HÖHERE TECHNISCHE BUNDESLEHRANSTALT WIEN 3, RENNWEG 89B
Höhere Abteilung für Informationstechnologie
Ausbildungsschwerpunkt Internet und Medientechnik, Netzwerktechnik

Projektnummer: **3R IT 15 19**		Wien, im September 2015

Ansuchen um Genehmigung einer Aufgabenstellung für die

DIPLOMARBEIT

Jahrgang: **5DN** Schuljahr: **2014/15**

Thema: Raven

Verschlüsselte, plattformunabhängige Kommunikation

Aufgabenstellung: Die Idee ist, eine reine End-zu-End Verschlüsselung für verschiedene Dienste wie Facebook, WhatsApp, SMS, E-Mail etc. zu entwickeln. Hierbei werden die Schlüssel nur auf den zwei betroffenen Geräten gespeichert, die anschließend direkt miteinander kommunizieren können, ohne die Hilfe eines zentralen Servers.

Das Ziel ist es, eine Software für Android und PC zu entwickeln, welche eine verschlüsselte Kommuniaktion über SMS und E-Mail anbieten. Für die PC-Version ist dir Kommunikation über SMS, für beide der Nachrichtenaustausch über Facebook ein optionales Ziel.

Anzahl der Beiblätter: 15

Zuordnung zu den Fachgebieten: Netzwerkprogrammierung (NTPR)

Kandidaten: **Philipp ADAM (PL)** .....
Projektleiter, PC-Version

Manuel CASPARI .....
Stv. Projektleiter, Androidanwendung

Nicolas LUKASCHEK .....
PC-Version

Betreuer: **Ferdinand KASPER (Hauptbetreuer)** .....

August HÖRANDL .....

Herbert SASSHOFER .....

....
AV Mag. Dr. Gerhard HAGER Dir. Mag. DI Dr. Martin WEISSENBÖCK

Als Diplomarbeit zugelassen

.....
LSI DI Judith WESSELY-KIRSCHKE

Executive Summary

Objectives

The main goal is the development of a software, which allows encrypted communications. The keys for the encryption shall only be stored on the devices themselves, no background server infrastructure shall be required.

The software must be available for PC and Android. The PC-version must be able to send and receive encrypted e-mails. The Android-version must be able to send and receive encrypted e-mails and SMS. For both versions it is an optional goal to send encrypted messages over Facebook.

Risks

The top risk is that the communication over Facebook cannot be implemented with justifiable expenditure. Therefore this goal is optional and not a critical factor for the project.

Milestones (Table of the most important milestones)

Date	Milestone
22.09.14	Project planning completed
06.10.14	Implementation concept created
08.12.14	Application is operable
26.01.15	Application can be published

Budget and Resources

Which hardware and software is needed?
Only an IDE (eclipse), an android sdk and a handy running android is needed.

Short summary of costs
This project causes no costs, all requirements are provided by the team.

Project budget	0€
Costs for school	0€
Total man hours	600 h.

Inhaltsverzeichnis

1 Projektidee

1.1 Ausgangssituation

Die Hintergrundgeschichte, die uns auf diese Idee brachte, war eine relativ einfache und noch immer in den Medien heiß diskutierte. Neben dem aufgedeckten NSA-Spionageskandal, der der gesamten Menschheit bewusst machte, dass kein digitaler Schritt unbemerkt bleibt und aufgezeichnet wird, war ebenfalls die Monopolstellung durch Facebook, insbesondere nach dem Kauf von WhatsApp, ein Hauptgrund. Es gilt als allgemein bekannt, dass Facebook & Co Hand in Hand mit der NSA gehen, obgleich sie diese Tatsache vehement abstreiten.

Es mag zwar bereits diverse Verschlüsselungsmethoden für Onlinekommunikation und Datenübertragungen geben, allerdings haben diese jedoch oftmals sogenannte Backdoors („Hintertüren“) eingebaut, welche den Sinn der Verschlüsselung ad absurdum führen. Dadurch ist es diesen Spionagekonzernen ohnehin möglich, den gesamten weltweiten Nachrichtenverkehr von der Initiierung weg bis zur Terminierung mitzulesen und in die Privatsphäre jedes Einzelnen einzugreifen.

Abschließend ein Zitat eines Gründervaters der Vereinigten Staaten von Amerika:

“Those who surrender freedom for security will not have, nor do they deserve, either one.”

- Benjamin Franklin

1.2 Beschreibung der Idee

Die Idee ist, eine echte End-zu-End Verschlüsselung für verschiedene Dienste, wie Facebook, WhatsApp, SMS, E-Mail etc. zu entwickeln. Hierbei werden die Schlüssel nur auf den zwei betroffenen Geräten gespeichert, die anschließend direkt miteinander kommunizieren können, ohne Hilfe eines zentralen Servers.

Gerade in Zeiten von Datenschutz- und NSA-Skandalen werden die Rufe nach einer einfachen und sicheren Verschlüsselung immer lauter.
Genau das möchten wir mit unserer Anwendung erreichen, eine einfach zu bedienende Software, mit der man über viele verschiedene Dienste sicher kommunizieren kann. Dies soll sowohl auf einem herkömmlichen PC, als auch auf der mobilen Plattform Android funktionieren. Unsere Anwendung dient hierbei als Multi-Messenger, welcher all diese Dienste vereint. Bei der Verschlüsselung werden wir auf herkömmliche Methoden verzichten und mehrere sichere Verfahren kombinieren, um die höchstmögliche Sicherheit gewährleisten zu können.

2 Projektziele

2.1 MUSS Ziele

2.1.1 Androidanwendung

Gefordert wird eine Androidanwendung, welche Schlüssel generieren und lesen kann und mithilfe dieser verschlüsselte Nachrichten sendet und empfängt.
Der Schlüssel soll sich aus dem Produkt der Hashfunktion Blake512, welche als Parameter vom System bereitgestellte Zufallszahlen (/dev/random) erhält bilden. Der Schlüsselaustausch zwischen Android-Geräten muss sowohl mittels QR-Code (Quick Response Code) ,als auch NFC (Near Field Communication) möglich sein. Beim Lesen des Schlüssels soll die Telefonnummer des Kommunikationspartners mit dem gelesenen Schlüssel in Verbindung gebracht werden. Sendet A nun beispielsweise eine SMS an B, so ist diese mittels AES und MARS (Verschlüsselungsalgorithmen) zu verschlüsseln und an B zu übermitteln. B soll die SMS mit demselben Key entschlüsseln. Es findet also eine symmetrische Verschlüsselung statt.
Die Anwendung muss zur Fertigstellung auf Deutsch und Englisch verfügbar sein.

2.1.2 Desktopanwendung

Gefordert wird eine Desktopanwendung, welche Schlüssel generieren und lesen kann und mit diesen Nachrichten über das Internet (IP) verschlüsselt sendet und empfängt.
Mit der Anwendung soll eine textbasierte, verschlüsselte Kommunikation über E-Mail möglich sein. Der Schlüsselaustausch zwischen den Kommunikationspartnern soll dabei im Voraus (pre-shared) erfolgen oder es findet ein asymmetrischer Schlüsselaustausch (mittels Diffie-Hellman) statt. Der Key muss dabei ebenfalls zufällig erzeugt werden.Mithilfe der Java Klasse SecureRandom werden sogenannte "cryptographically strong random numbers" generiert, welche als Basis für die Schlüsselerzeugung herangezogen werden sollen.
Funktional sollen Desktopanwendung und Android-App gleichwertig sein, wobei die Desktopanwendung natürlich weder SMS versenden, noch QR-Codes lesen können muss.

2.2 Optionale Ziele

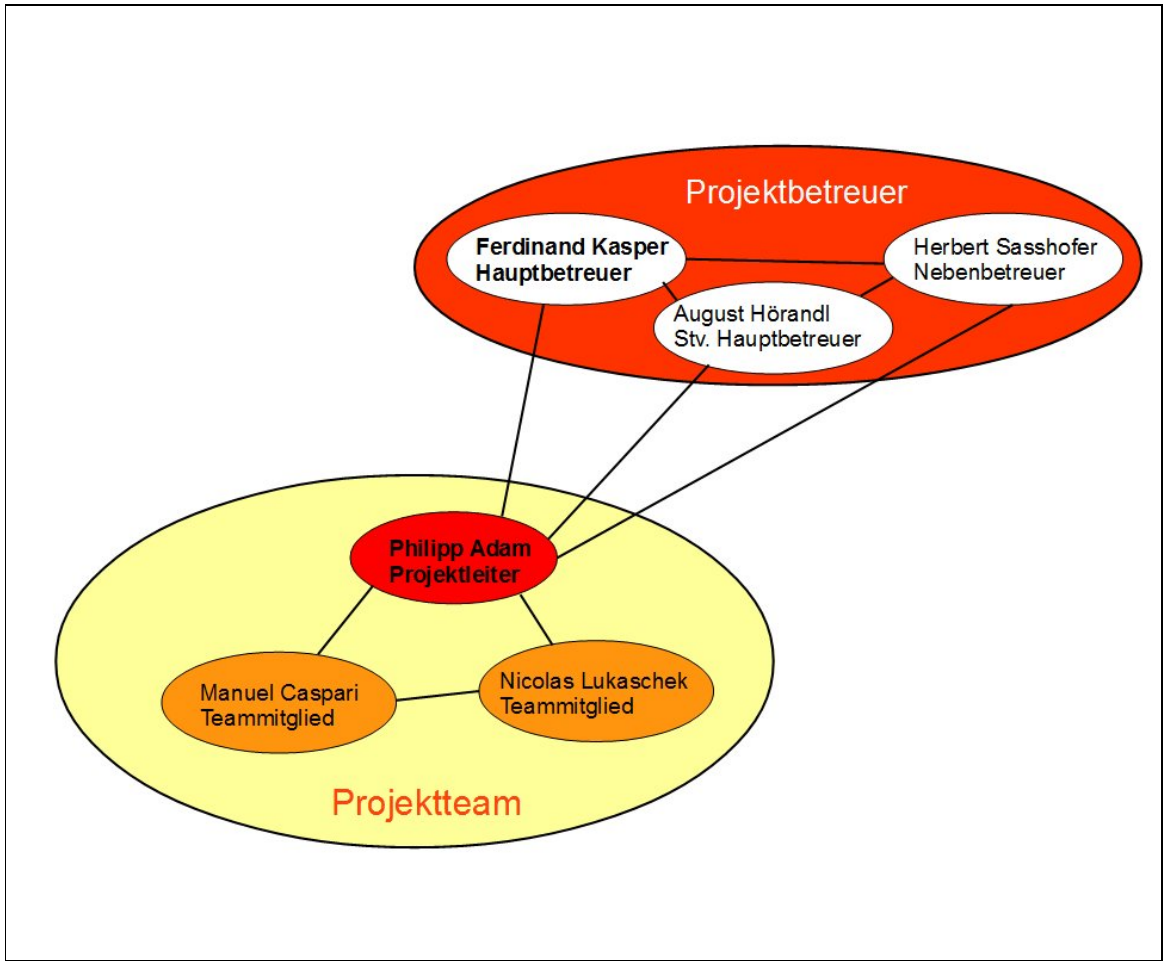
Sowohl Androidanwendung, als auch Desktopanwendung können verschlüsselt über Facebook Nachrichten austauschen

2.3 NICHT Ziele

Es wird eine User-Guide geschaffen, welches dem User grundlegende Anwendungsfunktionen erklärt

3 Projektorganisation

3.1 Grafische Darstellung (Empowered Projektorganisation)



3.2 Projektteam

Funktion	Name	E-Mail	Funktion
PL	Philipp Adam	philipp.adam@tmo.at	PL
STV PL	Manuel Caspari	manuel@caspari.at	STV PL
PTM	Nicolas Lukaschek	nicolas.lukaschek@outlook.com	PTM

3.3 Beschreibung der Aufgabenbereiche

3.3.1 Philipp Adam (PL)

Der Hauptfokus meines technischen Beitrages wird in der Entwicklung der Desktopanwendung liegen. Ich werde die grafische Oberfläche designen, umsetzen und die dahinterstehende Programmlogik implementieren. Weiters werde ich an der Lösungsfindung bezüglich des Problems "Kommunikation PC <--> Android" teilhaben.

Zudem übe ich die Position des Projektleiters aus. Daher wird ein weiterer Schwerpunkt meiner Arbeit in der Planung und Dokumentation des Projektes liegen. Ich werde daher auch als primärer Ansprechpartner für die Betreuer bzw. externe Personen zur Verfügung stehen.

3.3.2 Manuel Caspari (Stv. PL)

In meinem Aufgabenbereich als stellvertretender Projektleiter fallen einerseits Teile der Planung als auch ein Großteil der eigentlichen Programmierung der Software. Ich bin hauptverantwortlich für die Entwicklung der Android-Applikation, sowie der Protokolle. Darunter fällt unter anderem der Schlüsselaustausch mittels Near Field Communication (NFC), das Handshake-Konzept des Schlüsselaustausches, die Erzeugung der Schlüsselpaare, die Ver- und Entschlüsselung der Nachrichten,

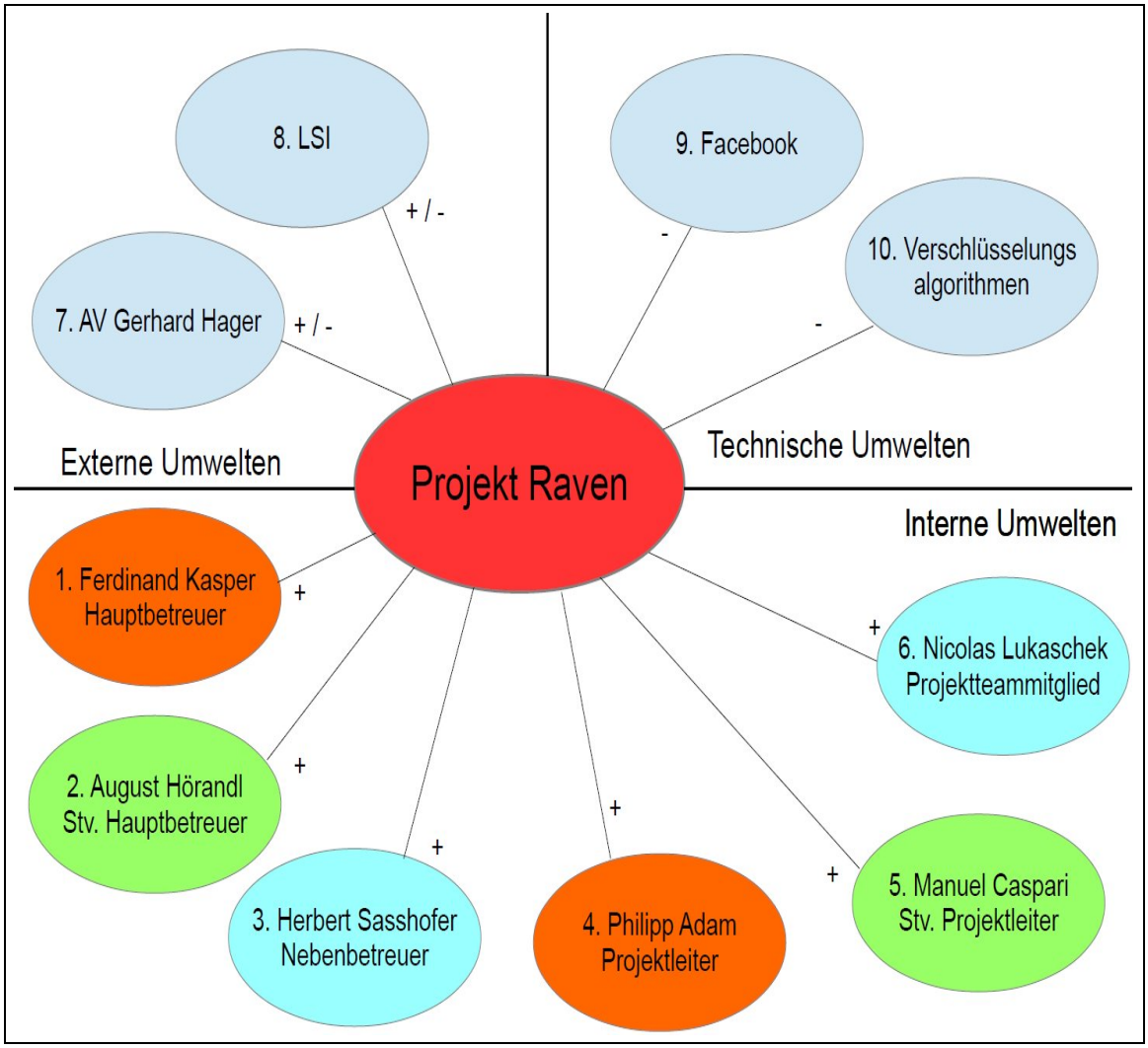
sowie das Schreiben von Schnittstellen für die verschiedenen APIs der Dienste. Zudem kümmere ich mich um die Verwaltung und Instandhaltung des Git-Servers, welcher für das Zusammenfügen (Merging) des Codes verwendet wird.

3.3.3 Nicolas Lukaschek (PM)

Ich, Nicolas Lukaschek, sehe mich in dieser Diplomarbeit als Mitarbeiter, der an beiden Fronten, sowohl dem Programmieren als auch dem Projektmanagement selbst, bestmöglich mithilft. Meine geplante Ressourcenverteilung beläuft sich auf 50 Prozent für jede Seite, wobei bei Bedarf und Notwendigkeit ebenfalls eine kurzzeitige Änderung des Verhältnisses vorgenommen werden kann. Neben diversen Dokumenten im Bereich des Projektmanagements, so z.B. Arbeitspaketdefinitionen und Protokolle, bin ich im Bereich des Programmierens hauptsächlich für das GUI (Deutsch/ Englisch, Anzeigen der entschlüsselten SMS), Benutzerfreundlichkeit und dem Auslesen und Anzeigen der Kontaktdaten verantwortlich.

4 Projektumweltanalyse

4.1 Grafische Darstellung



4.2 Beschreibung der wichtigsten Umwelten

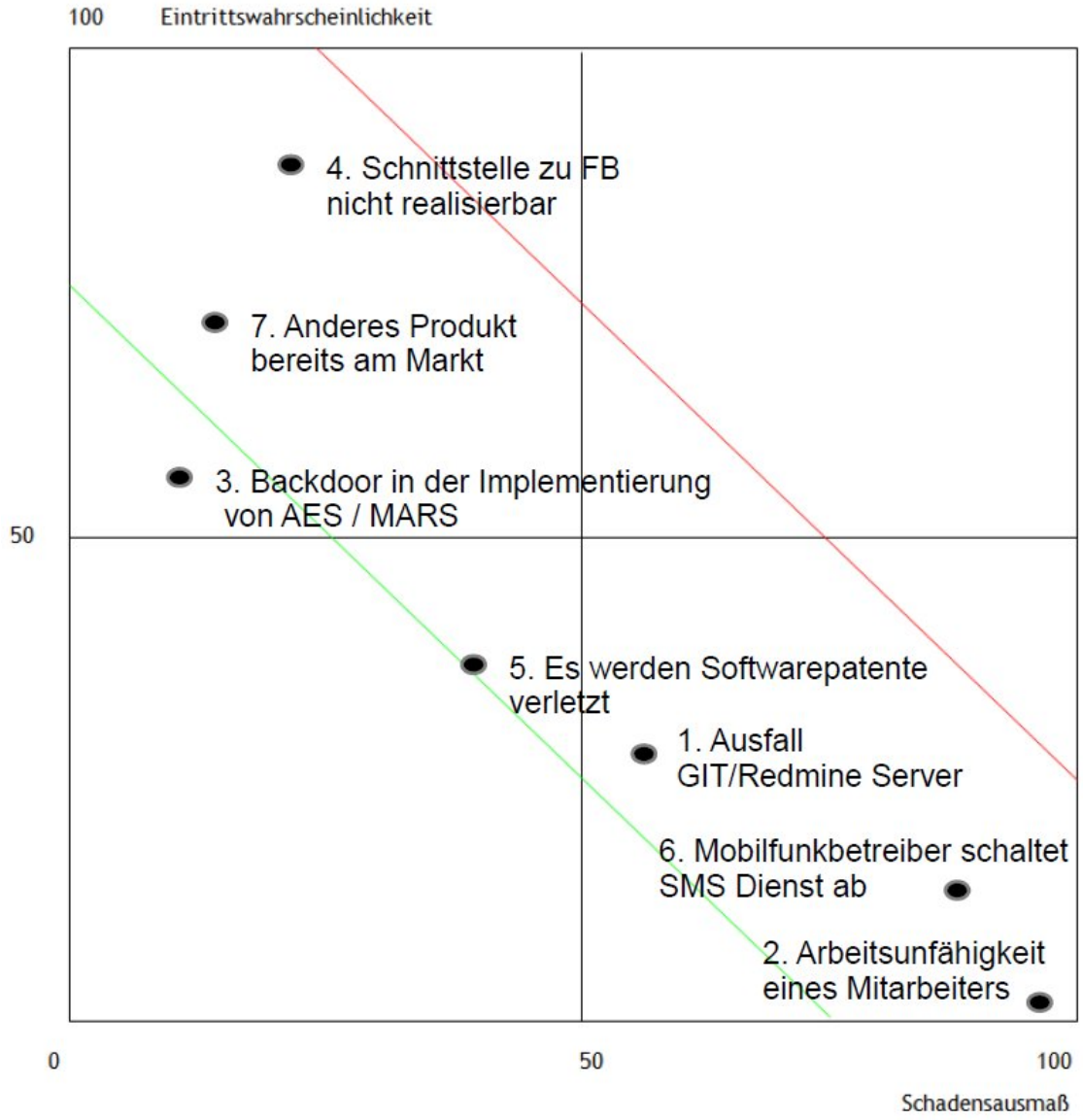
#	Bezeichnung	Beschreibung	Bewertung
9	Facebook	Die Implementation der Kommunikation über Facebook kann sich aufgrund fehlender/eingestellter API's negativ auf das Projekt auswirken	-
10	Verschlüsselungsalgorithmen	Da die genaue Funktionalität der verwendeten Implementationen der Verschlüsselungsalgorithmen nicht nachvollzogen werden kann, ist es möglich, dass eine Backdoor installiert ist.	-
8	LSI	Da die Landesschulinspektorin das Projekt sowohl genehmigen, als auch ablehnen kann, ist sowohl positiver, als auch negaitver Einfluss auf das Projekt möglich	+/-

5 Risikoanalyse

5.1 Beschreibung der wichtigsten Risiken

#	Bezeichnung	Beschreibung des Risikos
1	Ausfall GIT/Redmine Server	Der zur Verfügung gestellte Server für Redmine & GIT fällt aus, alle darauf gespeicherten Daten gehen verloren.
2	Arbeitsunfähigkeit eins Mitarbeiters	Ein Mitarbeiter des Projektteams verunglückt so schwer, dass er nicht mehr in der Lage am Projekt weiterzuarbeiten.
3	Backdoor in der Implementierung von AES / MARS	Es wird publik, dass die NSA ein Backdoor in der Javaimplementierung der verwendeten Verschlüsselungsalgorithmen AES und MARS eingebaut hat. Dadurch wäre der die Verschlüsselung der Nachrichten obsolet
4	Schnittstelle zu FB nicht realisierbar	Es ist technisch nicht möglich, eine Schnittstelle zu Facebook mit vertretbarem Aufwand zu etablieren.
5	Es werden Softwarepatente verletzt	Die technische Umsetzung des Projektes verstößt gegen Softwarepatente Dritter.
6	Mobilfunkbetreiber schaltet SMS Dienst ab	Ein großer österreichischer Mobilfunkbetreiber sieht den SMS Dienst als Verlustgeschäft und obsolet an und schaltet ihn daraufhin ab. Dadurch kann die Anwendung nicht mehr Nachrichten über SMS übertragen
7	Anderes Produkt bereits am Markt	Es exisitiert bereits vor der Veröffentlichung der Software ein Produkt mit gleichen oder weitgehend ähnlichen Funktionalitäten am Markt

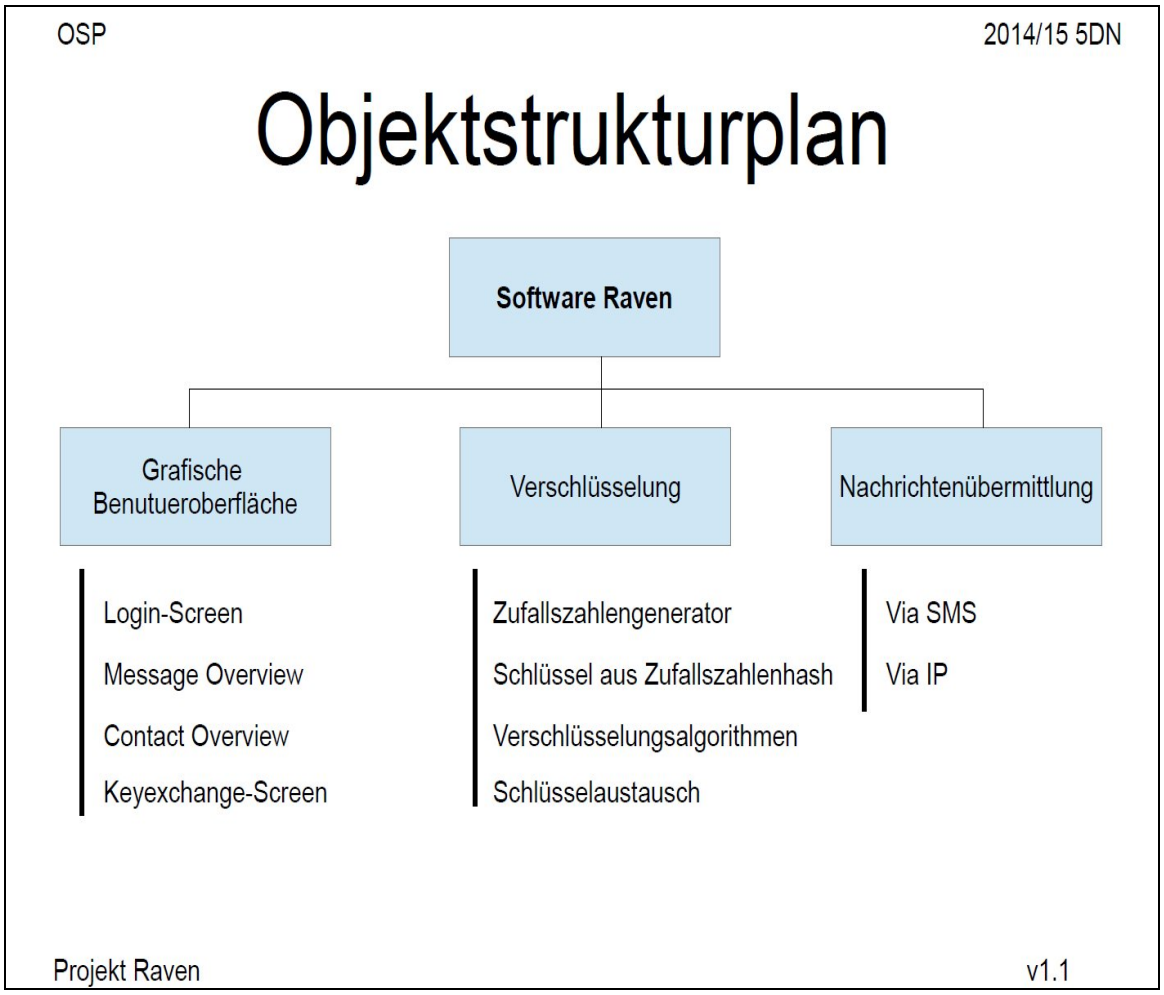
5.2 Risikoportfolio



Risiko Gegenmaßnahmen

#	Bezeichnung	Maßnahmen
1	Ausfall GIT/Redmine Server	Es sollen in regelmäßigen Abständen ein Backup dieser beiden Dienste des Servers erstellt werden.
3	Backdoor in der Implementierung von AES / MARS	Es werden andere Verschlüsselungsalgorithmen eingesetzt
4	Schnittstelle zu Facebook nicht realisierbar	Es wird auf andere Social Networks mit bereits bestehender Java API zurückgegriffen

6 Objektstrukturplan



7 Meilensteinliste

Datum	Meilenstein
22.09.14	Projektplanung abgeschlossen
06.10.14	Konzept zur Implementierung erstellt
08.12.14	Anwendung ist betriebsbereit
26.01.15	Anwendung kann veröffentlicht werden

8 Projektressourcen

8.1 Projektressourcen: Soll – Ist Vergleich

SOLL Bereich	IST	Risiko (X)	PSP (X)
Ausfallfreier Redmine-Server	nicht ausreichend	X	
Eclipse + Andoird SDK	ausrreichend		
Android Gerät	ausreichend		
Experten für Softwareentwickling	ausreichend		

8.2 Personelle Ressourcen

#	Teammitglied	Personenstunden
1	Philipp Adam	200
2	Manuel Caspari	200
3	Nicolas Lukaschek	200
SUMME		600

8.3 Kostenabschätzung

Voraussichtlich fallen keine Kosten an

8.4 Finanzierung

Voraussichtlich fallen keine Kosten an

9 Motivation

9.1 Philipp Adam

Meine Hauptmotivation für dieses Projekt rührt daher, dass mit "Raven" eine Software von großem praktischen Nutzen geschaffen werden soll.
Mit diesem Projekt soll das Chatten und Mailen genauso einfach wie bisher gestaltet werden, allerdings soll der Inhalt der NSA & Co verborgen bleiben. Die Tatsache, dass ich mit meinem Team der breiten Masse eine solche Anwendung zugänglich machen kann, hebt meine Motivation für dieses Projekt ungemein.
Ein weiterer Grund meiner Motivation ist, dass ich mit meinen langjährigen Freunden Manuel Caspari und Nicolas Lukaschek, die ich seit der ersten Klasse kenne, zusammenarbeiten kann. Mir macht es Spaß, die in 5 Jahren erlernten Kenntnisse produktiv einzusetzen und in diese Diplomarbeit einfließen zu lassen.

9.2 Manuel Caspari

Ich war furchtbar entsetzt, als der große NSA-Überwachungsskandal, wonach der gesamte weltweite Internetverkehr überwacht wird, publik wurde. Ich wollte meine Fähigkeiten als Programmierer und Netzwerktechniker dazu einsetzten, meine privaten Nachrichten durch Verschlüsselung auch privat zu halten.
Schnell war die Idee eines verschlüsselten Multi-Messengers geboren, welcher persönliche Nachrichten für Dritte (also die NSA) unlesbar machen sollte. Mit dieser Diplomarbeit möchte ich ein Tool zum Schutz der Privatsphäre kreieren und damit der totalen Internetüberwachung den Kampf ansagen.

9.3 Nicolas Lukaschek

Meine persönliche Motivation für unser Projekt „Raven“ besteht zu einem großen Teil aus dem Interesse, nach jahrelangem Lernen von theoretischen Grundlagen aus den Bereichen Programmierung und Netzwerksicherheit endlich etwas in die Praxis umsetzen und tatsächlich anwenden zu können.
Ich wollte schon immer einen eigenen Messenger für die mobile Plattform Android schreiben. Dieses Projekt bietet mir die Möglichkeit, mich im Rahmen der Diplomarbeit der Programmeirung von Apps ,was im Regelunterricht nicht zur Sprache kam, zu widmen. Ich möchte das bereits erlangte Wissen mit den Erkenntnissen aus dieser Diplomarbeit verbinden und somit meinen Horizont im Bereich der Softwareentwicklung maßgeblich erweitern.