# Yet Another Encrypted Messenger

## Abstract

Florian Amstutz

May 21, 2012

Mit dem zunehmenden Aufkommen von Attacken und gezieltem Abhorchen von Echtzeitkommunikation via E-Mail oder Instant Messaging steigt der Bedarf an eine sichere und einfache Übertragungsart von Nachrichten und Daten.

Als Nutzer eines Kommunikationskanals über das öffentliche Internet will ich die Möglichkeit haben meine privaten Daten verschlüsselt und sicher an einen oder mehrere Empfänger übertragen zu können. Ich will dabei eine einfach zu bedienende Applikation zur Verfügung haben um meine geheimen Daten versenden zu können und so potentiellen Mithörern keine Klartextinformationen zur Verfügung zu stellen.

Diese Applikation soll als Prototyp im Rahmen der Semesterarbeit im dritten Studienjahr an der ZHAW entwickelt werden. Dabei wird der Fokus der Arbeit auf der methodischen Vorgehensweise der Softwareentwicklung gelegt und weniger auf der Implementierung der kryptografischen Algorithmen.

Das Projekt wird zu Beginn mittels des Wasserfallmodells in Phasen unterteilt und in die Phasen

- Anforderungen
- Konzept und Architektur
- Implementierung
- Test

unterteilt.

Alle Anforderungen werden strukturiert als Use-Cases modelliert und stellen die funktionalen Anforderungen an die Applikation dar. Anschliessend wird das Konzept auf Basis der Anforderungen erstellt und die Architektur des Systems entworfen. Auf Grund des Konzepts wird mit der Entwicklung begonnen. Die einzelnen Komponenten werden testgetrieben entwickelt und es werden die dabei verwendeten Technologien vorgestellt. Abschliessend folgt die Testphase, in der auf die Testabdeckung durch automatisierte Unit-Tests eingegangen wird sowie werden Akzeptanztests vorgestellt, welche die Use-Cases der Anforderungen überprüfen.