Team Pretzels

Pflichtenheft Lauffeuer

Version 1.0

Vitali Kaiser, Philipp Serrer, Huyen Chau Nguyen und Tobias Sturm
01.12.2011

Inhaltsverzeichnis

Pflichtenheft

Zielbestimmungen

Katastrophen können überall auf der Welt auftreten. Dabei brechen oft viele Systeme wie z.B. die Kommunikationsnetze zusammen wodurch in Not geratene Menschen nicht in Kontakt mit anderen treten können.

Personen, die von Freunden und Angehörigen getrennt wurden, sind um das Wohlergehen dieser besorgt und wissen nicht, wie sie diese erreichen können.

An diesem Punkt setzt die Anwendung „Lauffeuer" ein, sie soll Benutzer in die Lage versetzen, in Krisensituationen ein kurzes Lebenszeichen an Bekannte zu senden oder Personen in der Umgebung über Sachverhalte zu informieren. Krisensituation sind z.B. Umweltkatastrophen, Kriege oder politische Unruhen.

Die Nachrichten sollen dabei unter den in der Nähe befindlichen Benutzern ausgetauscht werden. Wenn diese zu einem späteren Zeitpunkt weitere Benutzer treffen, reichen sie die eigenen und erhaltenen Nachrichten an diese weiter. Dadurch können sich die Nachrichten im Netz ausbreiten und die Benutzer auf indirektem Weg Nachrichten austauschen. Sobald ein Benutzer wieder Zugang zum Internet hat, z.B. durch Verlassen des Krisengebiets, können auch die Nachrichten zugestellt werden, die an Personen außerhalb des Krisengebiets adressiert sind.

Das Projekt wird im Rahmen des Praxis der Softwareentwicklung erstellt und darüber hinaus wird das Projekt beim *Microsoft Imagine Cup* eingereicht.

Musskriterien

Es sollen kurze Nachrichten zwischen zwei Benutzern zugestellt werden können, ohne dass eine herkömmliche Netzwerkinfrastruktur flächendeckend zur Verfügung steht.

Jeder Benutzer benötigt dafür ein Gerät (Im Folgenden auch Smartphone genannt), auf dem diese Software installiert ist. Die Anwendung muss vor Beginn der Krise installiert und eingerichtet worden sein.

Nachrichten werden dabei von Gerät zu Gerät via Bluetooth weitergereicht (kurz: P2P), bis der Empfänger einer Nachricht erreicht wurde. Für sogenannte private Nachrichten soll stets eine „Ende-zu-Ende" Verschlüsselung zwischen Sender und Empfänger solcher Nachrichten umgesetzt werden um die Privatsphäre der Benutzer zu gewährleisten. Diese privaten Nachrichten können nur vom Empfänger entschlüsselt und gelesen werden.

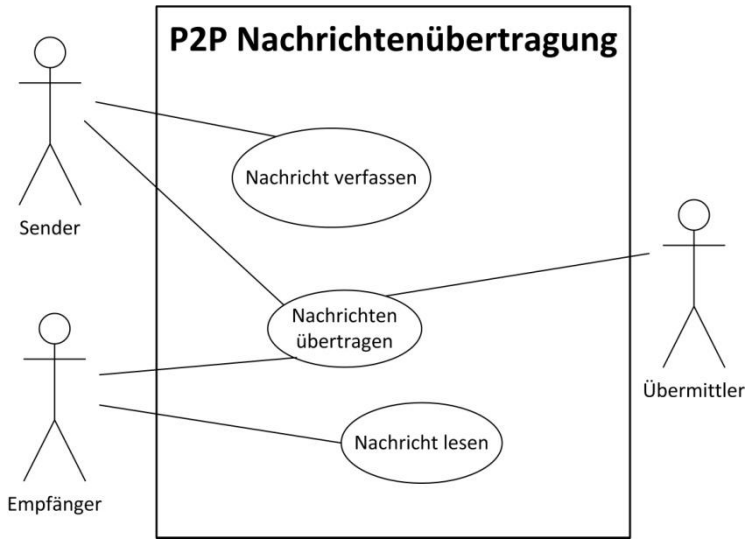

Abbildung 1 - Anwendungsfall "P2P Nachrichtenübertragung"

Neben privaten Nachrichten soll Benutzer in der Lage sein, öffentliche Nachrichten verfassen zu können - welche die von allen Benutzern gelesen werden können. Das kann vor allem dann hilfreich sein, wenn andere Personen vor Gefahren gewarnt werden sollen.

Zusätzlich zu dieser Übertragungsform, soll es möglich sein, mit Hilfe eines zentralen Servers Nachrichten via E-Mail weiter zu leiten. Ein Benutzer kann eine Nachricht an den Server adressieren. Die Nachricht wird wie oben beschrieben via P2P weitergereicht, bis ein Benutzer über eine Internetverbindung verfügt. Die Nachricht wird an den Server übertragen, der sie dann an die in der Nachricht selbst angegebenen E-Mail Adressen weiterleitet.

Über das Eintreffen privater Nachrichten wird der Absender informiert.

Die Benutzeroberfläche wird in Englischer Sprache umgesetzt.

Wunschkriterien

Die Anwendung soll nach Möglichkeit neben Bluetooth auch alle anderen Ad-hoc Bordmittel, insbesondere NFC und WLAN des *Smartphone* nutzen können um die Nachrichten von einem Gerät zum Nächsten zu übertragen.

Obwohl die Benutzeroberfläche auf Englisch umgesetzt wird, soll darauf geachtet werden, dass zu einem späteren Zeitpunkt mit möglichst wenig Aufwand weitere Sprachen hinzugefügt werden können.

Zu Entwicklungs- und Optimierungszwecken soll das System mit vielen Akteuren simuliert werden können. Der dafür benötigte Simulator wird im Rahmen des *Microsoft Imagine Cup* entwickelt und ist nicht Teil dieses Pflichtenhefts.

Der Benutzer soll vor dem Eintreten einer Katastrophe die Möglichkeit haben, auf dem Server Informationen zu hinterlegen, die im Krisenfall an den *Google Person Finder* (Im folgenden GPF genannt) übertragen werden können. Somit sollen Nachrichten außerhalb des Katastrophengebietes möglichst vielfältig propagiert werden können.

Neben Textnachrichten sollen auch kleine Multimediadaten wie z.B. Bilder unterstützt werden. Außerdem soll es eine alternative Übertragung Möglichkeit über Display und Kamera geschaffen werden.

Empfängern von E-Mailnachrichten (über den Server weitergeleitete Nachrichten, s.o.) soll die Möglichkeit gegeben werden Nachrichten von bestimmten Benutzern zu ignorieren. Nachrichten solcher Benutzer sollen dann vom Server nicht mehr an den entsprechenden Empfänger zugestellt werden. Zusätzlich hat jeder E-Mail Empfänger die Möglichkeit seine E-Mail Adresse grundsätzlich vom System auszuschließen („E-Mail auf Blacklist setzen").

Das Prinzip, der dezentralen Nachrichtenübermittlung lässt sich neben Katastrophen-Nachrichtenvermittlung auch auf andere Gebiete ausweiten. Es könnte z.B. verwendet werden um vermisste Kinder oder entführte Personen in Städten wieder zu finden. Dieses Produkt soll so gestaltet werden, dass große Teile für andere Anwendungen, wie z.B. die gerade beschriebene, verwend

Abgrenzungskriterien

- Kein soziales Netzwerk
- Kein Ersatz von Chat-Protokollen/-Software/E-Mail
- Keine garantierte Zustellungssicherheit
- Keine großen Datenmengen innerhalb einer Nachricht
- Keine zeitkritischen Nachrichten
- Keine zentrale Kontrolle des Nachrichtenaustauschs
- Kein Ersatz für Notruf

Produkteinsatz

Das Produkt dient zur Übermittlung kurzer, wichtiger Nachrichten in einer Krisensituation ohne direkte Internetverbindung.

Anwendungsbereich

Das Produkt soll in Krisengebieten, in denen normale (z.B. Mobilfunk, WLAN, etc.) nicht mehr gegeben ist, eingesetzt werden, um über mobile Geräte ein dezentrales, nicht beständiges Netzwerk aufzubauen. Die Geräte stellen Netzwerkknoten dar, die für kurze Zeit verbunden sind um Daten, sogenannte Pakete bzw. Nachrichten auszutauschen und auszuwerten. („Pakete synchronisieren").

Zielgruppe

Das Produkt soll unabhängig von Region und Infrastruktur auf *Smartphones* zur Verfügung stehen und so bedienbar sein, dass jeder damit umgehen und es verwenden kann. Vor allem Menschen, die in einer Krisensituation von Bekannten getrennt werden, sollen mit Hilfe des Produktes in Kontakt treten können. Auch die Verbreitung von öffentlichen Informationen im Krisengebiet ist ein wichtiger Aspekt. Zum Beispiel können ethnische oder politisch unterdrückte Minderheiten das System verwenden um sicher Nachrichten auszutauschen oder ins Ausland zu versenden.

Betriebsbedingungen

Um das Produkt zu benutzen müssen folgende Voraussetzungen erfüllt sein:

- Speicherplatz für die Anwendung und die hinterlegten Kontaktinformation (Größenordnung etwa 5-20 MB).
- Speicherplatz für fremde und eigene Pakete während der Krisensituation (Größenordnung 20-100 MB).
- Die übertragenden Geräte müssen angeschaltet sein und über genügend Stromreserven verfügen.
- Geräte müssen sich für den Datenaustausch zu einem Ad-hoc Netzwerk verbinden lassen.
- Um eine Paketsynchronisation durchführen zu können, müssen sich die beiden beteiligten Geräte in gegenseitiger Empfangsreichweite befinden.
- Es gibt pro Benutzer nur ein Gerät
- Anwendung muss installiert und eingerichtet sein

Produktfunktionen

Grundfunktionen

Übersicht:

- /F010/ **Installation**
- /F020/ **Startbildschirm**
- /F030/ **Personen sperren**
- /F040/ **Kontakte synchronisieren**
- /F070/ **Nachrichtenübersicht**
- /F080/ **Neue Nachricht verfassen**
- /F090/ **Pakete manuell übertragen**
- /F100/ **Pakete automatisiert übertragen**
- /F110/ **Übertragung im Standby-Modus**
- /F120/ **Nachricht empfangen**
- /F130/ **Server leitet Nachricht eines Benutzers via E-Mail weiter**
- /F140/ **Nachricht lesen**
- /F150/ **Benutzer-Einstellungen**
- /F160/ **E-Mail Adresse auf Blacklist setzen**
- /F170/ **Empfangsbestätigung anzeigen**
- /F180/ **Profil auf Server bearbeiten**
- /F190/ **Tutorial anzeigen**

/F010/ **Installation**

Ziel: Gerät für Krisensituationen vorbereiten

Beteiligte: Ein Gerät, Server, Benutzer

Auslösendes Ereignis: Anwendungssetup wird gestartet

Beschreibung: Die Anwendung initialisiert alle notwendigen Daten und der Benutzer legt ein Profil(siehe /D310/ und Glossar) auf Server an. Anschließend wird ein kurzes Tutorial (/F190/) angezeigt.

/F020/ **Startbildschirm**

Ziel: Überblick über aktuellen Status, Nachrichten und verfügbare Funktionen

Beteiligte: Ein Gerät, Benutzer

Auslösendes Ereignis: Starten des Programms

Beschreibung: Der Benutzer bekommt eine Übersicht zum aktuellen Übertragungsmodus und kann zu verschiedenen Funktionen navigieren. Zur Auswahl stehen /F030/ „Personen sperren", /F080/ „Neue Nachricht verfassen", /F090/ „Pakete manuell synchronisieren", /F070/ „Nachrichtenübersicht", /F150/ „Benutzer-Einstellungen", /F190/ „Tutorial anzeigen".

/F030/ **Personen sperren**

Ziel: Verwalten der Personen, mit denen der Benutzer in Kontakt treten möchte

Beteiligte: Ein Gerät, Benutzer

Auslösendes Ereignis: Auswahl der Funktion „Personen sperren"

Beschreibung: Dem Benutzer werden alle Personen aus dem Telefonbuch des *Smartphones* angezeigt. Der Benutzer kann einzelne Personen sperren, das bedeutet, es werden für diese Person keine Kontaktinformationen (/D210/) auf dem Gerät gespeichert. Der Benutzer ist dann nicht mehr in der Lage Nachrichten direkt an diese Person zu senden. Dies ist dann von Vorteil, wenn sich Einträge im Telefonbuch des Benutzers befinden, mit denen er speziell im

Krisenfall nicht kommunizieren möchte (z.B. Arbeitskollegen, Pizzalieferservice, …). Der Benutzer kann jederzeit Personen aus seinem Telefonbuch entsperren.

In der Ansicht wird graphisch zwischen reinen Personen und Benutzern unterschieden. Zusätzlich soll deutlich sein, welche Personen bereits als Kontakt gesperrt wurden und welche nicht. Sperrt/entsperrt der Benutzer Kontakte, wird anschließend /F040/ ausgeführt.

/F040/ **Kontakte synchronisieren**

Ziel: Aktualisierung aller Informationen die nötig sind um mit ausgewählten Personen in Kontakt treten zu können

Beteiligte: Ein Gerät, Server

Auslösendes Ereignis: Änderung des Telefonbuches des Smartphones, (Ent-)Sperren einer Person (/F030/)

Beschreibung: Wurde ein Telefonbucheintrag bearbeitet, bei dem es sich um einen Kontakt handelt, wird der Server angefragt, ob es sich bei diesem veränderten Eintrag immer noch um einen Benutzer handelt. Ist das der Fall, werden alle Kontaktinformationen dieses Benutzers neu auf das Gerät kopiert. Ebenso wird verfahren, wenn eine Person entsperrt wurde (/F030/).

Wurde eine Person aus dem Telefonbuch entfernt, werden die dazugehörigen Kontaktinformationen aus der Anwendung entfernt.

/F050/ **Nachrichtenübersicht**

Ziel: Verwalten von Nachrichten eines Benutzers

Beteiligte: Ein Gerät, Benutzer

Auslösendes Ereignis: Auswahl der Funktion „Nachrichtenübersicht"

Beschreibung: Alle Nachrichten die direkt (privat) oder indirekt (öffentlich) an den Benutzer adressiert waren, werden chronologisch und aufgelistet. Man kann diese zum Lesen aufrufen oder löschen. Darüber hinaus werden auch alle Nachrichten, die versendet wurden aufgelistet. Versendete Nachrichten, für die eine Empfangsbestätigung eingetroffen ist, werden farblich hervorgehoben. Der Benutzer kann einsehen, wann eine Empfangsbestätigung erzeugt wurde und ob sie vom Server (/F110/) oder vom Empfänger der Nachricht (/F070/ - /F090/) erstellt wurde.

/F060/ **Neue Nachricht verfassen**

Ziel: Übertragung einer Nachricht

Beteiligte: Ein Gerät, Benutzer

Auslösendes Ereignis: Auswahl der Funktion „Nachricht verfassen“

Beschreibung: Der Benutzer hat die Wahl ob die Nachricht privat oder öffentlich sein soll. Private Nachrichten werden verschlüsselt, öffentliche nicht. Bei privaten Nachrichten werden anschließend die Empfänger ausgewählt wo standardmäßig der örtliche Katastrophenschutz eingetragen ist. Zusätzlich gibt es ein Feld, in dem man den Inhalt der Nachricht eingeben kann. Falls möglich wird im Hintergrund die aktuelle Position des Gerätes ermittelt und angezeigt. Der Benutzer hat die Möglichkeit die Position nicht mit der Nachricht zu versenden.

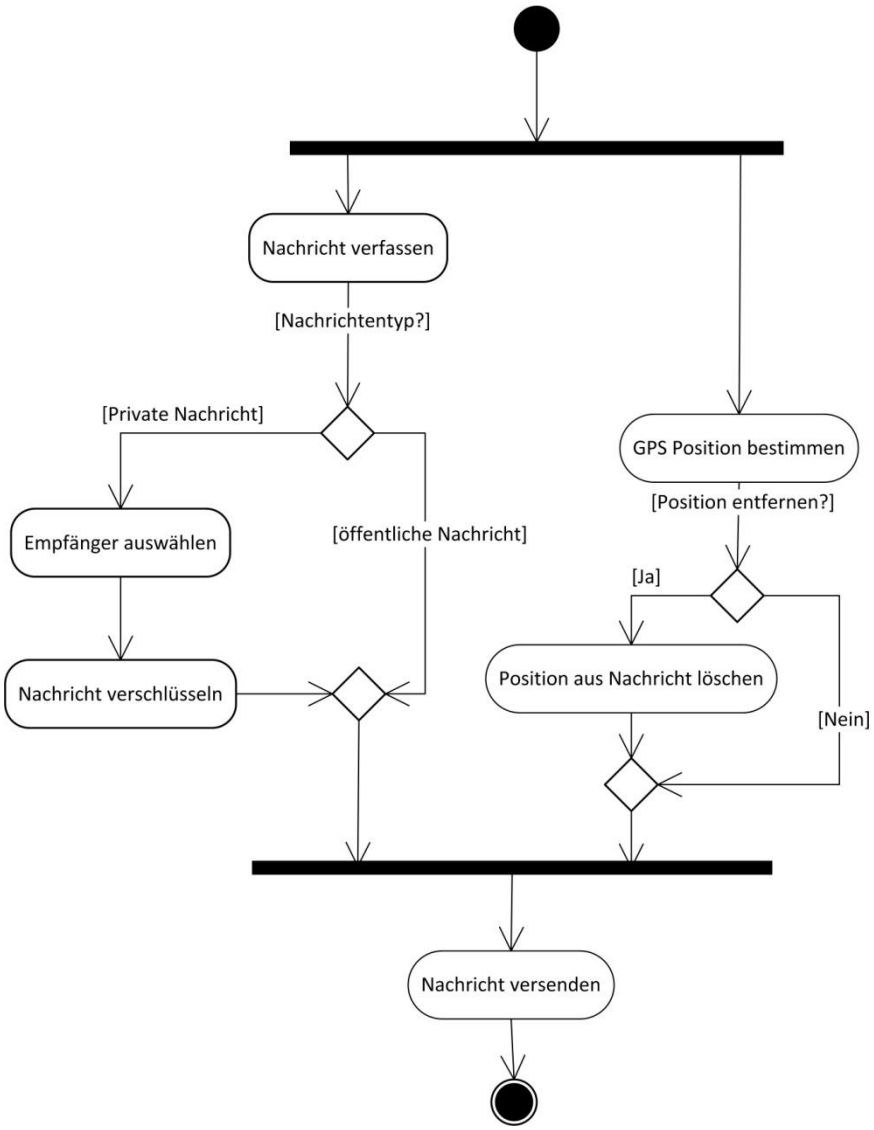

Abbildung 2 - Produktfunktion "Neue Nachricht verfassen"

/F070/ **Pakete manuell übertragen**

Ziel: Paketsynchronisation zwischen 2 Geräten

Beteiligte: zwei Geräte, ein oder mehrere Benutzer

Auslösendes Ereignis: Auswahl im Startmenü

Beschreibung: Beim Starten sucht das Gerät nach erreichbaren Geräten in der Umgebung, die zur Übertragung bereit sind und schlägt diese dem Benutzer für Übertragungen vor. Während des gesamten Vorgangs ist das suchende Gerät selbst für andere sichtbar und übertragungsbereit. Zusätzlich kann der Benutzer den Übertragungsweg manuell wählen.

Bei der Synchronisation empfangen beide Geräte die jeweils noch unbekannten Nachrichten vom anderen Gerät und verarbeiten sie (siehe /F100/).

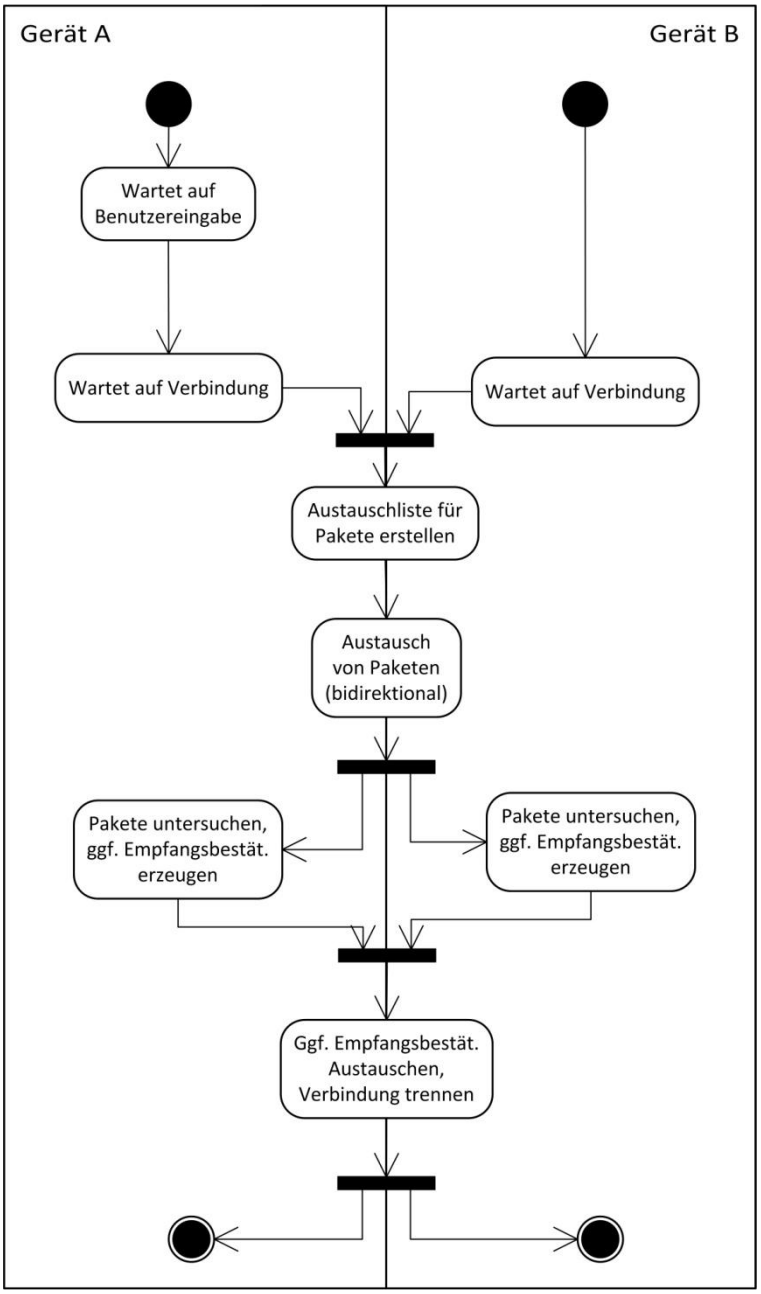

Abbildung 3- Produktfunktion "Pakete manuell übertragen"

/F080/ **Pakete automatisiert übertragen**

Ziel: Paketsynchronisation zwischen 2 Geräten

Beteiligte: zwei Geräte

Auslösendes Ereignis: Automatische Übertragung im Status „on” und ein neues Gerät in der Umgebung.

Beschreibung: Nach dem Ereignis wird geprüft ob das neue Gerät bereit für eine Übertragung ist und synchronisiert falls möglich die Pakete analog zu /F030/. Das Gerät sucht danach nach neuen Geräten.

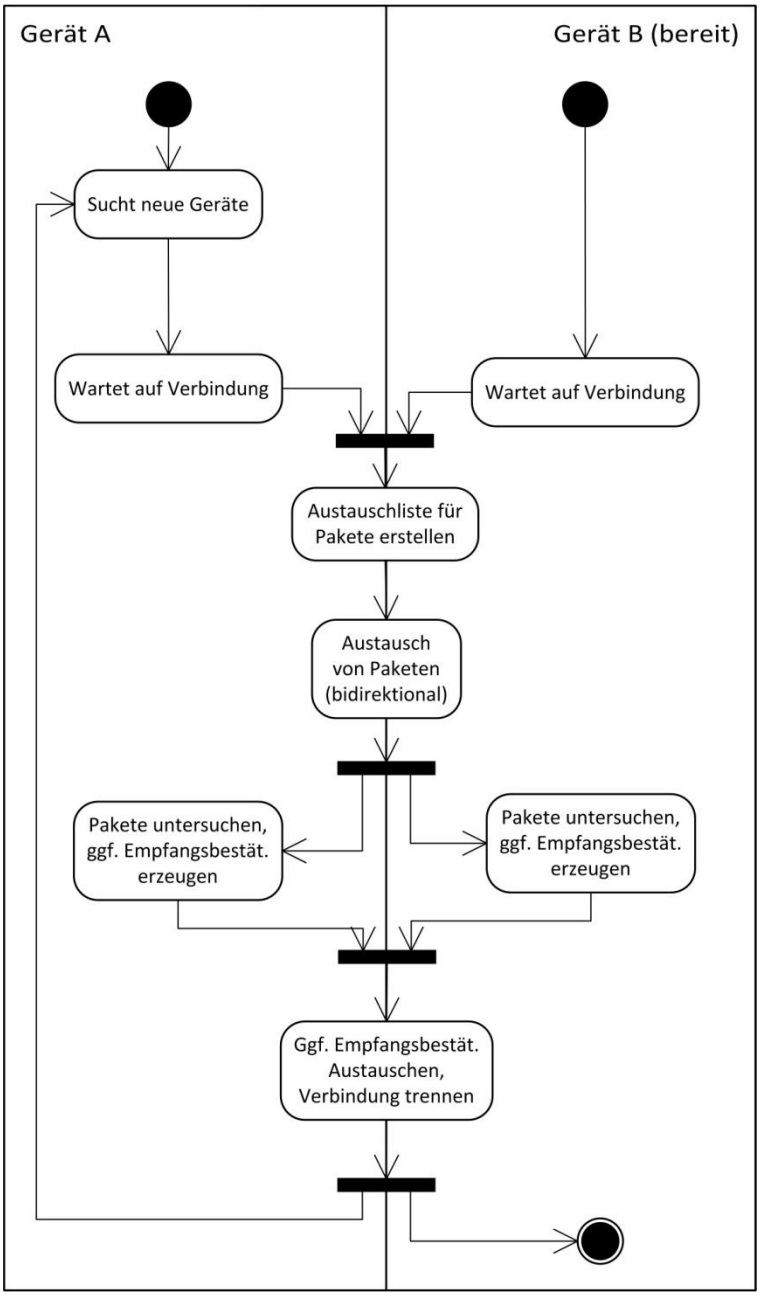

Abbildung 4 - Produktfunktion "Pakete automatisiert übertragen"

/F090/ **Übertragung im Standby-Modus**

Ziel: Benutzer zur Synchronisation animieren.

Beteiligte: zwei Geräte, ein oder mehrere Benutzer

Auslösendes Ereignis: Übertragungsmodus „standby" und ein neues Gerät in der Umgebung das zur Paketsynchronisation bereit ist.

Beschreibung: Der Benutzer wird optisch und akustisch darauf hingewiesen das ein anderes Gerät zur Paketsynchronisation bereit ist. Der Nutzer wird aufgefordert die Paketsynchronisation zu starten (/F070) in den automatischen Modus zu wechseln (/F080/) oder keine Synchronisation durchzuführen.

/F120/ **Nachricht empfangen**

Ziel: Nachricht entschlüsseln

Beteiligte: ein Gerät

Auslösendes Ereignis: Empfang von Paketen

Beschreibung: Prüfen ob eine der Pakete an den Benutzer direkt bzw. indirekt adressiert ist, diese gegebenenfalls entschlüsseln und den Benutzer mittels optischer und akustischer Signale auf die neue Nachricht hinweisen. Zusätzlich wird die Nachricht in der Liste der empfangenen Nachrichten gespeichert. Für jede empfangene, persönliche Nachricht wird automatisch eine Empfangsbestätigung generiert.

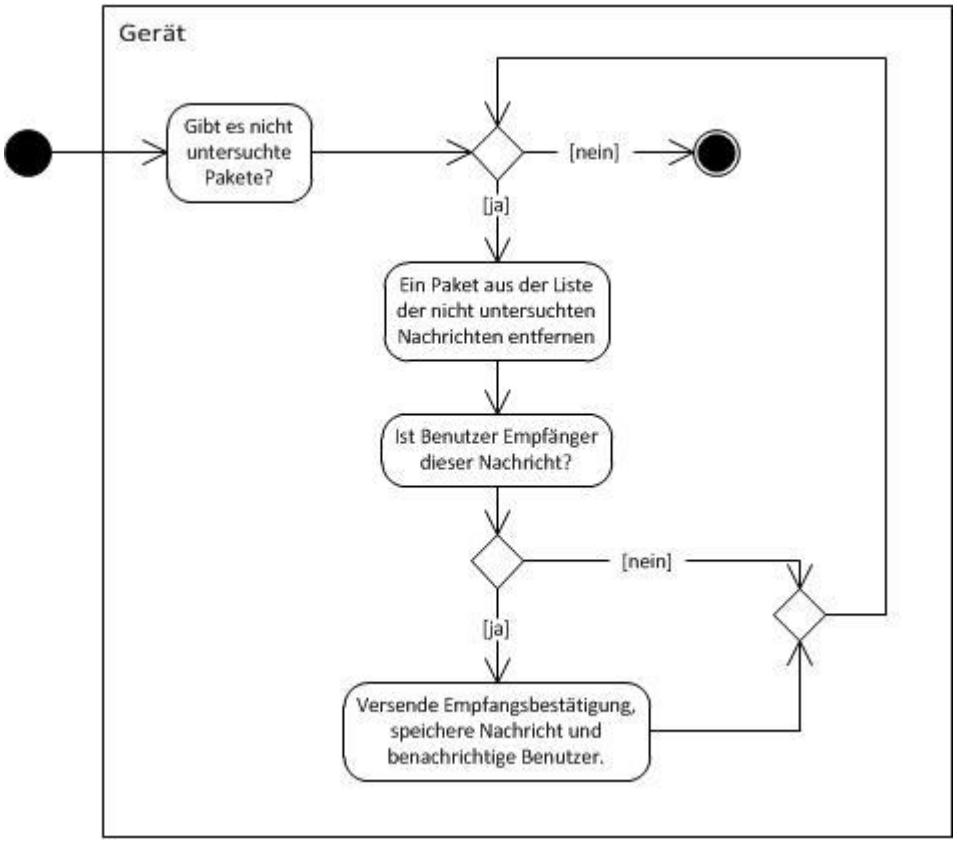

Abbildung 5 - Produktfunktion "Nachricht empfangen"

/F110/ **Paketaustausch zwischen Server und Benutzer**

Ziel: Übertragung von Paketen, die an den Server adressiert sind, zum Server

Beteiligte: ein Gerät, Server

Auslösendes Ereignis: Benutzer erhält Internetzugriff

Beschreibung: Erhält ein Gerät Internetzugriff, so sendet es automatisch alle Pakete von öffentlichen Nachrichten und alle an den Server adressierten Pakete dem Server.

Der Server generiert für diese Pakete Empfangsbestätigungen, die an den Benutzer zurückgegeben werden und die Verbindung wird getrennt.

Der Server kann nun die empfangenen Pakete abarbeiten und Nachrichten via E-Mail an die eigentlichen Empfänger verschicken.

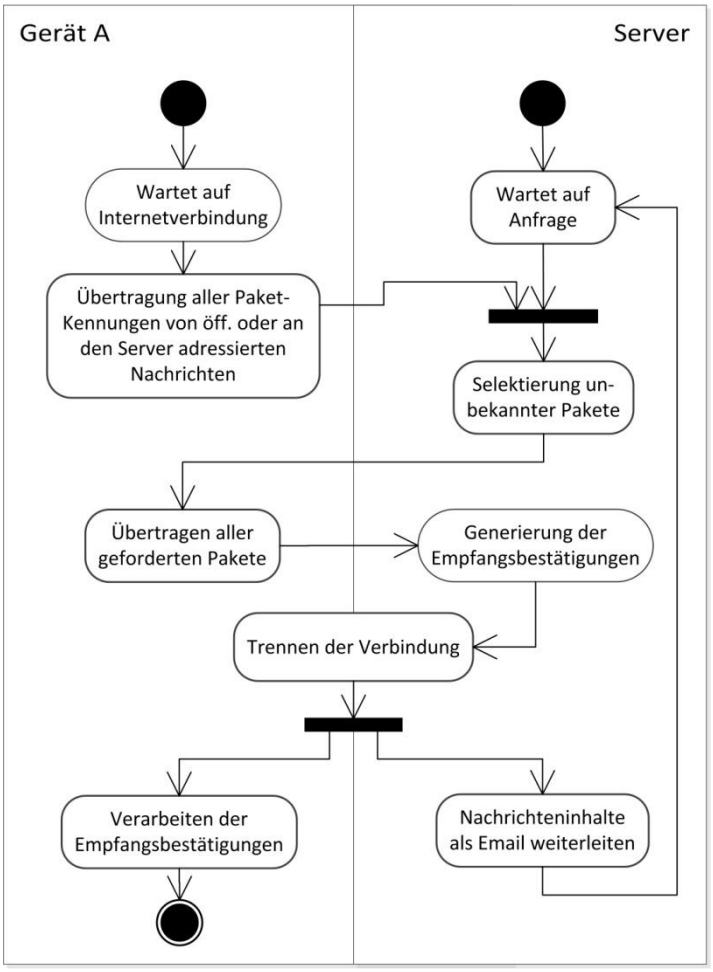

Abbildung 6 - Produktfunktion "Paketaustausch zwischen Server und Benutzer"

/F120/ **Nachricht lesen**

Ziel: Nachricht lesen

Beteiligte: ein Gerät, Benutzer

Auslösendes Ereignis: Auswahl der Funktion „Nachricht lesen“ / Auswahl einer Nachricht aus Nachrichtenübersicht (/F050/)

Beschreibung: Ausgewählte Nachricht wird dem Benutzer angezeigt. Dabei auch Details wie z.B. Absendezeitpunkt, Empfangszeitpunkt, Sendeposition. Handelt es sich um eine selbst versendete Nachricht, wird angezeigt, ob bereits eine Empfangsbestätigung eingetroffen ist, oder nicht.

/F130/ **Benutzer-Einstellungen**

Ziel: Verhalten der Anwendung anpassen

Beteiligte: ein Gerät, Benutzer

Auslösendes Ereignis: Auswahl der Funktion „Benutzer-Einstellungen“

Beschreibung: Der Modus der Synchronisation kann auf „automatisch”, „standby” oder „manuell” gestellt werden, wobei „automatisch” /F080/ entspricht, „standby” /F090/ und „off” das die Synchronisation pausiert wird. Der Benutzer kann sein Profil bearbeiten (/F160/). Außerdem gibt es die Möglichkeiten die Systemressourcen zu limitieren und Grenzen zu setzen (siehe /D010/).

/F140/ **E-Mail Adresse auf Blacklist setzen**

Ziel: E-Mail Adresse im Server komplett sperren / Spamschutz vor einzelnen Benutzern

Beteiligte: Server, eine Person

Auslösendes Ereignis: Person möchte keine E-Mails mehr vom Server/Benutzer erhalten

Beschreibung: Unter jeder E-Mail, die vom Server versendet wird, befindet sich ein Link, mit dem der E-Mail-Empfänger sich selbst auf die Blacklist setzen kann um in Zukunft keine weiteren E-Mails mehr zu erhalten (siehe /D120/).

/F150/ **Empfangsbestätigung anzeigen**

Ziel: Benutzer wird informiert dass eine versendete Nachricht zugestellt wurde

Beteiligte: ein Gerät, Benutzer

Auslösendes Ereignis: Empfang von Paketen

Beschreibung: Wenn unter den empfangen Paketen eine Empfangsbestätigung ist soll der Benutzer darauf hingewiesen werden, welche seiner versendeten Nachricht ihren Empfänger erreicht hat.

/F160/ **Profil auf Server bearbeiten**

Ziel: Benutzer ändert Profilinformationen die auf dem Server gespeichert sind

Beteiligte: ein Gerät, Benutzer, Server

Auslösendes Ereignis: Auswahl in den Benutzer-Einstellungen (/F130/)

Beschreibung: Der Benutzer hat die Möglichkeit seine persönlichen Daten zu verändern, die auf dem Server hinterlegt sind. Diese Daten (/D310/) sind öffentlich und können daher von anderen Kontakten kopiert werden. Daher hat der Benutzer die Möglichkeit alle Daten unwiderruflich vom Server zu löschen.

/F170/ **Tutorial anzeigen**

Ziel: Benutzer über optimalen Umgang mit System unterrichten

Beteiligte: ein Gerät, Benutzer

Auslösendes Ereignis: Auswahl der Funktion „Tutorial anzeigen”

Beschreibung: Es wird ein Tutorial mit erklärenden Bildern und Texten angezeigt, um den Benutzer über den optimalen Gebrauch der Anwendung zu unterrichten. Dabei werden alle Funktionen kurz erläutert.

Funktionen zu Wunschkriterien

/F210/ **Anlegen, löschen und bearbeiten eines GPF-Templates**

Ziel: Benutzer soll Informationen bereitstellen um sie im Katastrophenfall auf den GPF zu übertragen.
Beteiligte: ein Gerät, Benutzer, Server
Auslösendes Ereignis: Benutzer entschließt sich ein GPF-Template zu erstellen
Beschreibung: Der Benutzer hat die Möglichkeit umfangreiche Daten zu seiner Person auf dem Server zu hinterlegen (/D330/). Das Anlegen und Bearbeiten erfolgt durch die Eingabe über die Anwendung. In dieser Eingabe soll dem Benutzer auch die Möglichkeit zum Löschen bereitgestellt werden.

/F220/ **Verwendung eines GPF-Templates**

Ziel: Benutzer soll mit dem Versenden einer Nachricht an den Server sein GPF-Template einsetzen können.
Beteiligte: Benutzer, Gerät(e), Server
Auslösendes Ereignis: Versenden einer GPF-Nachricht
Beschreibung: Benutzer versendet eine Nachricht an den Server (siehe /F110/), die ihn anweist das GPF-Template zu verwenden. Die Nachricht wird an den Server übertragen (analog zu /F110/). Der Server entschlüsselt die Nachricht und prüft die Identität des Absenders und kann so den Absender eindeutig bestimmen. Das hinterlegte GPF-Template wird an den GPF übertragen.

Produktdaten

System-Daten auf mobilen Geräten

/D010/ **Die Einstellungen**

Die Einstellungen beinhalten:

- Benutzerkennung
- eine Liste der zentralen Server und deren Zugangsdaten
- Sonstige Parameter die über /F130/ eingestellt werden können

/D020/ **Tutorial**

Tutorial welches dem Benutzer nach der Installation der Anwendung angezeigt werden soll. Es enthält erklärende Bilder und Texte, die den Anwender über den korrekten Umgang mit der Anwendung unterrichten.

System-Daten auf zentralen Servern

/D110/ **Die Einstellungs-Datei eines Servers beinhaltet folgende Daten:**

Die Einstellungen beinhalten:

- Maximale Anzahl der E-Mail Kontakte jedes Benutzers
- Maximale Speicherdauer für öffentliche Nachrichten

/D120/ **E-Mail-Blacklist**

Liste aller E-Mail Adressen deren Benutzung durch den Server grundsätzlich ausgeschlossen sind inkl. mit Zeitpunkt, wann diese gesperrt wurden.

Benutzer-Daten auf mobilen Geräten

/D210/ **Kontaktinformationen**

Folgende Informationen werden pro Kontakt gespeichert:

- Benutzerkennung
- Verschlüsselungsdaten des Kontakts
- Verknüpfung mitt Telefonbucheintrag des *Smartphones*

/D220/ **Paket-Speicher**

Ein Paket besteht aus dem Nachrichtentext, dem Empfänger, Metadaten wie der Position und Routinginformationen wie z.B. wann die Nachricht gesendet wurde. Alle zu synchronisierenden Nachrichten und Empfangsbestätigungen werden hier gehalten und organisiert.

/D230/ **Eigene Verschlüsselungsdaten**

Verschlüsselungsdaten um ausgehende Nachrichten zu verschlüsseln und eingehende zu entschlüsseln.

/D240/ **Nachrichtenarchiv**

Liste aller öffentlichen oder privaten bereits empfangenen oder versendeten Nachrichten. Es wird zusätzlich der Empfangszeitpunkt gespeichert.

Benutzer-Daten auf den zentralen Servern

/D310/ **Profilinformationen der registrierten Benutzer**

Der Server speichert folgende Profilinformationen von jedem Benutzer

- Benutzerkennung
- (Öffentliche) Verschlüsselungsdaten
- Optionale Kontaktinformationen z.B.
  - Name
  - E-Mail
  - Handynummer
  - Geburtsjahr
  - Land/Region

/D320/ **Paketverarbeitungs-Historie**

Protokolliert alle bereits eingegangen bzw. versendete Nachrichten um unter anderem Duplikate zu erkennen.

Produktleistungen

Die folgenden Anforderungen muss die Anwendung leisten können. Sie sichern die Qualität des Produkts:

Stabilität

/L010/ Wird während einer Synchronisation die Verbindung unterbrochen, so sind die Pakete auf den jeweiligen Geräten dennoch nicht beschädigt.

/L020/ Alle gesammelten Pakete sind auch nach fehlerhafter Bedienung niemals beschädigt.

Datensicherheit

/L030/ Die Daten müssen während der Übertragung ausreichend gesichert und verschlüsselt sein, sodass kein Unbefugter Zugang zu diesen Daten hat.

/L040/ Der Benutzer kann genau entscheiden, wer seine Nachrichten lesen kann.

/L050/ Die Routing- und Verschlüsselungsdaten müssen möglichst klein gehalten werden sodass das System skaliert.

Benutzbarkeit

/L060/ Die Reaktionszeit des Servers für die Funktion /F110/ dauert nicht länger als 30s.

/L070/ Die Anwendung schlägt für Datenübertragungen automatisch die vorhandenen und benutzbaren Übertragungsmöglichkeiten vor.

/L080/ Der Benutzer kann innerhalb von wenigen Minuten die Nachricht verfassen.

/L090/ Das Umwandeln von einer Nachricht zu einem Paket dauert wenige Sekunden.

/L100/ Internetverbindungen sollen automatisch erkannt werden.

Änderbarkeit

/L110/ Programmteile die für die Übertragungs- und Synchronisationsmöglichkeiten zuständig sind, sollen wiederverwendbar sein, dass sie leicht für andere Anwendungsfälle benutzt werden können.

/L120/ Andere Sprachen sollen nachträglich leicht eingepflegt werden können.

/L130/ Systematische Trennung zwischen Programmteilen, die für Übertragung von Paketen zuständig sind, und sonstigen Programmteilen.

Produktumgebung

Da dieses Produkt auf dem *Microsoft Imagine Cup 2012* vorgestellt werden soll, wird als Anwendungsplattform das Microsoft Windows Phone 7 (WP7) benutzt. Passend dazu wird die Microsoft Azure Plattform/Serverinfrastruktur verwendet.

Da es zu gegebenen Zeitpunkt noch keine Unterstützung für Ad-hoc Verbindungen in WP7 gibt, werden wir eine eigens entwickelte simulierte Bluetooth Schnittstelle nutzen, die über eine bereits bestehende WLAN Verbindung realisiert wird. Die Schnittstelle wird Betriebssystemen anderer Smartphone-Hersteller nachempfunden. Dadurch ist gewährleistet, dass sobald die Unterstützung seitens Microsoft nachgerüstet wird, ohne großen Aufwand diese implementiert werden kann.

Architektur

- außerhalb des Krisengebiets: Client-Server Umgebung (Nachrichten über Server an Bekannte)
- innerhalb des Krisengebiets: P2P-Architektur (Kommunikation zweier Benutzer im selben Krisengebiet)

Software

Serverseite: Microsoft Azure[1]

- HTTP-Instanz
- Microsoft SQL-Instanz
- SMTP-Dienst

Clientseite:

- Windows Phone 7.5 Betriebssystem

Hardware

Serverseite:

- Keine eigene Hardware, da Azure.

Clientseite:

- Ein Smartphone mit folgenden Eigenschaften:
  - Eingabegerät (Tastatur und/oder Touchscreen)
  - Ausgabegerät (Display)
  - WLAN
- Optionale Eigenschaften:
  - GPS Modul
  - Kamera
- Bluetooth vorerst simuliert, bis Windows Phone 7 die Schnittstellen unterstützt.

[1] https://www.microsoft.com/windowsazure/

Qualitätsbestimmungen

- Pakete sollen nicht mittels Angriffen unerlaubt entschlüsselt werden können
- Pakete sollen von Geräten als reine Dateneinheit behandelt werden, sodass keine Schadsoftware installiert werden kann.
- Nachrichten sollen unverändert am Empfänger eintreffen. Sollten Änderungen an einer Nachricht vorgenommen worden sein, soll dies vom Empfänger erkannt werden können.
- Bei Paketübertragungen zwischen zwei Geräten sollen keine Pakete unbemerkt verloren gehen
- Bei zu vielen Nachrichten sollen oft übertragene Nachrichten niedrig priorisiert oder sogar verworfen werden und neuere bevorzugt übertragen werden.
- Durch geeignete Strategien soll eine Überlastung des Systems z.B. durch Überflutung von Nachrichten durch einzelne Benutzer vermieden werden.

Diese Kriterien sollen, wenn möglich, mittels der Simulation überprüft werden.

Globale Testfälle

Testfälle

Die hier aufgeführten Testfälle sind zu überprüfen und dienen dazu, alle Anforderungen sicherzustellen.

Basis-Testfälle

/T010/ Installation und Einrichten der Anwendung

/T020/ Blockieren und wieder Entsperren von Kontakten

/T030/ Schlüsselaustausch und –aktualisierung zwischen zwei Benutzern

/T040/ Bearbeiten eines Kontaktes im Telefonbuch

/T050/ Synchronisation von fremden und eigenen Nachrichten

/T060/ Automatische / Stand-By Synchronisation von fremden und eigenen Nachrichten

/T070/ Anzeigen und löschen empfangener Nachrichten

/T080/ Übertragung der Nachrichten an den Server und Weiterleitung via E-Mail

/T090/ Generieren, Übermittlung und Verarbeitung von Empfangsbestätigungen

Erweiterte Testfälle

Stabilitätstestfälle

/T110/ Erhalten einer Nachricht während Verfassen einer neuen Nachricht

/T120/ Benutzung der Anwendung während laufender Synchronisation

/T130/ Abbruch einer Verbindung während einer Synchronisation

/T140/ Löschen von Nachrichten während dem Empfangen neuer Nachrichten

/T150/ Mehrfaches Eintreffen ein und derselben Nachricht an einem Gerät

/T160/ Empfangen einer manipulierten Nachricht

Testszenarien

Testszenario 1 - Installation und Einrichten der Anwendung

1. Starten der Anwendung
2. Erstellen eines Accounts, Registrierung
3. Prüfen welche Einträge aus dem Telefonbuch ebenfalls Nutzer sind
4. Kopieren aller öffentlicher Schlüssel von Kontakten vom Server zum Gerät

Testszenario 2 - Bearbeiten der Kontakte

1. Sperren eines Kontaktes
2. Gesperrter Kontakt ändert seinen Schlüssel
3. Email-Adresse eines Kontaktes im Telefonbuch ändern
4. Entsperren des Kontakts
5. Hinzufügen eines neuen Kontaktes zum Telefonbuch

Testszenario 3 - Verwalten empfangener Nachrichten

1. Lesen einer neu empfangenen Nachricht
2. Lesen einer bereits gelesenen Nachricht
3. Löschen einer Nachricht
4. Anzeigen welche Empfänger eine Empfangsbestätigung gesendet haben
5. Anzeigen versendeter Nachrichten

Testszenario 4 - Synchronisation von Nachrichten über Bluetooth

1. Verbinden mit einem anderen Gerät mittels Bluetooth
2. Übertragen von Paketen und Erhalten von Nachrichten
3. Austauschen von evtl. neu generierten Empfangsbestätigungen

Testszenario 5 - Nachrichtenvermittlung öffentlicher Nachrichten

1. Öffentliche Nachricht verfassen und anschließende
2. Mehrfache Paketsynchronisation
3. Lesen der öffentlichen Nachricht auf beliebigen beteiligtem Gerät

Testszenario 5 - Nachrichtenvermittlung öffentlicher Nachrichten

1. Nachricht verfassen
2. Paketsynchronisation
3. Sobald eine Internetverbindung vorhanden ist, sendet der Paketsynchronisationspartner die Nachrichten via Internet an Server
4. Server entschlüsselt Nachricht und leitet sie via Mail an Empfänger weiter.

Datenkonsistenzen

/T200/ Es können nur Nachrichten gelesen werden, die an den Benutzer adressiert wurden

/T210/ Der Server kann Nachrichten eindeutig einem Benutzer zuordnen

/T220/ Ein Gerät speichert nur die öffentlichen Schlüssel der nicht-blockierten Kontakte plus den des Servers

/T230/ Dem Server sind alle öffentlichen Schlüssel bekannt

/T240/ Telefonbuch des Smartphone und Kontaktinformationen der Anwendung sind konsistent

Systemmodelle

Szenarien

Szenario 1

Alice und Bob haben die Anwendung auf ihren WP7-Geräten installiert. Eine weitere Person Carol besitzt diese Anwendung nicht. Mit der Installation erstellen Alice und Bob einen Account und wählen dabei die Personen aus, die sie im Falle eines Notfalls kontaktieren wollen. Alice hat unter anderem Carol ausgewählt.

Ein Tornado zerstört die örtlichen Telefon- und Internetverbindungen. Alice und Bob sind betroffen. Das Gebiet in dem sich Carol befindet ist nicht betroffen und sie verfügt über Internetzugang. Alice verfasst nun eine Notfallnachricht an Carol und tauscht diese mit Bob durch eine Paketsynchronisation aus.

Nach einer Zeit erhält Bob Internetzugang, da er sich nun in einem Gebiet befindet, in dem die Netzwerkinfrastruktur wieder zur Verfügung steht. Nun schickt Bob all seine gesammelten Notfallnachrichten, unter Anderen die von Alice, an den Server.

Jetzt ist der Server in der Lage Carol die Nachricht von Alice via Mail zuzustellen.

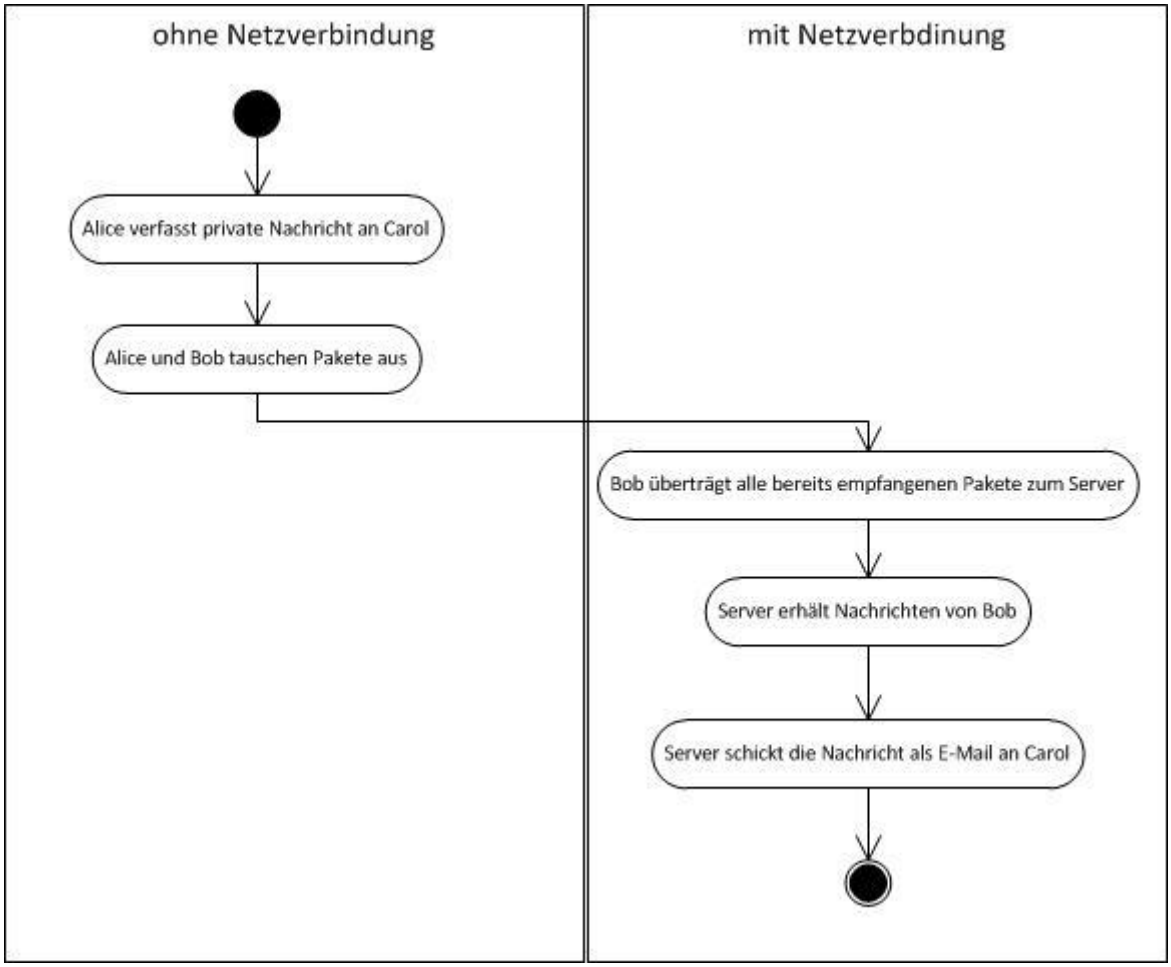

Abbildung 7 - Diagramm "Szenario 1"

Szenario 2

Alice, Bob und Carol haben die Anwendung auf ihren WP7-Geräten installiert.

Mit der Installation erstellen Alice, Bob und Carol einen Account. Nach der Installation erstellen Alice und Bob einen Account und wählen dabei die Personen aus, die sie im Falle eines Notfalls kontaktieren wollen. Alle nötigen Profilinformationen werden vom Server auf ihre Geräte kopiert. Alice hat unter anderem Carol ausgewählt.

Nun kommt es zu einem Erdbeben und die örtlichen Telefon- und Internetleitungen sind dort, wo sich Alice, Bob und Carol befinden, stark beschädigt. Alice verfasst eine Notfallnachricht an Carol und tauscht diese durch eine Paketsynchronisation mit Bob aus.

Später trifft Bob Carol und beide tauschen ihre gesammelten Nachrichten ebenfalls mit einer Paketsynchronisation aus.

Dabei erhält Carol von Bob die Nachricht von Alice, die an Carol adressiert war und kann diese gleich lesen. Für Bob ist die Nachricht von Alice an Carol nicht lesbar.

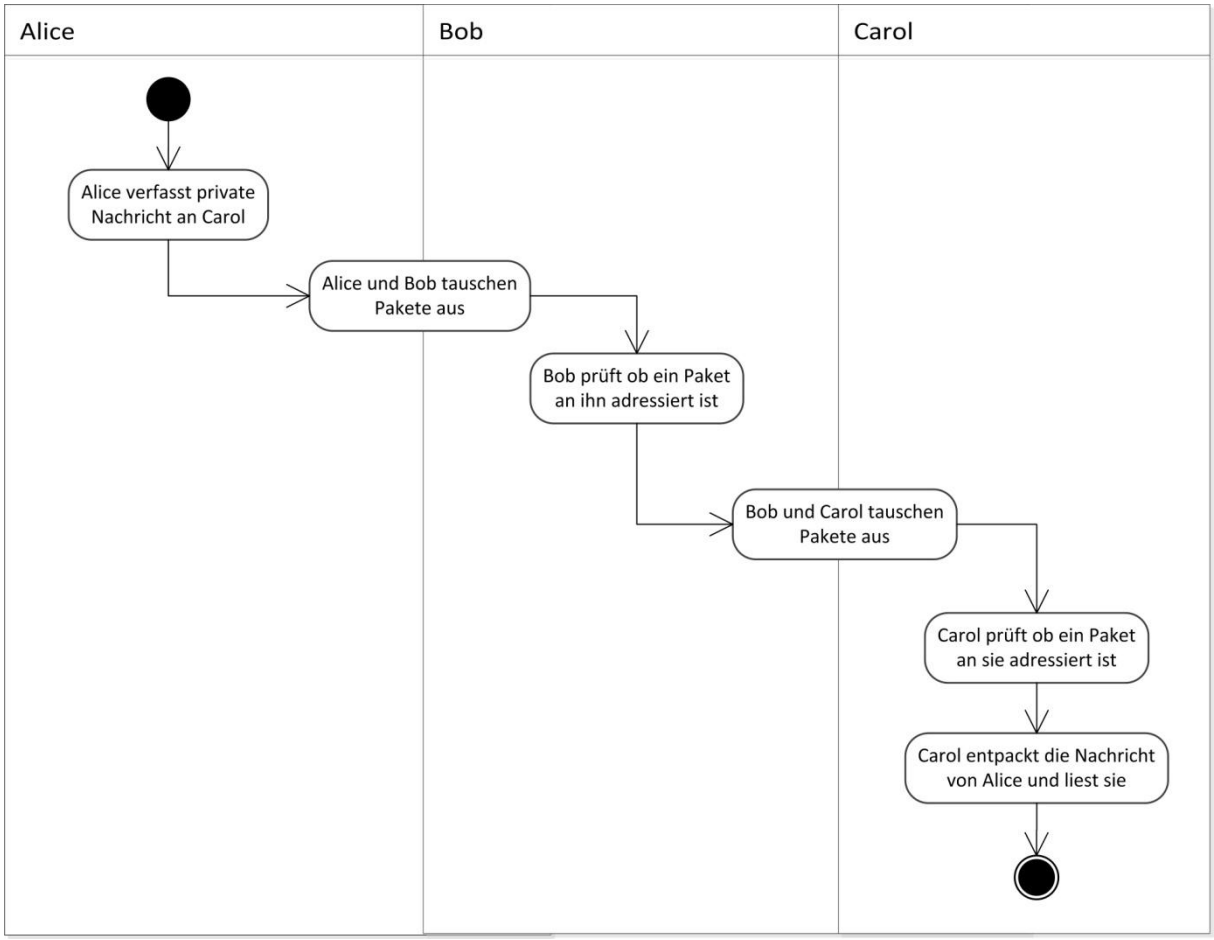

Abbildung 8 - Diagramm "Szenario 2"

Szenario 3

Alice, Bob und Carol haben die Anwendung auf ihren WP7-Geräten installiert. Mit der Installation erstellen Alice, Bob und Carol einen Account. Nach der Installation erstellen Alice und Bob einen Account und wählen dabei die Personen aus, die sie im Falle eines Notfalls kontaktieren wollen.

Durch eine Überflutung befinden sich Alice, Bob und Carol in einem Gebiet ohne Netzwerkinfrastruktur.

Alice entdeckt eine unpassierbare Stelle und verfasst eine öffentliche Nachricht um andere über diese Stelle zu informieren. Nun trifft sie Bob und übergibt ihm durch eine Paketsynchronisation ihre Nachrichten. Bob liest die Warnung und ist informiert.
Zu einem späteren Zeitpunkt trifft sich Bob mit Carol und die Nachrichten werden automatisch ausgetauscht, weil sich beide Geräte im Modus ‘automatisch’ befinden. Carol erhält nun die Warnung die Alice verfasst hat und ist ebenfalls informiert.

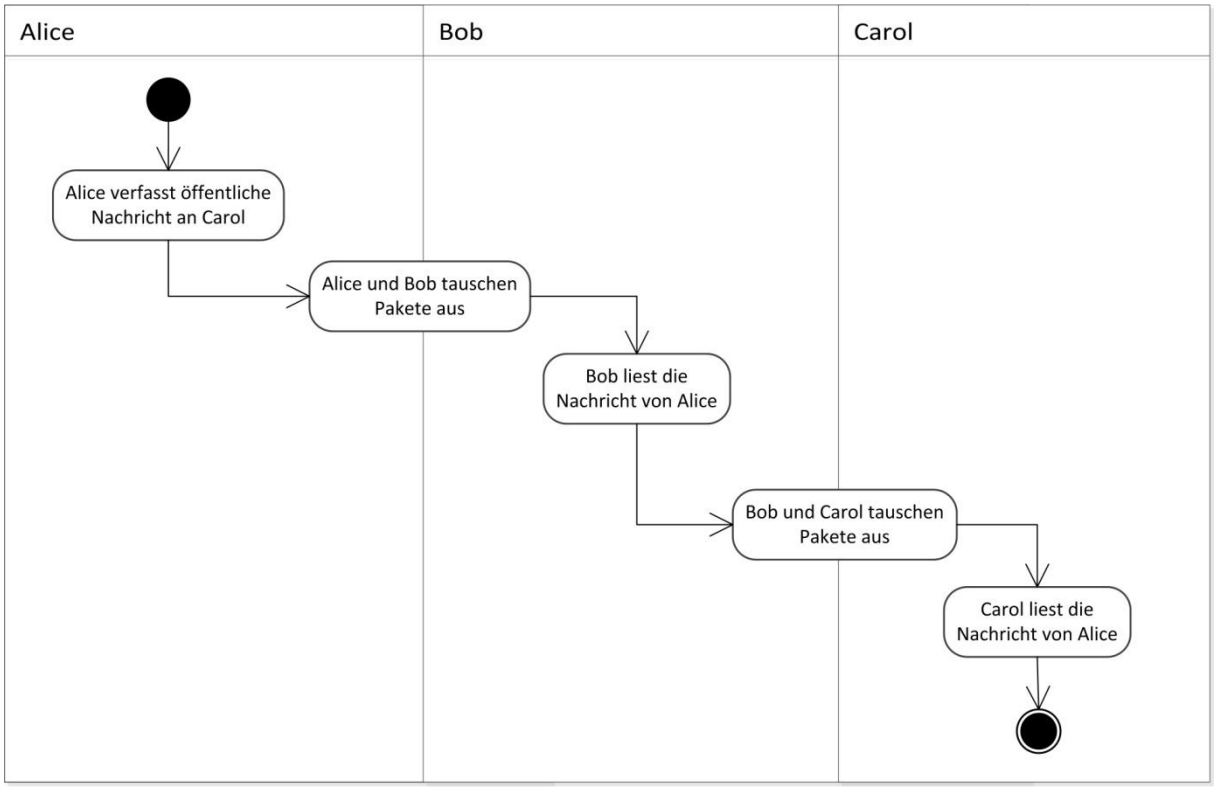

Abbildung 9 - Diagramm "Szenario 3"

Glossar

Ad-hoc Bordmittel

Alle Netzwerkschnittstellen eines Gerätes, die in der Lage sind direkte Verbindungen zu anderen Geräten mit der gleichen Netzwerkschnittstelle herzustellen. Dabei erfolgt die Konfiguration einer solchen Verbindung selbständig und ohne Konfiguration. Zu Ad-hoc-Schnittstellen gehören z.B. Bluetooth, Near Field Communication (NFC) und Ad-hoc Wifi.

Benutzer

Eine Person, die die Anwendung benutzt. Somit verfügt sie unter anderem über Profilinformationen, die auf dem Server gespeichert sind.

Empfangsbestätigung

Eine kleines Paket, die beim Eintreffen einer Nachricht beim Empfänger erstellt wird. Nur der Empfänger kann dieses Paket erzeugen. Es wird automatisch an den Verfasser der ursprünglichen Nachricht adressiert. Durch diese Empfangsbestätigung werden alle anderen Netzwerkknoten darüber informiert, dass sie das ursprüngliche Paket aus ihrem lokalen Speicher löschen können. Für öffentliche Nachrichten gibt es keine Empfangsbestätigung. Der Server versendet Empfangsbestätigungen unabhängig davon ob die E-Mail gelesen wurde.

Google Person Finder (GPF)

Projekt von Google, das Leuten helfen soll Vermisste in Katastrophengebieten wieder zu finden. Diese Anwendung soll nach Möglichkeit eine Schnittstelle zur Verfügung stellen, dass Benutzer vordefinierte Informationen mit dem Versenden eine Nachricht im Google Person Finder veröffentlichen können.

Kontakt

Person bzw. Benutzer A ist ein Kontakt von Benutzer B, wenn B über Profilinformationen von A verfügt.

Nachricht

Eine Botschaft von einem Benutzer an eine andere Person oder von einem Benutzer an den Server.

Netzwerkinfrastruktur

Beschreibt die Infrastruktur, die Kommunikation zwischen mehreren Teilnehmern ermöglicht. Notwendig sind Kabelleitungen und sonstige Hardware, sowie Funkverbindungen. Beispiele hierzu wären Telefonnetze, GPRS, UMTS, LTE oder ISDN.

Öffentliche Nachricht

Eine Nachricht die für alle lesbar ist.

Öffentlicher Schlüssel

Schlüssel eines Benutzers, der auf dem Server gespeichert wird. Um einen Benutzer eine verschlüsselte Nachricht senden zu können, braucht man diesen öffentlichen Schlüssel.

Paket

Eine Nachricht auf dem Übertragungsweg. Zusätzlich sind Metainformationen im Paket enthalten. Die Übertragenden können den Inhalt nicht lesen.

Pakete synchronisieren

Beschreibt dem Vorgang, bei dem zwei Geräte untereinander Pakete austauschen und jeweils auswerten.

Peer-to-Peer (P2P)

Eine direkte Verbindung zwischen zwei Geräten. Es sind keine weiteren Geräte erforderlich um die Verbindung aufzubauen, als die beiden Kommunikationspartner.

Person

Eine beliebige Person, dabei muss es sich nicht zwingend um einen Benutzer der Anwendung handeln.

Profil

Die vom Benutzer auf dem Server hinterlegten persönlichen Daten und Informationen, die es anderen Benutzern ermöglichen mit dem Profileigentümer zu kommunizieren. Dient zur Identifizierung von Benutzern untereinander.

Smartphone

Mobilfunkgerät, das über höhere Konnektivität und Rechenleistung als herkömmliche Modelle verfügt.

System

Alle Beteiligten Personen, Geräte und zentralen Server.

Telefonbuch

Das gewöhnliche Telefonbuch, das auf dem Gerät bereits vor der Installation der Anwendung verwendet wird.

Übertragungsmodus

Manuell, standby, automatisch. Gibt an ob die Anwendung selbständig Paketsynchronisationen beginnt oder nicht. Der Modus ‘automatisch’ sucht selbständig nach Geräten die zur Paketsynchronisation bereit sind. Standby sucht nicht aktiv, sondern reagiert nur auf Anfragen. Daraufhin wird der Benutzer gefragt, ob eine Synchronisation durchgeführt werden soll, oder nicht.

Windows Phone 7 (WP7)

Ein Betriebssystem, das von Microsoft für *Smartphones* entwickelt wurde.

Benutzeroberfläche

Beispiel 1

Abbildung 10 - Benutzeroberfläche "Startbildschirm WP7"

Beispiel 2

Abbildung 11 - Benutzeroberfläche "Startbildschirm Lauffeuer"

Beispiel 3

Abbildung 12 - Benutzeroberfläche "Kontakte"

Abbildungsverzeichnis