eine Verbindung zum Server	Die Tasteneingaben werden auf dem Client zwischengespeichert. Nach dem Senden ist der temporäre Speicher wieder leer.
5	Keyboard Inputs lesen	Der Benutzer gibt auf dem Client einen Grossbuchstaben ein	Die Tasteneingabe wird so zwischengespeichert, dass daraus folgend wiederum ein Grossbuchstabe reproduziert werden kann.
6	Keyboard Inputs lesen	Der Benutzer gibt auf dem Client ein CTRL + Alt + Delete ein.	Die Tasteneingabe wird so zwischengespeichert, dass daraus folgend wiederum ein Ctrl + alt + Delete reproduziert werden kann.
7	Verbindung herstellen	Der Client wird gestartet, während keine Verbindung zum Server hergestellt werden kann.	Der Client wird gestartet und liest die Tasteneingaben in den temporären Speicher ein.
8	Verbindung herstellen	Der Client wird gestartet, während eine Verbindung zum Server möglich ist.	Der Client wird gestartet und stellt eine Verbindung zum Server her. Die Tasteneingaben werden auf dem Client zwischengespeichert und danach an den Server geschickt.
9	Verbindung her-	Der Client wird gestartet	Der Client wird nach dem Verbindungs-

	stellen	und er stellt eine Verbindung zum Server her. Der Server wird währenddessen heruntergefahren.	abbruch die Daten temporär Speichern und weiterhin funktionieren.
10	Verbindung herstellen	Der Client wird ohne Verbindung gestartet. Der Server wird danach gestartet, wobei die Konfiguration des Client mit dem des Servers übereinstimmt.	Der Client wird nachdem der Server erreichbar ist die Verbindung mit dem Server herstellen.
11	Verbindung herstellen	Testfall 10 ausführen, wobei im Zwischenspeicher Daten vorhanden sind.	Der Client schickt dem Server die gespeicherten Daten.
12	Verbindung herstellen	Der Server wird gestartet ,ohne dass ein Client die Verbindung herstellt	Der Server zeigt an, dass kein Client verbunden ist.
13	Verbindung herstellen	Der Server wird gestartet, während ein Client die Verbindung herstellen will. (Gegenstück zu Testfall 10)	Der Server stellt die Verbindung mit dem Client her, sobald der Client eine Anfrage schickt.
14	Verbindung herstellen	Der Server läuft ohne Verbindung. Anschliessend wird ein Client gestartet.	Der Server stellt die Verbindung mit dem Client her.
15	Verbindung herstellen	Der Server läuft mit einer (oder mehreren) Clientverbindung. Ein weiterer Client stellt die Verbindung her.	Der Server stellt die Verbindung mit dem weiteren Client her. Die Clients sind in der Ausgabe der Servers zu unterscheiden.

6 Projektplanung

Die Projektplanung wurde in einem separaten Dokument geführt:

Siehe 1_3_projektplan Version 1.0 – 04.03.2014