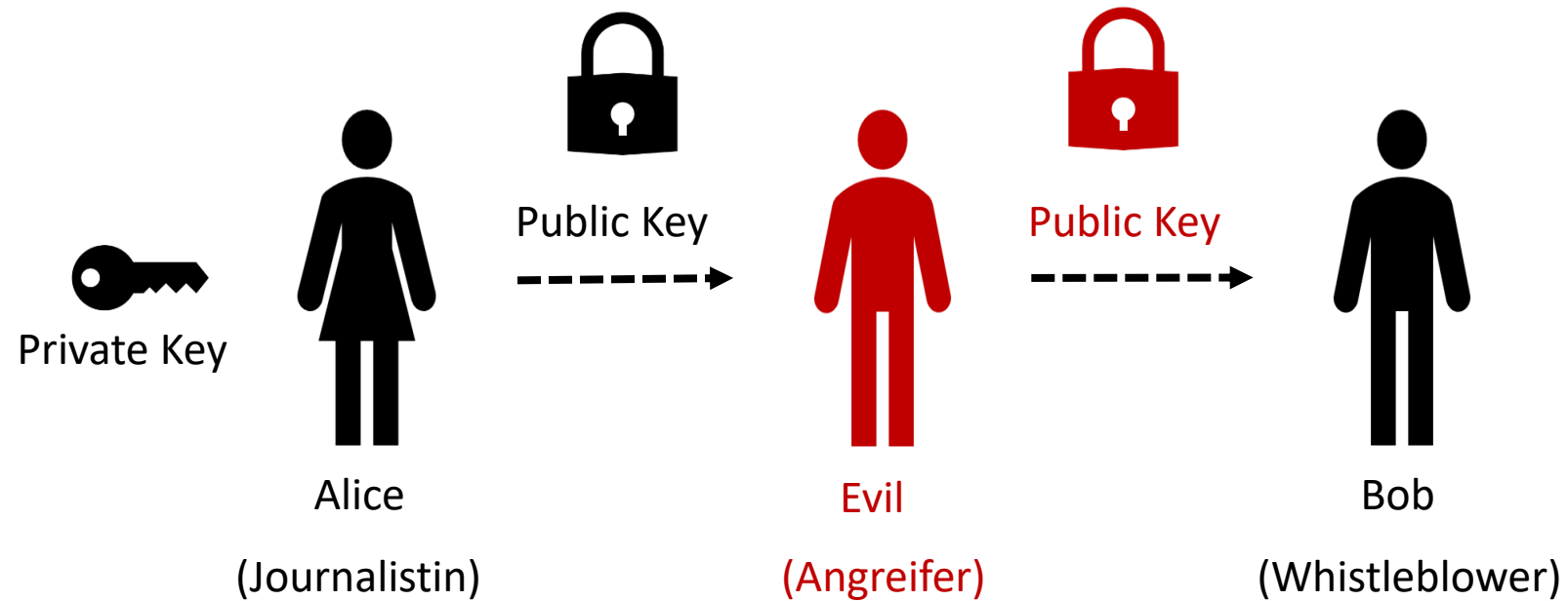


Letterbox

Sichere E-Mails für Nicht-Informatiker

Worum geht es ?



Ausgangsproblem

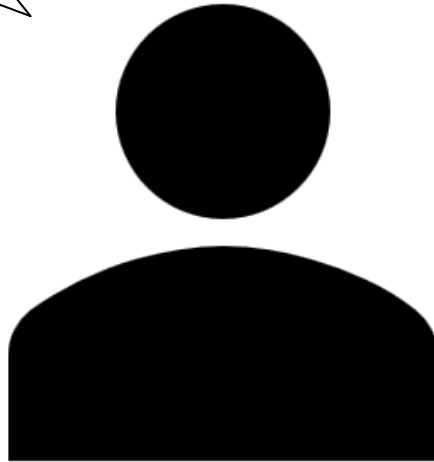
Technisch ungenau!



Unverständlich!

Persona: Alice

Die Nachrichten
meiner Kontakte müssen
geheim bleiben!
Sind die Nachrichten sicher?



- Journalistin
- Steht mit Whistleblower im Kontakt
- Motiviert zu verschlüsseln
- Kein technischer Hintergrund

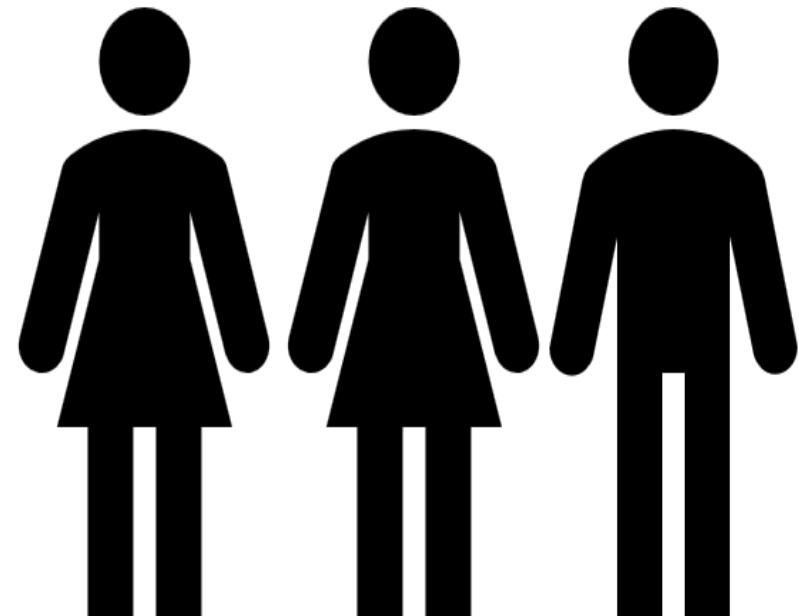
Die EntwicklerInnen: Wir

Asymmetrische Verschlüsselung
Verifikation
Man in the middle

Vertraulichkeit
Authentifizierung

Public Key
Private Key
Signaturen

- Angehende InformatikerInnen
- Absichten: verständlich entwerfen
- Denkweise: technisch







Low Fidelity Prototyp

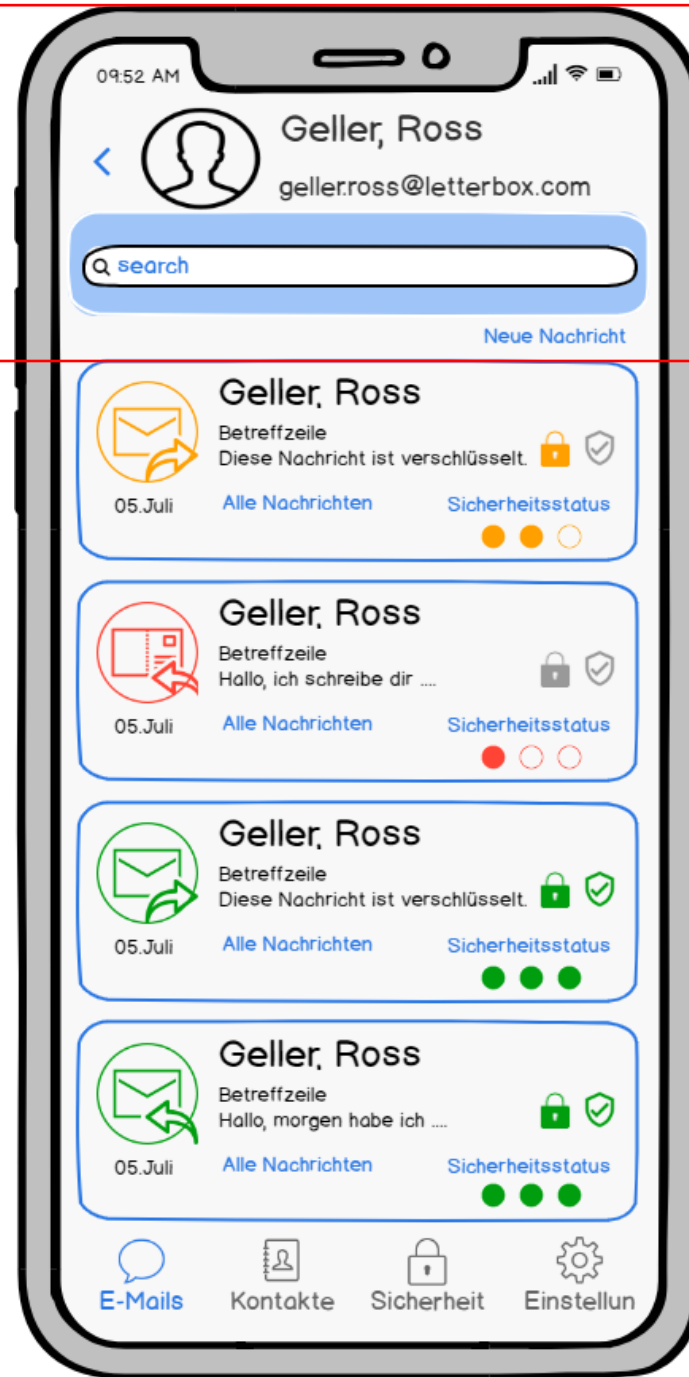


Unverständlich!

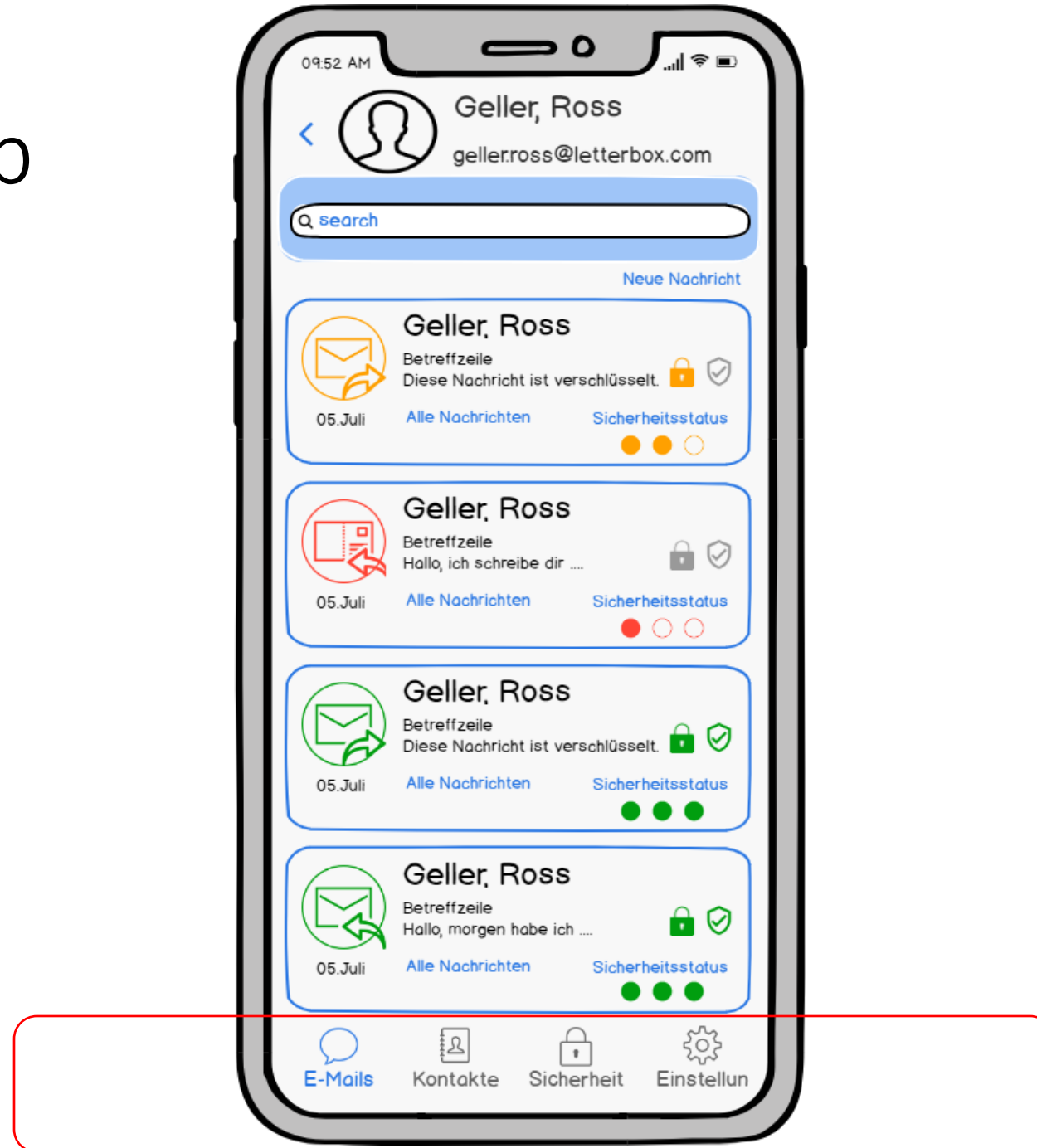
Key 1

Mails	Status
	Verifiziert ✓ Erste Nutzung min 10 Zweite Nutzung max 20
	Verifiziert
	Deprecated □ □ □ □
	Bad

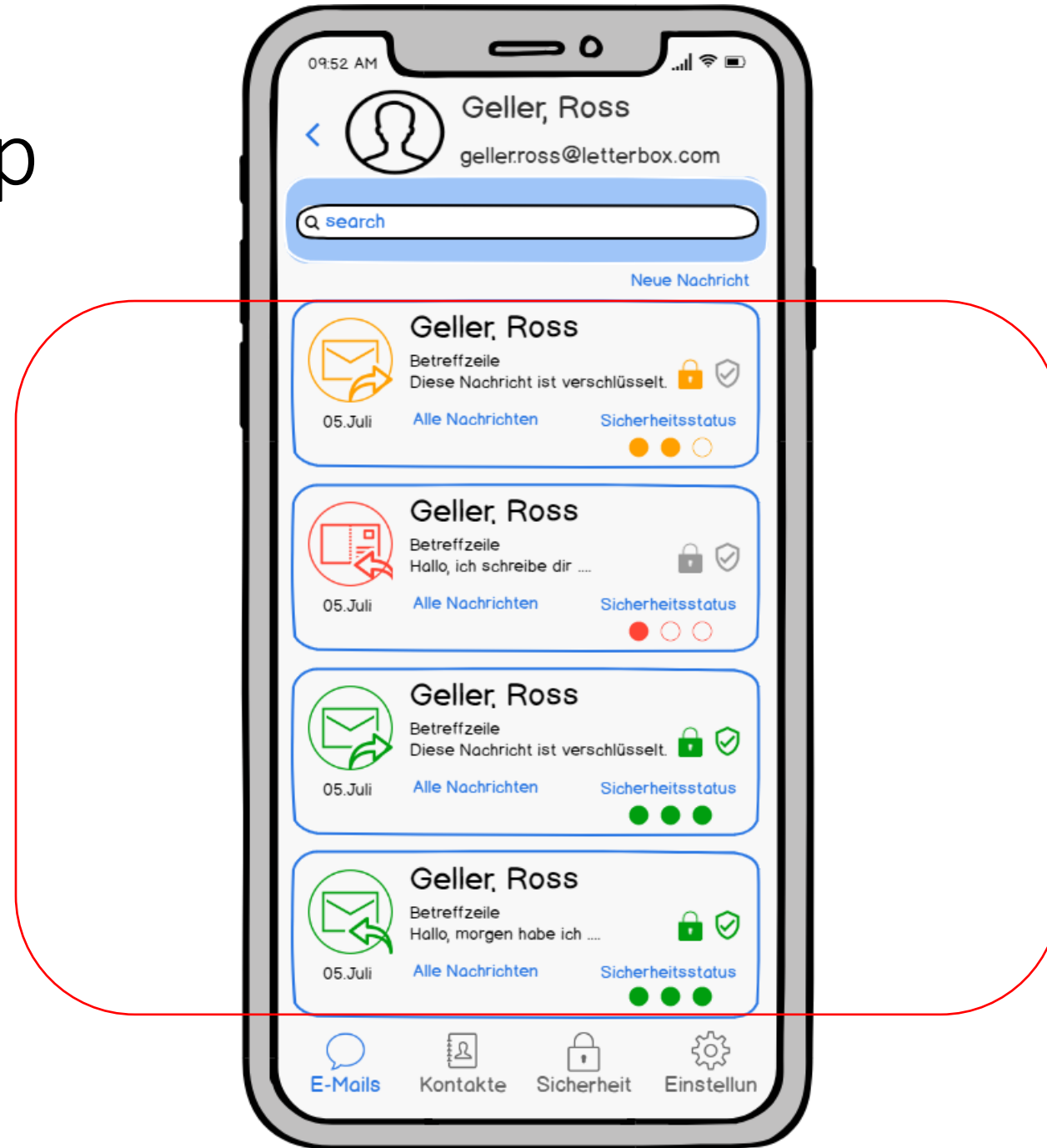
Hi-Fi Prototyp



Hi-Fi Prototyp



Hi-Fi Prototyp





 **Verschlüsselt**


 **Geller, Ross**
Betreffzeile
Diese Nachricht ist verschlüsselt.  
05. Juli [Alle Nachrichten](#) [Sicherheitsstatus](#)



 **Schlüssel nicht
verifiziert**


 **Green, Rachel**
Betreffzeile
Diese Nachricht ist verschlüsselt.  
27. Juni [Alle Nachrichten](#) [Sicherheitsstatus](#)



 **Mittel**

 **Tribiani, Joe**
Betreffzeile
Diese Nachricht ist verschlüsselt.  
22. Juni [Alle Nachrichten](#) [Sicherheitsstatus](#)


 **Hoch**

 **Unverschlüsselt**

 **Buffay, Phoebe**
Betreffzeile
Sehr geehrter Tester, wie...  
13. Apr. [Alle Nachrichten](#) [Sicherheitsstatus](#)


 **Gering**

Ausblick

- Features
 - Signaturen
 - Keys im Detail anzeigen
 - Verifikation explizit pro Key, nicht pro Nutzer
- Gestaltung verbessern
 - Hilfe erneut validieren
 - Unsicher und veraltet besser verständlich
 - Nutzung und Zweck der Historie

Fazit

- Perspektivwechsel
 - Wissen eines technisch unbedarften Users einschätzen
 - Hilfreich: mit Menschen testen
- Inhaltlicher Fokus
 - Ursprüngliches Thema: Schlüsselhistorienvergleich
 - Nötige Basis: verschlüsselte Nachrichten, umgesetzte Verifikation

Vielen Dank