

pribook.com  
**Handbuch**

Finn Siebert  
23. Februar 2012

**Im Rahmen der Diplomarbeit:**

Ein RSA-basiertes Konzept zum Erhalt der  
Privatsphäre in Social Network Services



# Inhaltsverzeichnis

<b>1</b>	<b>Handbuch</b>	<b>1</b>
1.1	Einleitung . . . . .	1
1.2	Voraussetzungen . . . . .	1
1.3	Registrierung . . . . .	2
1.4	Anmeldung . . . . .	5
1.5	Nachrichten . . . . .	5
1.5.1	Nachrichten versenden . . . . .	5
1.5.2	Nachrichten empfangen . . . . .	6
1.5.3	Eine Nachricht . . . . .	6
1.5.4	Nachrichten löschen . . . . .	7
1.6	Suche . . . . .	7
1.7	Profildaten . . . . .	8
1.7.1	Profildaten speichern . . . . .	8
1.7.2	Profile . . . . .	9
1.7.3	Profilinformationen . . . . .	10
1.7.4	Profildaten löschen . . . . .	10
1.8	Freundschaften . . . . .	10
1.8.1	Freundschaftsanfragen stellen . . . . .	11
1.8.2	Freundschaften kündigen . . . . .	11
1.8.3	Freundschaftsanfrage bestätigen . . . . .	11
1.8.4	Freundschaftsanfragen verstecken . . . . .	11
1.9	Gruppen . . . . .	11
1.9.1	Gruppen gründen . . . . .	13
1.9.2	Nutzer in Gruppen einladen . . . . .	13
1.9.3	Gruppeninformationen speichern . . . . .	13
1.9.4	Gruppeninformationen ansehen . . . . .	13
1.9.5	Mitgliedschaft ein einer Gruppen beantragen . . . . .	15
1.9.6	Mitgliedschaft ein einer Gruppen löschen . . . . .	15
1.9.7	Nachrichten an Gruppen schicken . . . . .	15
1.10	Circles . . . . .	15

1.10.1	Circle erstellen . . . . .	15
1.10.2	Nutzer zu einem Circle hinzufügen . . . . .	16
1.10.3	Einen Circle löschen . . . . .	16

# Kapitel 1

## Handbuch

Dieses Kapitel ist ein Handbuch für pribook.com. Hier wird beschrieben, wie die prototypische Umsetzung für den Endbenutzer aussieht und wie die einzelnen Funktionen bedient werden.

### 1.1 Einleitung

Pribook ist ein Social Network Service, der die Privatsphäre der Nutzer bewahrt. Mit Hilfe des asymmetrischen Verschlüsselungsverfahrens RSA werden die Inhalte von Nachrichten und Profilinformatoren vor dem Versenden verschlüsselt. Auf den Inhalt der Nachrichten können dann nur der Absender und die Empfänger zugreifen. Da die Daten schon im Webbrowser verschlüsselt werden, noch bevor sie an den Server geschickt werden, hat selbst der Netzbetreiber keine Chance auf die Daten zuzugreifen.

Bei der Registrierung wird für jeden Nutzer ein RSA-Schlüsselpaar erstellt. Der private Schlüssel wird mit dem Passwort des Nutzers verschlüsselt und dann zusammen mit dem öffentlichen Schlüssel an das Netzwerk gesendet. So muss sich der Nutzer lediglich sein eigenes Passwort merken. Beim Verschicken einer Nachricht werden automatisch die öffentlichen Schlüssel der Empfänger vom Server geholt und die Nachricht noch vor dem Versenden verschlüsselt. Empfangene Nachrichten werden mit dem privaten Schlüssel der Nutzer entschlüsselt, der selbst zunächst vom Server geholt und dann mit dem eingegebenen Passwort entschlüsselt wird.

### 1.2 Voraussetzungen

Zum Starten von Pribook muss ein Webbrowser geöffnet und die URL <http://www.pribook.com> in die Adressleiste eingegeben werden. Pribook wurde mit den folgenden Webbrowsern getestet:



Achtung: Diese Internetseite ist noch in der Beta-Testphase. Sollst du einen Fehler finden, oder einen Verbesserungsvorschlag haben, so kannst du entweder im pribook eine Nachricht an den Nutzer "hilfe" schicken oder eine Email an [hilfe@pribook.com](mailto:hilfe@pribook.com). Vielen Dank! Wichtiger Hinweis: Wie angekündigt, wurden am 01.02.12 alle bestehenden Accounts gelöscht.

Abbildung 1.1: pribook.com: Anmeldebildschirm

**Registrieren:**

Name:\*

Passwort:\*

Passwort wiederholen:\*

(Achtung: Das erstellen des Schlüssels kann ein paar Minuten dauern!)

Abbildung 1.2: pribook.com: Registrierung

- Firefox 10.0
- Chromium 16.0

Die Nutzung von anderen Webbrowsern kann dazu führen, dass Pribook nicht richtig ausgeführt wird. Nach dem Aufrufen der URL lädt der Webbrowser den Anmeldebildschirm. Siehe Abbildung 1.1.

### 1.3 Registrierung

Um das Netzwerk nutzen zu können, braucht jeder Nutzer einen Account. Das Formular zum Registrieren wird durch einen Klick auf "oder erst registrieren" im Anmeldebildschirm geöffnet. Siehe Abbildung 1.2. In das Formular müssen für die Registrierung ein Pseudonym und ein Passwort eingegeben werden. Das Pseudonym muss mindestens 3 Zeichen lang sein,

und darf nur Buchstaben, Ziffern und Unterstriche enthalten. Umlaute sind nicht erlaubt. Um bei der Passworteingabe die Wahrscheinlichkeit eines Tippfehlers zu minimieren, wird eine doppelte Passworteingabe verlangt. Das Passwort muss mindestens acht Stellen haben. Damit das Passwort möglichst sicher ist, sollten die folgenden Regeln eingehalten werden:

- Das Passwort sollte Ziffern, Kleinbuchstaben, Großbuchstaben und Sonderzeichen enthalten.
- Das Passwort sollte möglichst zufällig sein und keine Worte, Namen oder Begriffe enthalten.

Eine sichere Möglichkeit, sich Passwörter auszudenken und zu merken ist laut [LINK] die Methode, die Anfangsbuchstaben, Sonderzeichen und Zahlen eines Satzes zu nehmen. Dafür muss ein Satz erfunden werden, in dem sowohl Zahlen als auch Sonderzeichen vorkommen. Ein Beispiel dafür ist der Satz: "Beim Italiener um die Ecke bestelle ich am liebsten die Nummer 28, Pizza mit Champignons." Die Anfangsbuchstaben, Ziffern und Sonderzeichen dieses Satzes, der relativ einfach zu Merken ist, bilden das Passwort. Der vorliegende Satz würde also zu dem Passwort: "BiudEbialdN28,PmC."

Achtung: Passwörter können bei Verlust nicht zurückgesetzt werden. Bei Verlust des Passwortes sind alle Daten unwiderruflich verloren und können nicht mehr entschlüsselt werden.

Nach einem Klick auf "Schlüssel generieren" werden die Passwörter überprüft und bei Übereinstimmung und ausreichender Länge wird in RSA-Schlüsselpaar generiert. Sollten die Passwörter nicht den Voraussetzungen entsprechen, erscheint eine Fehlermeldung und der Nutzer kann die Passwörter erneut eingeben. Das Erstellen der Schlüssel kann je nach System und Webbrowser einige Minuten dauern. Nachdem das Schlüsselpaar erstellt wurde, wird der private Schlüssel mit dem eingebenden Passwort verschlüsselt. Anschließend werden alle Schlüssel – der private, der öffentliche und der verschlüsselte private Schlüssel angezeigt. Siehe Abbildung 1.3.

Nun kann sich der Nutzer durch einen Klick auf "Registrieren" im Netzwerk registrieren. Sollte das Pseudonym schon vergeben sein, oder nicht den Voraussetzungen entsprechen, so gibt es jetzt eine Meldung und der Nutzer kann das gewählte Pseudonym ändern und erneut auf "Registrieren" klicken. Für die Registrierung werden das Pseudonym, der öffentliche Schlüssel, der verschlüsselte private Schlüssel, ein Hashwert des Passwortes und ein zufällig gewählter Salt an den Server geschickt. Das Passwort und der private Schlüssel bleiben nur dem Nutzer sichtbar. Hat die Registrierung geklappt, erscheint eine entsprechende Meldung.

**Name:\***

**Public Key:**  
*yUeiFC9h7CLhiAN0AxaRdwsvwsKW3pG1DVcUUaZwWkWxxYU70G3tllQj9m5ZZ6WAf6FLZMnh  
RV2K5WyxrsRDdWe63uAFLZg44Fs3Raz9NNFzQGqyzXRvqSbxa8GA4WVvxamyTt5WeB6WDB  
nOKN6ywnihXa8a7egDxaQd7Cjif9DyeUTVngQq7qxx72yHqsxae2lnSbxxovxasvSIX5AhrVQBNMxb  
d5vRyrJHC4MEC20YVRIXe9ISA*

**Private Key:**  
*e6llNja1xxNkcke2UDjsk4L504bJeVlsT9w1xaDOQ3VgBM6JaKZFUgc0S3OfgfPoc5NV4F7YxbVTt  
QPubiB5JB3qIp5tFVbR8ALSV8igNDR0tPEeWxa6NxbRnIUzT0ryaPgimCxb75UWiy8zltjJwRxxX  
PxbihWjR4N9d6MPq2xxBn5Pcaxaj9HXzaqv800FU0NxaxageTOlcp9fEUmexaTIhzB3EMuxbA3dq  
bzFKIQRHxa5veac24pQ8ulqUhrscnZ4cr8SnpRxxF4Avzxa0VNaHaRxaCVR00jXgJAF6kxa6WRd  
ekFZENxaxad630j0jQTW7hUwCWz92JxbubZMhzMCIIEpRmLxarhInTxbqxaYCULPBeTM9eZd119  
bYMtHCPUpTfwqOCgfnNtqbrRpuVmfVnxxdkj8tOIOITKDAPO*

**Private Key (verschlüsselt):**  
1xbM16oqVJbcLpcnZrOexx2bAqFzxbLjOsoQWJqcLwLoS9YGYbsJJCJPCCxx2u774vGP8WNPjV  
Hmrzp8AORHiE7vUv6xxSLbdopKHJm7DVn4fFNcRtleAdeUZvoj2iRYH5siebluePRLbOlx4KqI9  
T9cw1EYg77CjinoPznubWwaZUuWGc3nF7NKxxE8ee7Zxx0DxbvtQgB9Km1ukSnebo9t3xbzBB91  
V0vc3RWvyu7slGWWwKANdTas5ogEfxbnUMuxxBYG3ZUxxXIRExbxxdOzmkL2D21USqSNqyB5  
lb1salpN5DMqbbWEHpFd0RvuaaW1qu4rHO5HY2Ut4pUU9ab8sPpMe9eAZ7edJCMu1evV6tRS  
pujxxAjLAnyBAAsQk7v8lZX7UGriFvpXWB1rc2E2Lst4bV55purEBxxfsw0kRMU4a9qZlj6fjBLJWZJ  
WVqvBhI7W6pnfFZxacYxaz0dYhqLuwHoloxRyfk0YlioRD9EbK1r0TxbdqsfuysNNbRmxaJ05QDx  
xJITlFRXuSX55GcakWAFYrmDC9xxZ82qluGQxxFivA9zAGmTClmFGXgoC37AHp8l8DqTIN1e8gsZ  
7o13DLIGTTRSq8xxbN2CPyCiZN8rFhwWcSrpQ

Abbildung 1.3: pribook.com: Erstellte Schlüssel



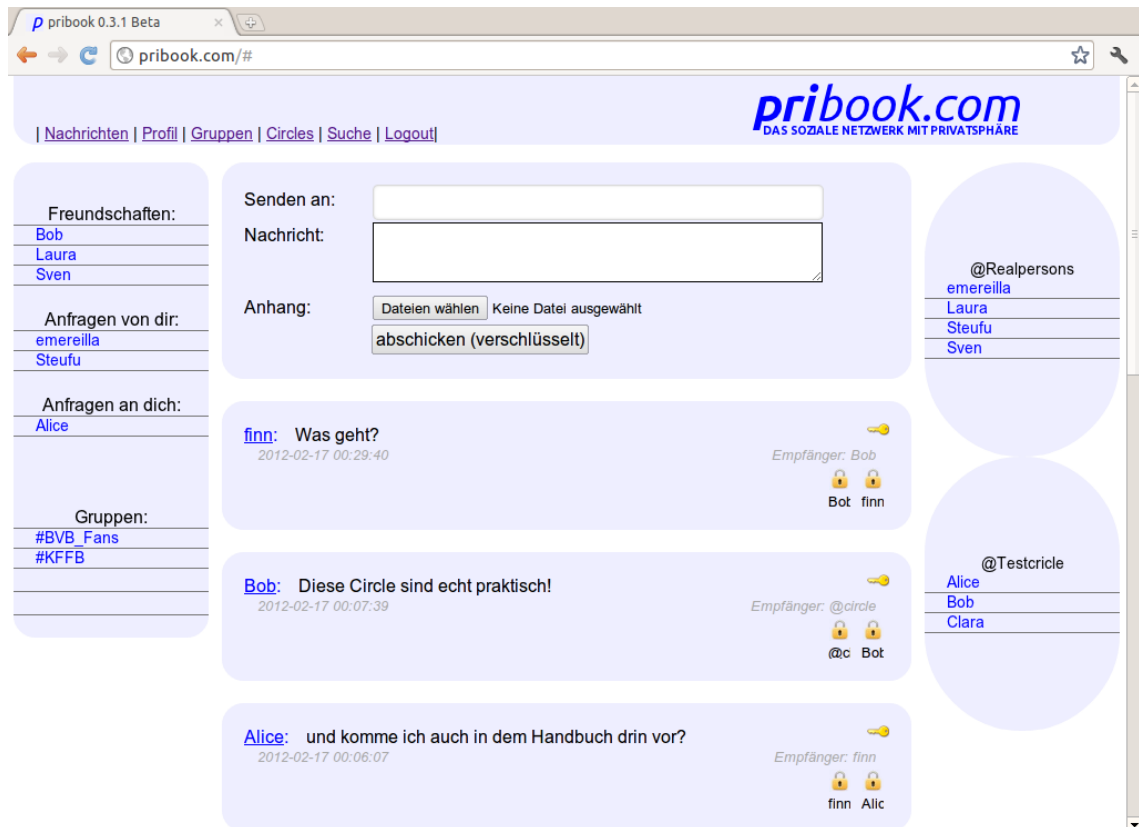


Abbildung 1.4: pribook.com: Hauptbildschirm

## 1.4 Anmeldung

Zur Anmeldung im Netzwerk reicht es, das bei der Registrierung gewählte Pseudonym zusammen mit dem Passwort im Anmeldebildschirm einzugeben und auf "anmelden" zu klicken. Sollten Pseudonym und Passwort korrekt sein, erscheint eine Meldung, die den Anwender mit "Hallo" begrüßt und der Hauptbildschirm öffnet sich. Ist Passwort oder Pseudonym falsch, dann gibt es eine Fehlermeldung und der Anmeldebildschirm bleibt sichtbar. Siehe Abbildung 1.4.

## 1.5 Nachrichten

Direkt nach dem Anmelden oder durch einen Klick auf "Nachrichten" befindet sich der Nutzer auf der Nachrichtenseite. Im oberen Teil befindet sich das Formular zum Versenden und im unteren Teil werden die neusten empfangenen und verschickten Nachrichten angezeigt.

### 1.5.1 Nachrichten versenden

Zum Versenden einer Nachricht wird das Pseudonym des Empfängers in das Feld "Senden an:" und die Nachricht in das Feld "Nachricht" eingegeben und auf "abschicken (verschlüsselt)" geklickt.

Die Nachricht wird daraufhin automatisch verschlüsselt und an den Server verschickt. Dafür wird automatisch ein zufälliger AES-Schlüssel generiert, mit dem die Nachricht verschlüsselt wird. Für die Empfänger und den Absender holt sich die Webanwendung selbstständig die öffentlichen Schlüssel vom Server und generiert damit die Pris(Privacy-Padlocks), die zusammen mit der Nachricht an das Netzwerk gesendet werden.

Wenn die Nachricht erfolgreich verschickt wurde, erscheint eine Meldung und sie wird bei den Nachrichten im unteren Teil der Seite angezeigt. Sollte es ein Problem geben, zum Beispiel, weil das Pseudonym des Empfängers falsch geschrieben ist, so erscheint eine Fehlermeldung.

Eine Nachricht kann auch an mehrere Empfänger gleichzeitig gesendet werden. Dafür müssen die Pseudonyme durch ein Semikolon getrennt werden. Auch Gruppen und Circle können Empfänger einer Nachricht sein. Ein Gruppenname beginnt immer mit einer Raute "# " und ein Circle beginnt immer mit einem At "@ ". Eine korrekte Eingabe für die Empfänger, sähe also zum Beispiel folgendermaßen aus: "Alice; Clara; #Gruppe1; @Friends; Bob" Die Nachricht würde in dem Fall dann an die Nutzer - Alice, Bob und Clara - sowie an den Circle "@Friends" und an die Gruppe "#Gruppe1" gesendet. Es ist auch möglich, Nachrichten Bilder anzuhängen. Dafür müssen vor dem Versenden im Feld "Anhang" Bilder vom lokalen Speicher ausgewählt werden. Diese werden auch automatisch mit demselben AES-Schlüssel wie die Nachricht verschlüsselt und können nach dem Absenden nur noch vom Absender und den Empfängern eingesehen werden.

### 1.5.2 Nachrichten empfangen

Die neusten empfangenen Nachrichten werden im Hauptbildschirm angezeigt und automatisch entschlüsselt. Um nach neuen Nachrichten zu schauen, reicht ein Klick auf "Nachrichten" im oberen Menü. Zunächst werden lediglich die 10 neusten Nachrichten angezeigt. Mit einem Klick auf den Button "ältere Nachrichten anzeigen", der sich unterhalb der Nachrichten befindet, werden 10 weitere Nachrichten angezeigt. Dieser Vorgang lässt sich wiederholen, bis alle empfangenen und versendeten Nachrichten angezeigt werden.

Im Startbildschirm werden die Nachrichten angezeigt, die der Nutzer selbst versendet hat, die er direkt empfangen hat oder die an eine Gruppe oder einen Circle gesendet wurden, deren Mitglied er ist.



Abbildung 1.5: pribook.com: Eine Nachricht

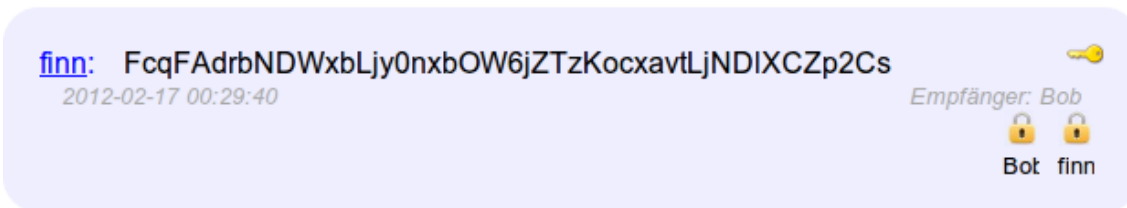


Abbildung 1.6: pribook.com: Eine verschlüsselte Nachricht

### 1.5.3 Eine Nachricht

Eine Nachricht wird folgendermaßen dargestellt: Siehe Abbildung 1.5.

Links befindet sich der Name des Absenders gefolgt von der Nachricht. Oben links befindet sich ein Schlüsselsymbol, das anzeigt, dass die Nachricht verschlüsselt vom Server geholt - und für den Nutzer entschlüsselt wurde. Durch einen Klick auf dieses Symbol wird die verschlüsselte Nachricht angezeigt, so wie sie in der Datenbank gespeichert ist. Siehe Abbildung 1.6.

Unterhalb des Namens befindet sich links das Datum, an dem die Nachricht versendet wurde - oder genauer: an dem die Nachricht laut MEZ den Server erreicht hat. Alle Empfänger der Nachricht stehen rechts davon. Im unteren Teil der Nachricht werden die Privacy-Padlocks - oder kurz Pris - angezeigt. Nur Nutzern, für die ein solches Schloss an der Nachricht hängt, ist es möglich, mit ihrem Passwort die Nachricht zu lesen. Durch einen Klick auf die Schlosssymbole werden die Pris angezeigt, so wie sie in der Datenbank gespeichert sind.

### 1.5.4 Nachrichten löschen

Nutzer können alle Nachrichten löschen, die sie selbst verfasst haben. Sie werden dann vollständig aus der Datenbank entfernt und können nicht mehr wieder hergestellt werden. Auch die Nutzer, die die Nachricht bereits empfangen und gelesen haben, können danach nicht mehr auf sie zugreifen. Wenn ein Nutzer mit dem Mauszeiger über eine Nachricht geht, die er selbst verfasst hat, dann erscheint oben links ein kleines "x". Ein Klick auf dieses "x" reicht, um die Nachricht nach einer weiteren Sicherheitsabfrage zu löschen.



Abbildung 1.7: pribook.com: Suche

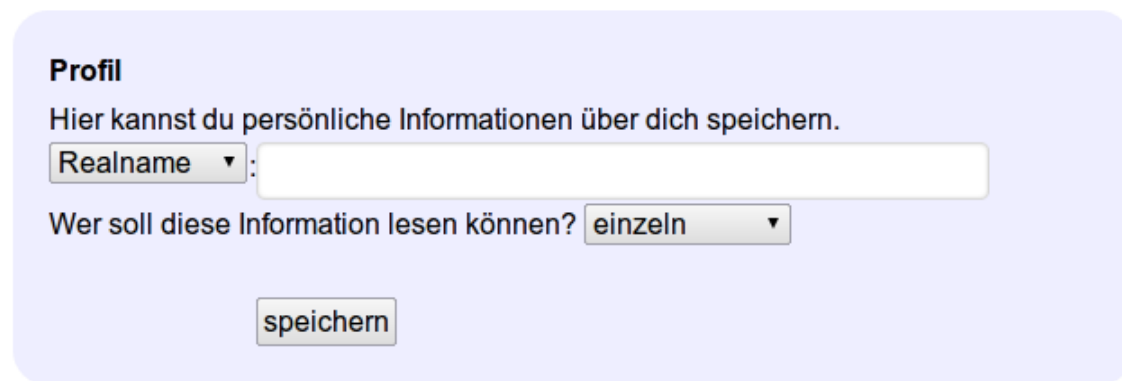


Abbildung 1.8: pribook.com: Profilmnü

## 1.6 Suche

Durch einen Klick auf “Suchen“ im oberen Menü gelangt der Nutzer zum Suchmenü. Siehe Abbildung 1.7.

Um andere User oder Gruppen zu finden, kann die Suche benutzt werden. Hier wird das Pseudonym des gesuchten Nutzers oder der Name der gesuchten Gruppe eingegeben und auf “suchen“ geklickt. Es werden sowohl die passenden Gruppen als auch die passenden Pseudonyme angezeigt. Es reicht, einen Teil des gesuchten Namens einzugeben. Es werden dann alle Pseudonyme und Gruppennamen angezeigt, die das eingegebene Wort enthalten. Klickt ein Anwender auf “suche“ ohne vorher etwas in das Suchfeld einzugeben, so werden die Pseudonyme aller angemeldeten Nutzer und die Namen aller Gruppen angezeigt.

## 1.7 Profildaten

Um Profildaten über sich einzugeben, muss ein Anwender im oberen Menü auf “Profil“ klicken. Es öffnet sich das Profilmnü. Siehe Abbildung 1.8.

### 1.7.1 Profildaten speichern

Zum Speichern einer neuen Profilinformatio n muss zunächst aus der linken Drop-down-Liste ein Attribut wie zum Beispiel “Hobbys“ ausgewählt werden. Die eigentliche Information – zum Beispiel “Schwimmen“ wird in das Textfeld daneben eingegeben. Zusätzlich muss für jede Profilinformatio n in der Drop-down-Liste unten rechts ausgewählt werden, wer diese Information lesen können soll. Zur Auswahl stehen “öffentlich“, die Circle und “einzeln“. Wird das Attribut “öffentlich“ gewählt, so wird die Information nicht verschlüsselt, sondern in Klartext an die Datenbank geschickt. Öffentliche Profilinformatio nen werden jedem Nutzer bei Ansicht des entsprechenden Profils angezeigt. Wird einer der Circle aus der Drop-down-Liste ausgewählt, so wird die Information für den Circle verschlüsselt und nur noch alle Mitglieder des Circles bekommen sie angezeigt und können sie entschlüsseln. Wird in der Drop-down-Liste “einzeln“ ausgewählt, so öffnet sich ein neues Textfeld. In dieses Textfeld können - genau wie bei normalen Nachrichten - einzeln die Empfänger eingegeben werden, die Information lesen können soll. Eine korrekte Eingabe sieht also genauso wie für normale Nachrichten aus. Die Eingabe: “Clara; @Friends; @Kollegen; @Verein“ wäre korrekt. Die Profilinformatio n wird dann für alle Empfänger verschlüsselt an den Server geschickt.

### 1.7.2 Profile

Der Profilbildschirm der verschiedenen Nutzer wird durch einen Klick auf deren Pseudonyme angezeigt. Siehe Abbildung 1.9.

Im oberen Teil des Profilbildschirms befindet sich der Freundschaftsindikator. Hier wird angezeigt, ob eine Freundschaft besteht und die Einstellungen der Freundschaft können verändert werden. Im mittleren Teil befinden sich die Profilinformatio nen des Nutzers, sowie seine Freundschaften und seine Gruppen. Im unteren Teil werden Nachrichten angezeigt, die zwischen den beiden Nutzern versendet wurden.

### 1.7.3 Profilinformatio nen

Profilinformatio nen werden folgendermaßen dargestellt: Siehe Abbildung 1.10.

Links befindet sich das Attribut der Profilinformatio n Name gefolgt von der Information selbst. Wenn die Information nicht öffentlich gespeichert wurde, dann befindet sich oben links ein Schlüsselsymbol, das anzeigt, dass die Information verschlüsselt vom Server geholt - und für den Nutzer entschlüsselt wurde. Durch einen Klick auf dieses Symbol, wird die verschlüsselte Information angezeigt, so wie sie in der Datenbank gespeichert ist. Unterhalb des Attributs befindet sich links das Datum, an dem die Information erstellt wurde. Alle Empfänger, die die Information angezeigt bekommen und entschlüsseln können, stehen rechts davon. Im unteren Teil der Information werden die Privacy-Padlocks - oder kurz Pris - angezeigt. Nur Nutzern, für die ein solches Schloss an der Profilinformatio n hängt,



Abbildung 1.9: pribook.com: Profil



Abbildung 1.10: pribook.com: Profilinformaton

ist es möglich, mit ihrem Passwort die Information zu lesen. Durch einen Klick auf die Schlösser Symbole werden die Pris angezeigt, so wie sie in der Datenbank gespeichert sind.

#### **1.7.4 Profildaten löschen**

Nutzer können ihre eigenen Profilinformatoren jederzeit löschen. Die Profilinformatoren werden dann vollständig aus der Datenbank entfernt und können nicht mehr wieder hergestellt werden. Auch die Nutzer, die die Profilinformatoren bereits eingesehen und gelesen haben, können danach nicht mehr auf sie zugreifen.

Wenn ein Nutzer mit dem Mauszeiger über eine seiner eigenen Profilinformatoren geht, dann erscheint oben links ein kleines "x". Ein Klick auf dieses "x" reicht, um die Information nach einer weiteren Sicherheitsabfrage zu löschen.

## **1.8 Freundschaften**

Nach dem Einloggen wird stets links im Bild die Freundschaftsliste angezeigt. Siehe Abbildung 1.4. Freundschaften sind Verknüpfungen zwischen den Nutzern, die beidseitig bestätigt werden müssen. Wurde eine Freundschaft von beiden Seiten bestätigt, so ist dies eine Freundschaft und wird im oberen Teil der Freundschaftsliste angezeigt. Eine Freundschaftsanfrage, die noch nicht bestätigt wurde, wird darunter unter "Anfragen von dir" angezeigt. Freundschaftsanfragen an den Nutzer selbst, die er noch nicht bestätigt hat, werden darunter unter "Anfragen an dich" angezeigt. Im Profilbildschirm eines Nutzers, werden alle Freundschaften, die beidseitig geschlossen wurden und nicht versteckt sind angezeigt.

### **1.8.1 Freundschaftsanfragen stellen**

Um eine Freundschaftsanfrage zu stellen, muss auf das Pseudonym des entsprechenden Nutzers geklickt werden, damit sich der Profilbildschirm des Nutzers öffnet. Im oberen Bereich des Profilbildschirms befindet sich der Freundschaftsindikator. Hier muss auf "Freundschaft anbieten" geklickt werden, um eine Freundschaft anzubieten.

### **1.8.2 Freundschaften kündigen**

Eine Freundschaftsanfrage wird zurückgezogen, in dem im Freundschaftsindikator im Profilbildschirm auf "Freundschaft zurückziehen" oder "zurückziehen" geklickt wird.

### **1.8.3 Freundschaftsanfrage bestätigen**

Wurde eine Freundschaftsanfrage an einen User gestellt, so kann dieser die Freundschaftsanfrage bestätigen, in dem er auf "bestätigen" im Freundschaftsindikator klickt.

#### 1.8.4 Freundschaftsanfragen verstecken

Freundschaftsanfragen können versteckt werden. Wenn eine Freundschaftsanfrage versteckt ist, so wird sie nur noch den beiden befreundeten Usern angezeigt. Es reicht, wenn die Freundschaftsanfrage von einem der beiden User versteckt wird.

### 1.9 Gruppen

Gruppen dienen dazu, dass Nutzer sich miteinander vernetzen können. Gruppen teilen sich einen Schlüssel, so dass alle Gruppenmitglieder Nachrichten an die ganze Gruppe senden und empfangen können. Es können auch Gruppeninformationen gespeichert werden, die entweder öffentlich oder nur für die Gruppe sichtbar sind. Alle Mitglieder einer Gruppe können neue Leute in eine Gruppe einladen. Eingeloggte Nutzer bekommen stets unten links die Gruppen angezeigt, in denen sie Mitglied ist oder für die sie eine Einladung bekommen haben. Siehe Abbildung 1.4. Durch einen Klick auf "Gruppen" im oberen Menü öffnet sich das Gruppenmenü Siehe Abbildung 1.11.

#### 1.9.1 Gruppen gründen

Eine neue Gruppe kann gegründet werden, indem unter "Neue Gruppe erstellen" ein Gruppenname in die Textbox eingegeben und auf "gründen" geklickt wird. Ist der Gruppenname noch nicht vergeben und entspricht den Voraussetzungen (Nur Ziffern, Unterstriche und Buchstaben, keine Umlaute) so wird die Gruppe jetzt erstellt und es gibt eine entsprechende Meldung. Andernfalls erscheint eine Fehlermeldung. Bei der Gründung einer Gruppe wird automatisch ein Schlüssel generiert, der für jedes Mitglied verschlüsselt in der Datenbank gespeichert wird.

#### 1.9.2 Nutzer in Gruppen einladen

Im Gruppenmenü unter "Gruppeneinladungen" können andere Nutzer in die eigenen Gruppen eingeladen werden. Dazu wird aus der Drop-down-Liste die entsprechende Gruppe ausgewählt, in die Textbox das Pseudonym des Nutzers getippt, der eingeladen werden soll und dann auf "einladen" geklickt. Ein Nutzer, der in die Gruppe eingeladen wird, bekommt den Gruppenschlüssel und kann nun auf alle Nachrichten und Informationen zugreifen, die an die Gruppe adressiert sind. Nutzer können nur freiwillig wieder aus einer Gruppe austreten. Aber auch dann kann es sein, dass sie den Schlüssel gespeichert haben und damit die Nachrichten der Gruppe entschlüsseln können.

#### 1.9.3 Gruppeninformationen speichern

Jedes Mitglied kann für seine Gruppen Informationen speichern. Diese können öffentlich sein, sodass sie nicht verschlüsselt werden und von allen Nutzern gesehen werden können.



**meine Gruppen**

Hier kannst du Informationen über die Gruppen speichern bei denen du Mitglied bist. Wähle zunächst eine Gruppe und dann ein Attribut aus und gebe dann die Info ein. Du kannst entscheiden, ob die Info öffentlich sein soll, oder nur für Gruppenmitglieder.

#KFFB ▾ : Beschreibung ▾ :

Wer soll diese Information lesen können?

**Gruppeneinladungen:**

Hier kannst du Menschen in deine Gruppen einladen! Wähle eine Gruppe aus und gebe dann den Namen ein.

#KFFB ▾ :

**Neue Gruppe erstellen:**

Name:

Abbildung 1.11: pribook.com: Gruppenmenü



**Abbildung 1.12:** pribook.com: Gruppenprofil

Dies kann zum Beispiel sinnvoll sein, um neue Leute für die Gruppe zu interessieren. Informationen können aber auch intern sein, dann werden sie mit dem Schlüssel der Gruppe verschlüsselt und nur noch die Gruppenmitglieder können darauf zugreifen. Gruppenmitglieder speichern neue Gruppeninformationen folgendermaßen. Zunächst wird im Gruppenmenü unter meine Gruppen in der ersten Drop-down-Liste die entsprechende Gruppe ausgewählt. In der zweiten Drop-down-Liste wird ein Attribut für die Information ausgewählt zum Beispiel "Beschreibung". Dann wird die Information in das Textfeld eingegeben, in der unteren Drop-down-Liste ausgewählt, ob die Information öffentlich oder intern sein soll und dann auf "speichern" geklickt.

#### 1.9.4 Gruppeninformationen ansehen

Durch einen Klick auf einen Gruppennamen öffnet sich der Gruppenbildschirm. Siehe Abbildung 1.12.

Oben befindet sich der Mitgliedschaftsindikator, darunter die Gruppeninformationen, die für den eingeloggtten Nutzer sichtbar sind. Darauf folgen die Mitglieder der Gruppe. Ist der eingeloggte Nutzer auch Mitglieder der Gruppe, so werden unten die Nachrichten angezeigt, die an die Gruppe gesendet wurden.

### 1.9.5 Mitgliedschaft ein einer Gruppen beantragen

Um die Mitgliedschaft in einer Gruppe zu beantragen oder die Einladung in eine Gruppe zu bestätigen, muss der Gruppenbildschirm der entsprechenden Gruppe geöffnet und im Mitgliedsindikator auf “Mitgliedschaft beantragen“ oder “bestätigen“ geklickt werden.

### 1.9.6 Mitgliedschaft ein einer Gruppen löschen

Um die Mitgliedschaft in einer Gruppe zu löschen, muss der Gruppenbildschirm der entsprechenden Gruppe geöffnet und im Mitgliedsindikator auf “Mitgliedschaft kündigen“ geklickt werden. Mitgliedschaft verstecken. Mitgliedschaften in Gruppen können versteckt werden. Ist eine Mitgliedschaft in der Gruppe versteckt, so wird sie nur noch dem eingeloggten Nutzer und den Mitgliedern der Gruppe angezeigt. Zum Verstecken einer Gruppenmitgliedschaft muss der Gruppenbildschirm der entsprechenden Gruppe geöffnet und im Mitgliedsindikator unter “Mitgliedschaft verstecken?“ “Ja“ ausgewählt werden.

### 1.9.7 Nachrichten an Gruppen schicken

Gruppenmitglieder können Nachrichten an die gesamte Gruppe schicken in dem sie als Empfänger den Gruppennamen (Inklusive der “#“) eingeben.

## 1.10 Circles

Ein Nutzer kann seine Kontakte in verschiedene Circles aufteilen um dann verschiedene Informationen mit bestimmten Circles zuteilen. So kann der Nutzer zum Beispiel je einen Circle für seine Familie, seine Arbeitskollegen und seinen Sportverein erstellen und mit ihnen unterschiedliche Informationen teilen. Circles teilen sich einen Schlüssel und alle Nachrichten, die an einen Circle versendet werden, werden von allen Mitgliedern des Circles empfangen und können von diesen entschlüsselt werden. Die Circles eines Nutzers werden nach dem Einloggen stets rechts im Bild angezeigt. Siehe Abbildung 1.4 Das Circlemenü erscheint durch einen Klick auf “Circles“ im oberen Menü. Siehe Abbildung 1.13.

### 1.10.1 Circle erstellen

Ein neuer Circle wird erstellt, in dem im Circlemenü unter “Neuen Circle erstellen“ ein Name für einen Circle eingegeben und auf “erstellen“ geklickt wird. Der Name eines Circles darf noch nicht für einen anderen Circle verwendet werden und nur Buchstaben, Zahlen, Unterstriche und keine Umlaute enthalten. Entspricht der Name den Voraussetzungen, erscheint eine Meldung und der Circle wird im rechten Bildschirmbereich angezeigt.

**Circles:**  
Neuen Circle erstellen:  
Circle

Personen zu Circles hinzufügen:  
@Testcricle

Abbildung 1.13: pribook.com: Circlemenü

### 1.10.2 Nutzer zu einem Circle hinzufügen

Im Circlemenü wird unter “Person zu Circle hinzufügen“ in der Drop-down-Liste der entsprechende Circle ausgewählt und dann das Pseudonym des Nutzers in die Textbox eingetragen und auf “hinzufügen“ geklickt. Wenn das Hinzufügen erfolgreich war, erscheint das Pseudonym des hinzugefügten Nutzer im entsprechenden Circle auf der rechten Seite.

### 1.10.3 Einen Circle löschen

Um einen Circle zu löschen, muss man mit dem Mauszeiger über den Circle gehen, dann erscheint oben links im Circle ein kleines “x“. Durch einen Klick auf dieses x wird der Circle nach einer Sicherheitsabfrage gelöscht.