

Lastenheft

- SecureMessage -



*„Entwicklung einer Software für die verschlüsselte Kommunikation
innerhalb des Unternehmensnetzwerkes“*

Stand: 15.12.2017

Auftraggeber: MoneyGroup AG
Hauptstraße 28
D-20095 Hamburg
Ansprechpartner: Ariane Freithaler, Tel. 040 / 62306-165

Inhaltsverzeichnis

1 Einleitung	1
2 Ausgangssituation (Ist-Zustand)	2
3 Soll-Konzept	2
3.1 Anwendungsbereich	2
3.2 Systemidee (Vision).....	2
3.3 Ziele	2
3.4 Zielgruppen.....	2
4 Projektgegenstand.....	2
4.1 Problemdomäne	3
4.2 Prozesse.....	3
4.3 Produktumgebung	3
4.4 Schnittstellen	3
4.5 Benutzerschnittstelle	3
5 Projektbedingungen.....	3
5.1 Zeitlicher Rahmen	3
5.2 Auftragswert.....	3
5.3 Technische Einschränkungen.....	3
5.4 Projektplan und Projektmanagement	3
5.5 Angebotserstellung	3
6 Anforderungen	3
6.1 Funktionale Anforderungen	4
6.2 Nicht-funktionale Anforderungen	4
7 Lieferumfang.....	4
7.1 Prototyp	4
7.2 Beta-Version	4
7.3 Release	4
7.4 Wiederverwendbare Komponenten/Module/Bibliotheken	4
7.5 Testung	4
7.6 Inbetriebnahme.....	4
7.7 Abnahme	4
7.8 Monitoring	4
7.9 Schulung.....	4
7.10 Support	4
7.11 Wartung	4
7.12 Dokumentation	4
8 Glossar	5

1 Einleitung

Eine kurze Einstimmung zum Projekthintergrund.

Der technische Fortschritt ist unaufhaltsam, damit steigen jedoch auch die Möglichkeiten, dass sensible Daten über IT-Systeme in die falschen Hände geraten. Dieser Gefahr wollen wir Herr werden und die Daten

unserer Kunden schützen. Hierfür benötigen wir unter anderem ein verschlüsseltes Kommunikationstool für unser Unternehmensnetzwerk – Hier sind Sie gefragt!

2 Ausgangssituation (Ist-Zustand)

Überblick über den Ist-Zustand.

Derzeit existiert kein derartiges System mit den geforderten Sicherheitsmaßnahmen.

3 Soll-Konzept

3.1 Anwendungsbereich

Beschreibung der vorgesehenen Anwendungsfälle des zu schaffenden Systems.

Die innerbetriebliche Kommunikation via E-Mail soll durch die Anwendung dieser Verschlüsselungssoftware noch sicherer werden. Die im Klartext vorliegende Nachricht wird mit dem Public-Key im Programm verschlüsselt, dann in eine normale E-Mail kopiert und anschließend an den Empfänger versendet. Dieser kann dann mit dem Privat-Key die Nachricht entschlüsseln.

3.2 Systemidee (Vision)

Welche Idee wird mit dem System umgesetzt?

Eine intuitive und übersichtliche Java-Anwendung mit grafischer Benutzeroberfläche. Das Programm wird mit dem Klartext und dem Public-Key des Empfängers befüllt, danach wird der Text durch Drücken des Encrypt-Buttons verschlüsselt. Der Empfänger kann dann mit seinem Privat-Key auf dieselbe Weise die Nachricht in einen Klartext überführen.

3.3 Ziele

Welche konkreten Ziele sollen erreicht werden? (Aufteilung der Idee/Vision in Teilziele)

Bereitstellung einer sicheren Kommunikation innerhalb des Betriebs. Kundendaten und interne Daten sollen sicher zwischen den Mitarbeitern gesendet werden. Hervorzuheben ist hier noch einmal die übersichtliche Benutzerführung und intuitive Benutzung.

Teilziele	Anforderung
Benutzeroberfläche	Übersichtlich und leicht bedienbar
Back-End	Verschlüsselungsalgorithmus
Plattform	Lauffähig unter Windows und Linux

3.4 Zielgruppen

Benennung der Anforderungsbeitragenden mit Bezug zu deren Anforderungen.

Folgende Beteiligte lassen sich den grob erfassten Anforderungen zuordnen:

Anforderungsbeitragende	Anforderung
Mitarbeiter MoneyGroup AG	Intuitiv und leicht bedienbares Verschlüsselungstool

4 Projektgegenstand

Beschreibung des Projektes aus fachlicher Sicht. Einordnung des Systems in die Prozesse des Auftraggebers. Erklärung fachlicher Termini. Modell der Domäne. Beschreibung der Vorgaben an Soft-, Hard- und Orgware, Architektur, Technologien, Komponenten und Schnittstellen. Vorgaben an die Benutzerschnittstelle.

Einheitliches Erscheinungsbild der Benutzeroberfläche mit Anlehnung an das Corporate Design der MoneyGroup AG. Die Software soll stabil und effizient arbeiten.

4.1 Problemdomäne

Unser Kerngeschäft ist der Finanzsektor, dementsprechend liegen unsere Kompetenzen fern ab der Softwareentwicklung. Nichtsdestotrotz benötigen wir eine verschlüsselte Kommunikation, um mit dem immerwährenden technischen Fortschritt schrittzuhalten. Hier sind Sie gefragt, um den Bereich der Informationssicherheit abzudecken.

4.2 Prozesse

Das Programm soll den Prozess der Nachrichtenübertragung zwischen den Mitarbeitern sicherer gestalten.

4.3 Produktumgebung

Die Verschlüsselungs-Anwendung soll in Java entwickelt werden und auf einer Java-VM ab Version 1.0 lauffähig sein. Es ist eine Umsetzung mit grafischer Oberfläche vorgesehen. Hauptbenutzer sollen unsere Mitarbeiter im Betrieb sein. Der Einsatz erfolgt in all unseren betrieblichen Standorten. Als Betriebssysteme kommen Linux und Windows zum Einsatz. Alle Räume sind klimatisiert und die Rechner haben keine unterbrechungsfreie Stromversorgung.

4.4 Schnittstellen

Schnittstellen zu Produkten oder APIs von Drittanbietern sind nicht vorgesehen. Datenspeicherung soll keine erfolgen.

4.5 Benutzerschnittstelle

Die Benutzerschnittstelle ist als grafische Benutzerschnittstelle vorgesehen. Das Menu soll in der deutschen Sprache gestalten werden. Für eine spätere Erweiterung ist eine Ausgabe in englischer Sprache denkbar.

5 Projektbedingungen

Angabe zeitlicher, monetärer, technischer, planerischer Bedingungen, die für eine seriöse Angebotserstellung wichtig sind.

5.1 Zeitlicher Rahmen

Die Leistung ist bis zum Oktober 2018 zu erbringen.

5.2 Auftragswert

Der Nettoauftragswert beträgt aufgrund der beschränkten Ausschreibung maximal 60.000 €.

5.3 Technische Einschränkungen

Das System soll auf Linux und Windows lauffähig sein. Der Public- und Private-Key soll aus mindestens 15 Zeichen (Groß-, Kleinbuchstaben, Sonderzeichen) bestehen. Die Größe des Textfeldes soll mindestens 10.000 Zeichen fassen.

5.4 Projektplan und Projektmanagement

Das Vorgehensmodell zur Softwareentwicklung soll mit dem Auftraggeber vereinbart werden. Es ist ein Projektplan mit Meilensteinen zu erstellen und mit dem Auftraggeber abzustimmen.

5.5 Angebotserstellung

Zur Prüfung der Angemessenheit der Preise ist mit dem Angebot die Kalkulation mit Auflistung der Bestandteile der Gesamtsumme einzureichen.

6 Anforderungen

Hier sind die Anforderungen in einer einheitlichen und übersichtlichen Form darzustellen. Als Template eignet sich z. B. eine Tabelle. Eine Gruppierung nach Prozessen, Nutzerrollen oder fachlichen Bereichen und das Vergeben eines Identifikators, sowie Verweise auf verwandte Anforderungen ist ratsam.

6.1 Funktionale Anforderungen

Es gibt nur drei Anforderungen: die Verschlüsselungsfunktion und eine Entschlüsselungsfunktion. Weiterhin noch einen Kopierbutton für das bequeme Kopieren des gesamten Textes im Textfeld.

Der am Betriebssystem angemeldete Nutzer führt das Programm aus. Der Aufruf erfolgt durch Doppelklick des Icons auf dem Desktop.

F1	Verschlüsselung	Der Klartext im Textfeld wird verschlüsselt und ersetzt
F2	Entschlüsselung	Die Verschlüsselte Nachricht wird entschlüsselt und ersetzt
F3	Kopier-Button	Der gesamte Inhalt im Textfeld wird in die Zwischenablage kopiert

6.2 Nicht-funktionale Anforderungen

NF1	Look and feel: UI	Das Programm soll eine angemessene Benutzeroberfläche haben und im Sinne unseres Corporate Designs gestaltet werden.
NF2	Look and feel: Antwortzeit	Die Ausgabe der Texte soll unmittelbar erfolgen.
NF3	Sicherheit	Die höchstmögliche Sicherheit in Verbindung mit dem angemessensten Preises
NF4	Normen	Die Anwendung braucht keine besonderen Normen zu erfüllen.

7 Lieferumfang

Genaue Beschreibung des vom AG geforderten Lieferumfangs. Mögliche Punkte sind dabei:

7.1 Prototyp

7.2 Beta-Version

7.3 Release

Für das Release ist vorgesehen, das Programm zusammen mit den nötigen Unterlagen vorzulegen.

7.4 Wiederverwendbare Komponenten/Module/Bibliotheken

7.5 Testung

Das Verschlüsselungstool soll ausreichend durch die beauftragte Firma getestet werden und auf etwaige Schwachstellen geprüft werden.

7.6 Inbetriebnahme

7.7 Abnahme

7.8 Monitoring

7.9 Schulung

Ein individueller Support soll nicht erfolgen. Eine eintägige Schulung unserer Mitarbeiter gilt als völlig ausreichend.

7.10 Support

7.11 Wartung

7.12 Dokumentation

Eine textuelle Anwenderdokumentation und eine Entwicklerdokumentation sind zu erstellen. Die Erstellung einer Administratordokumentation ist unter technischen Aspekten abzuwägen. Eine kurze Bedienungsanleitung ist zu erstellen.

8 Glossar

Erklärung unbekannter oder unscharfer Begriffe der Domäne des Auftraggebers. Das nachstehende exemplarische Glossar ist ausführlicher zu fassen.

<i>UI:</i>	<i>User Interface</i>
<i>Private-Key:</i>	<i>Privater Schlüssel</i>
<i>Public-Key:</i>	<i>Öffentlicher Schlüssel</i>
<i>Encrypt:</i>	<i>Verschlüsseln</i>
<i>Decrypt:</i>	<i>Entschlüsseln</i>
<i>Back-End:</i>	<i>Unterbau im Sinne von Anwendungen</i>