SecMes

Bachelorarbeit

Secure Messaging: WhatsApp Alternative

Autor: Thomas Hütter

Betreuer: Ass.-Prof. Mag. Dr. Bernhard Collini-Nocker

Naturwissenschaftliche Fakultät
FB Computerwissenschaften
UNIVERSITÄT SALZBURG

Übersicht

- Einführung
  - Motivation
  - Aktuelle Systeme
  - Sicherheitsprobleme
  - Aufgabenstellung
- Umsetzung „SecMes“
  - Konzept
  - Implementation
- Live Demo

Motivation

"Der Zugriff auf die Informationen ist total"
[07.06.2013] - faz.net

"Experten ...
[17...

"NSA ENTWICKELT QUANTENCOMPUTER"
[03.01.2014] - nzz.ch

...ei WhatsApp"

...auf Mobilfunknetze: NSA kann fast alle Hand...
[14.12.2013] - spiegel.de

"Wird Merkel zu...
[24.10.2013]

"WhatsApp ist kaputt, richtig kaputt"
[18.09.2013] - sueddeutsche.de

...are zum Skandal"

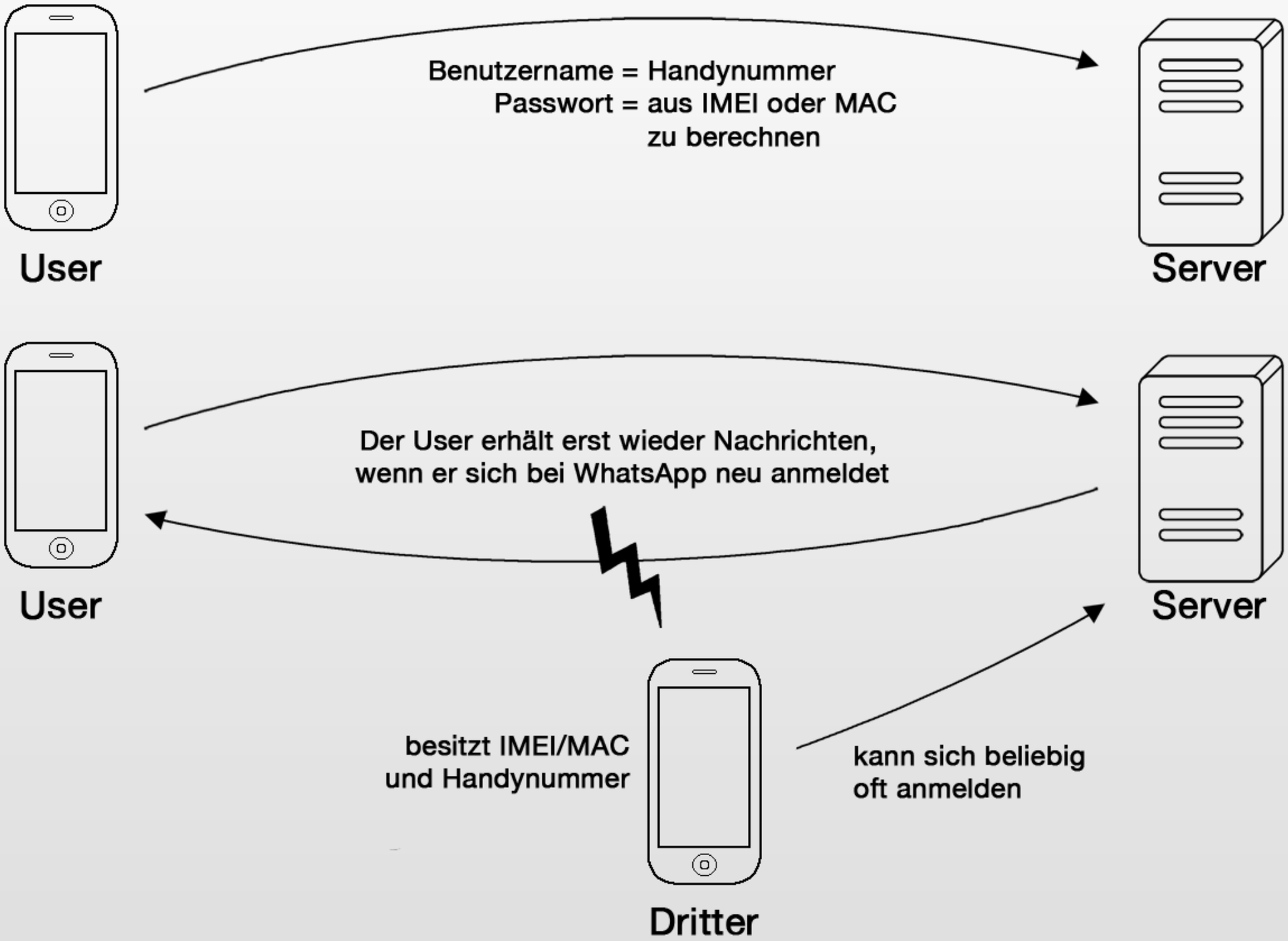
WhatsApp

- Allgemein
  - Veröffentlicht 2009, WhatsApp Inc.
  - Rekord 27 Milliarden Nachrichten/Tag
  - 300 Millionen Benutzer
- Funktionen
  - Gruppenchats
  - Fotos und Videos
  - Standort
  - Sprachnachrichten

WhatsApp

- Sicherheitsprobleme zu Beginn
  - bis August 2012, keine Nachrichtenverschlüsselung
  - Authentifizierung
  - Passworterstellung

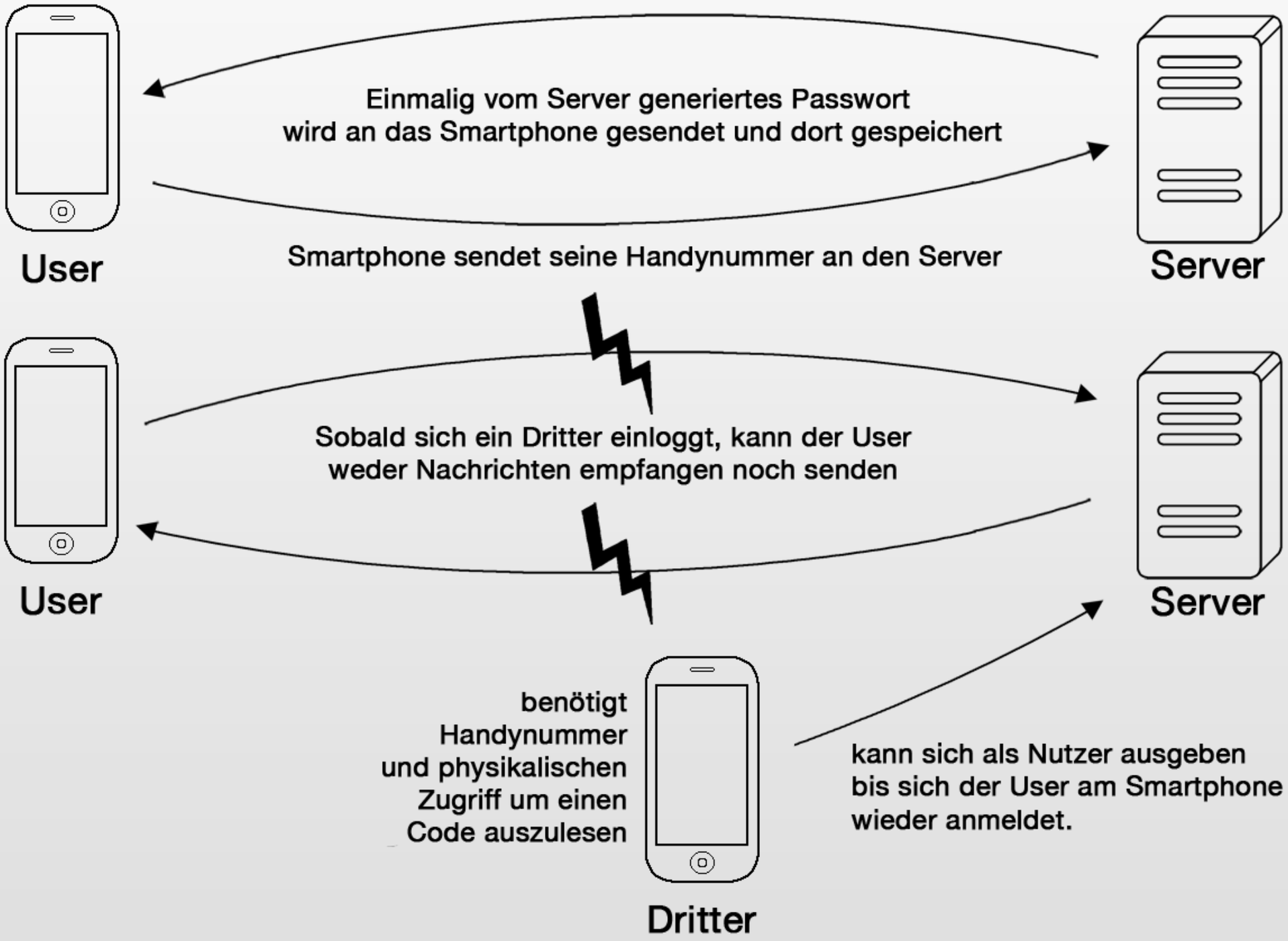
WhatsApp


Benutzername = Handynummer
Passwort = aus IMEI oder MAC
zu berechnen
User
Server
Der User erhält erst wieder Nachrichten,
wenn er sich bei WhatsApp neu anmeldet
User
Server
besitzt IMEI/MAC
und Handynummer
kann sich beliebig
oft anmelden
Dritter

WhatsApp

- Sicherheitsprobleme (Stand Mai 2013)
  - RC4 Verschlüsselung der Nachrichten
  - Priyanka
  - neue Passworterstellung

WhatsApp


Einmalig vom Server generiertes Passwort
wird an das Smartphone gesendet und dort gespeichert
Smartphone sendet seine Handynummer an den Server
User
Server
Sobald sich ein Dritter einloggt, kann der User
weder Nachrichten empfangen noch senden
User
Server
benötigt
Handynummer
und physikalischen
Zugriff um einen
Code auszulesen
kann sich als Nutzer ausgeben
bis sich der User am Smartphone
wieder anmeldet.
Dritter

Threema

- Allgemein
  - Kasper Systems GmbH
- Sicherheitskonzepte
  - 2 Verschlüsselungsschichten
    - Ende zu Ende zwischen Teilnehmern
    - zwischen App und Server
  - 3 stufige Authentifizierung
    - ID wird eingegeben
    - Abgleich mit Kontakten
    - Persönliches Scannen des QR-Codes

Wickr

- Allgemein
  - Gruppe aus Sicherheitsexperten
- Selber Funktionsumfang wie WhatsApp
- Sicherheitskonzepte
  - Vielzahl an Verschlüsselungsstandards
  - Selbstzerstörungsfunktion

Sicherheitsprobleme

- Nachrichtenverschlüsselung
- Anonymität
- Integrität
- Authentifizierung

Aufgabenstellung

Unter Betrachtung der bisher analysierten Daten, soll ein sicheres System zur Nachrichtenübertragung konzeptioniert und implementiert werden. Das Programm soll als systemunabhängige WebApp, basierend auf HTML5, realisiert werden.

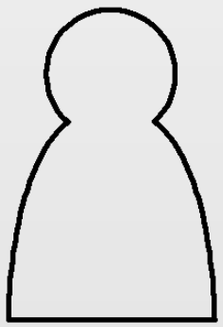
Implementierung

Sicherheitsanforderungen

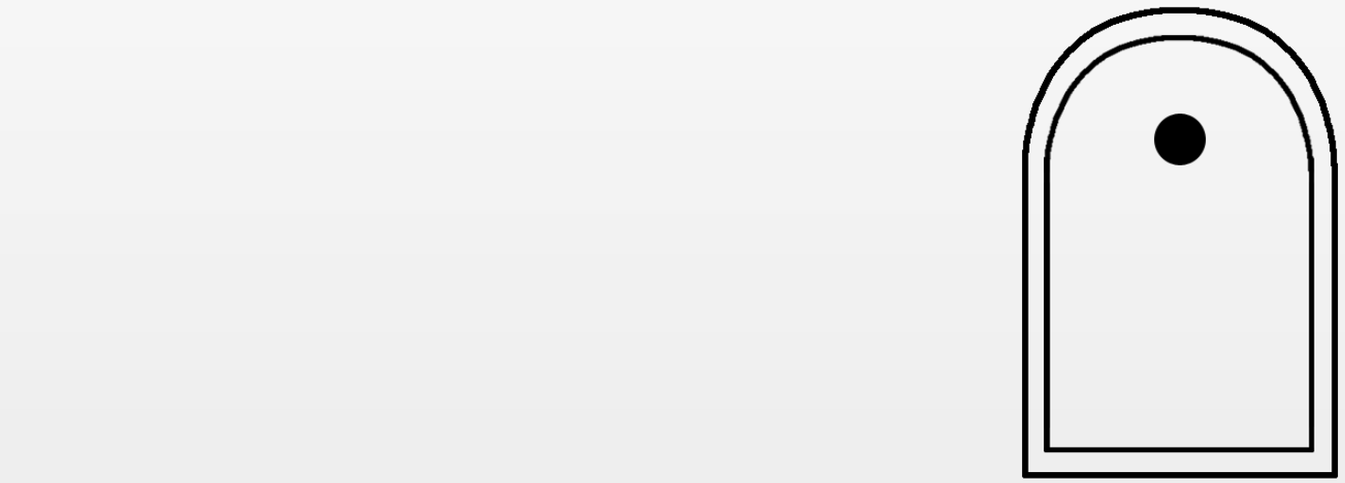
- Kein Zugriff auf lokale Daten
- Keine privaten Daten
- Guter Verschlüsselungsstandard
- Schlüsselmanagement
- Authentifizierung
- Keine permanente Speicherung von Daten

Konzept

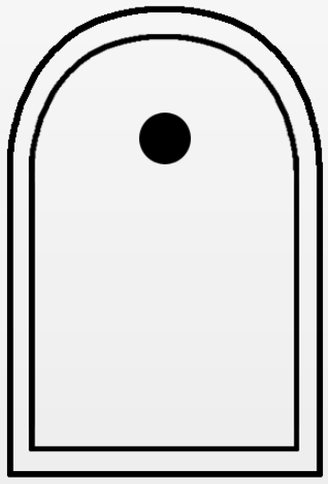
Konzept

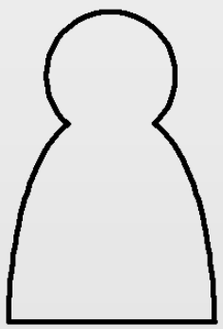


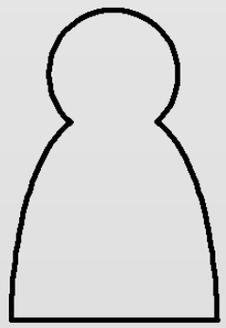
Konzept

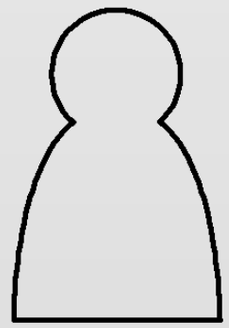


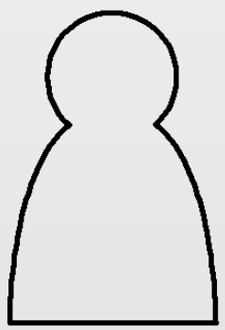
Konzept



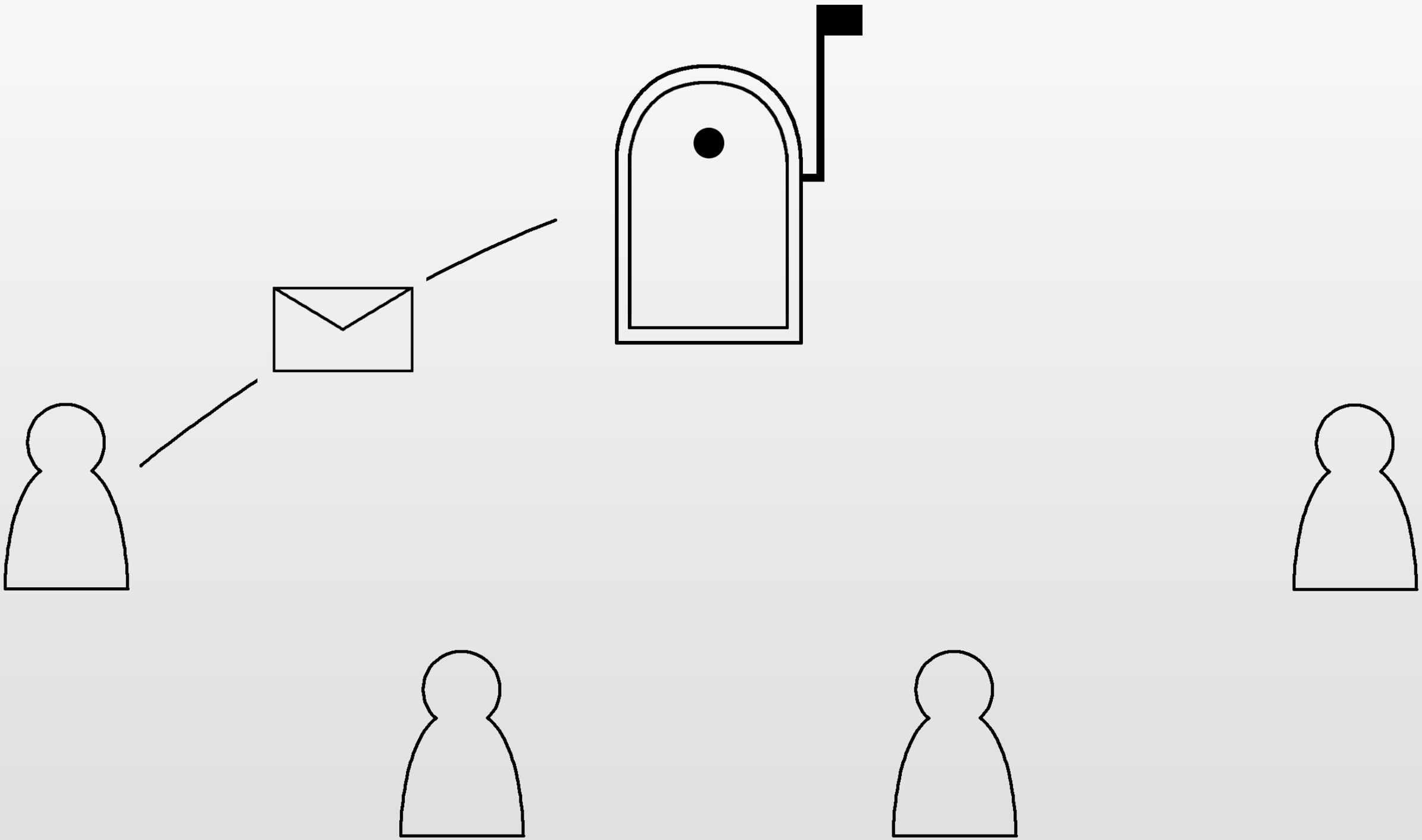




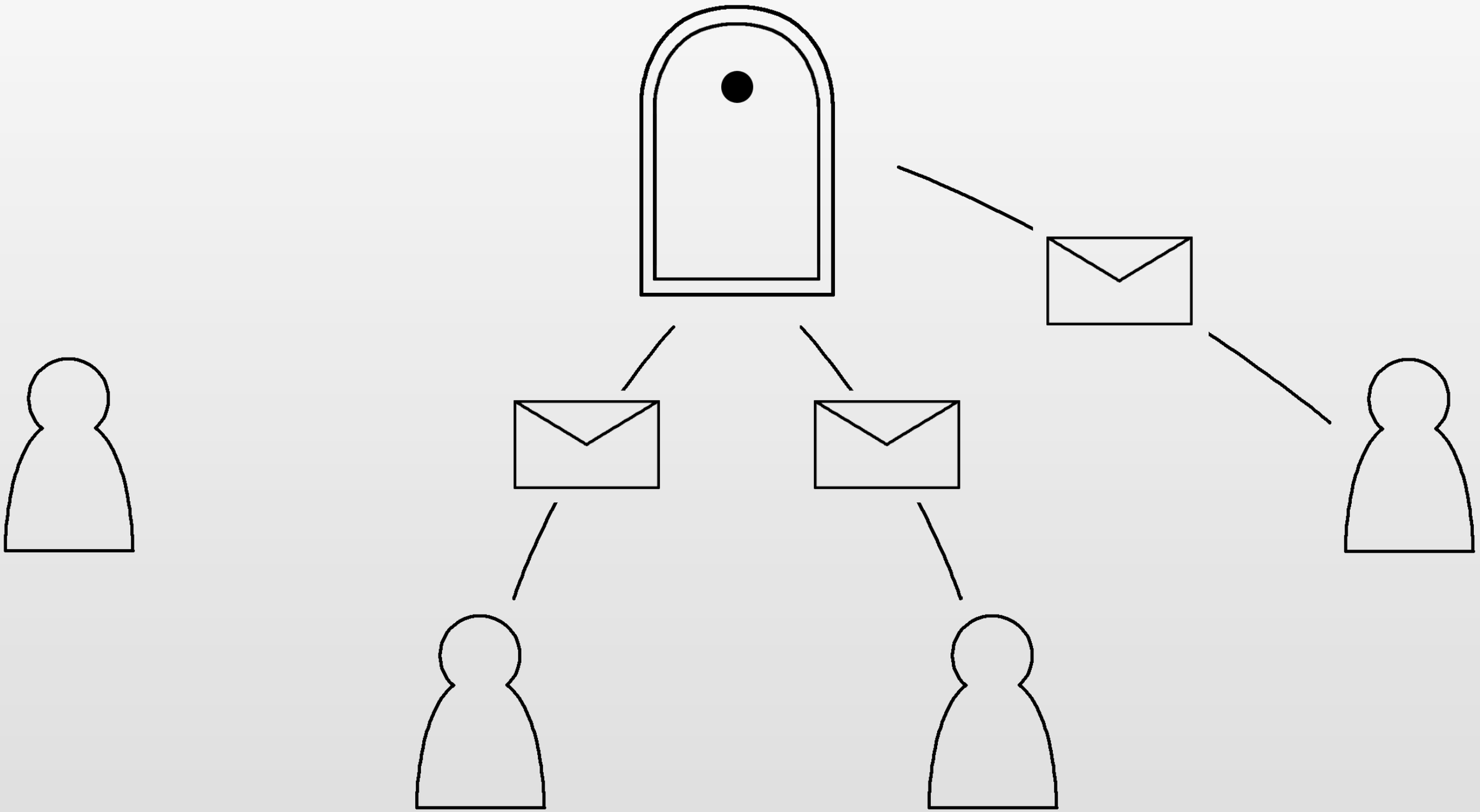




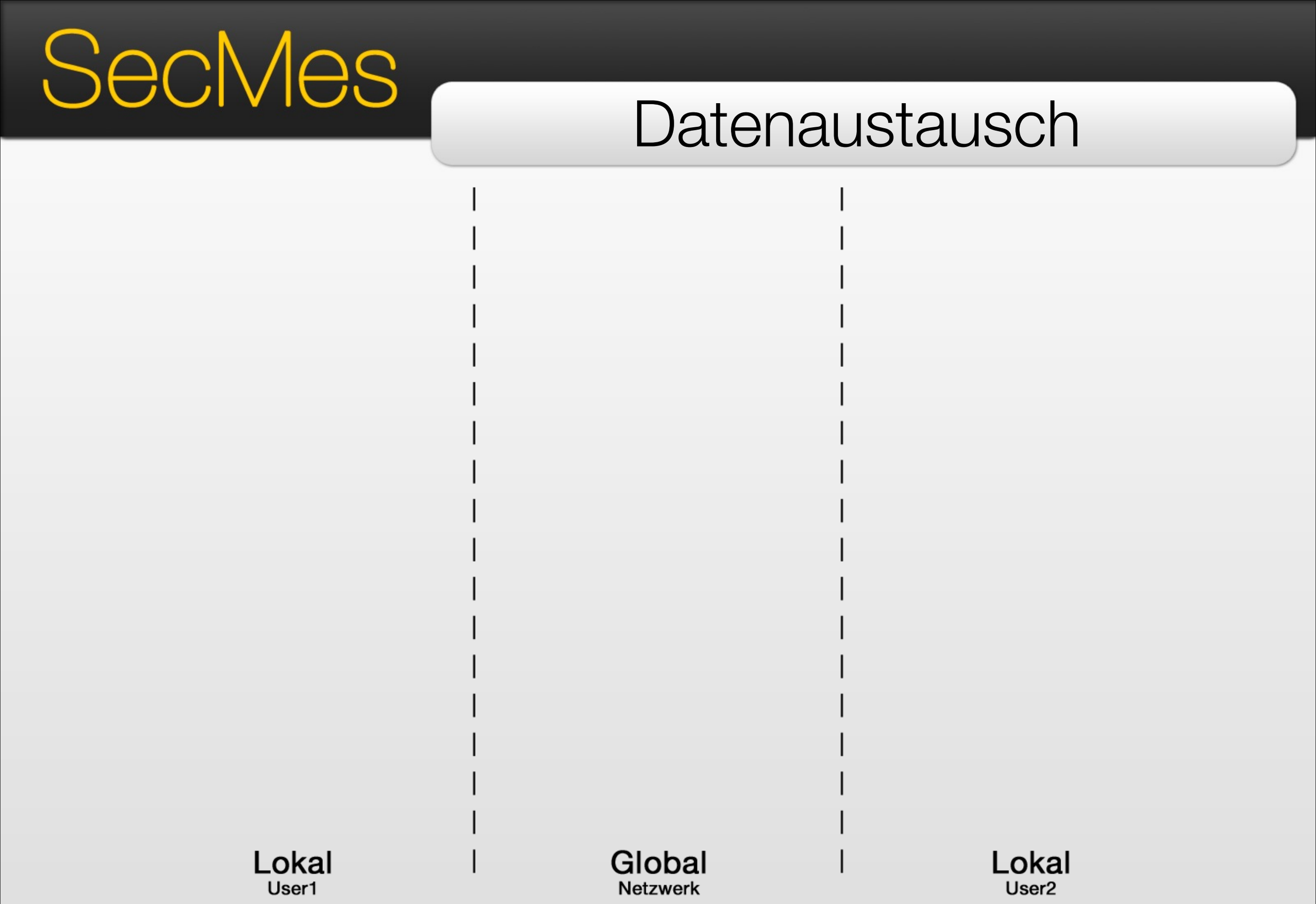
Konzept



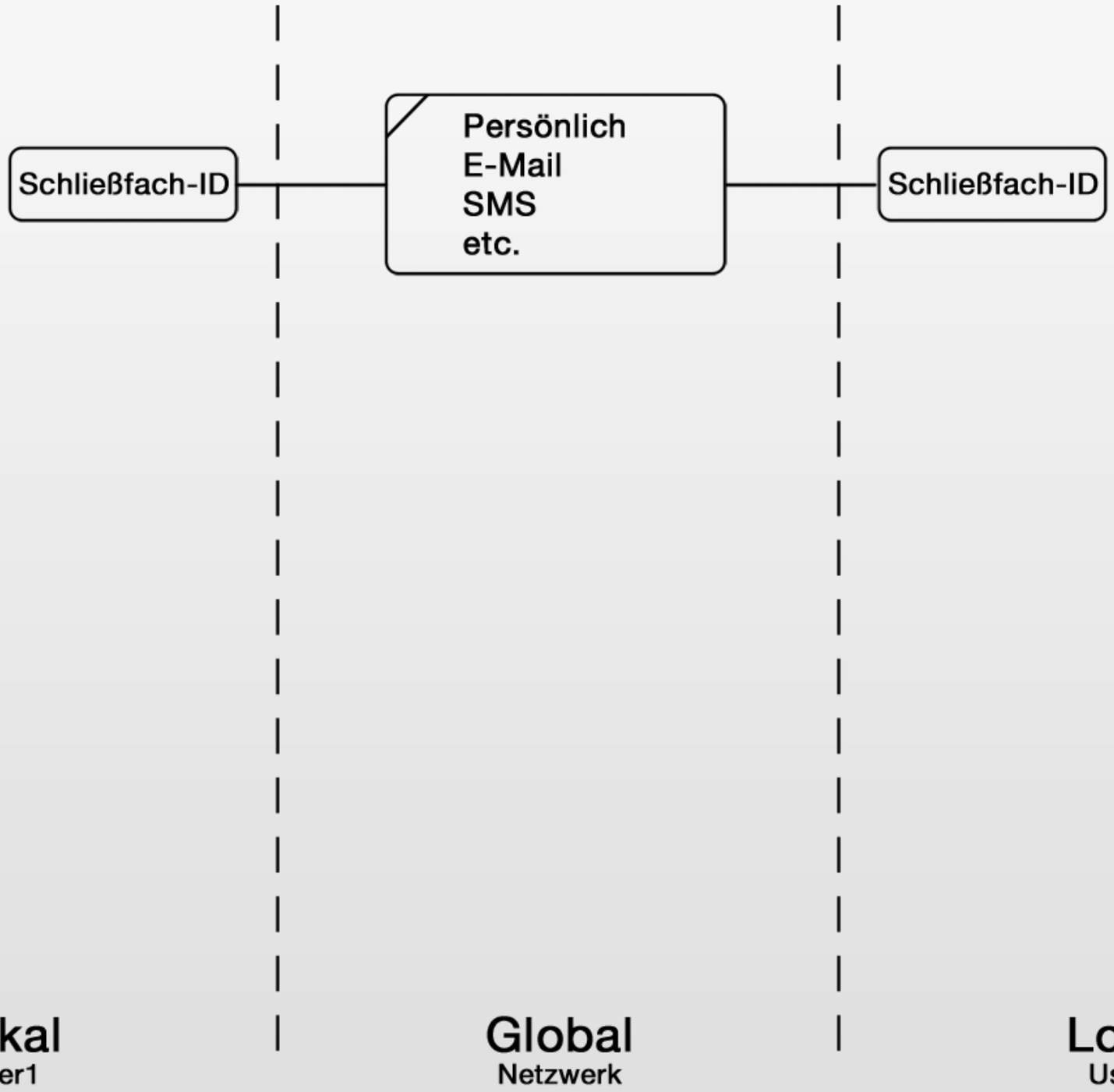
Konzept



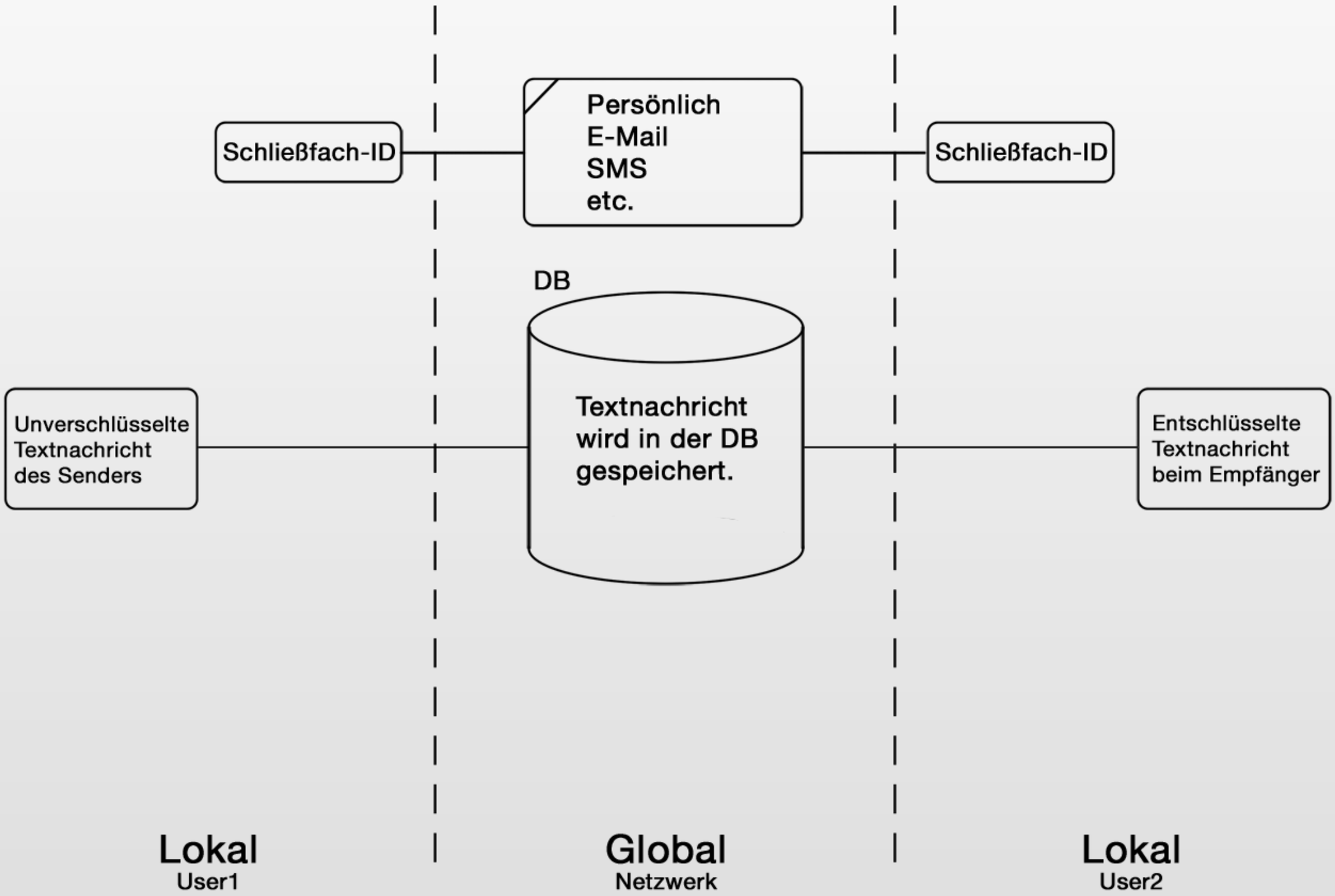
Datenaustausch



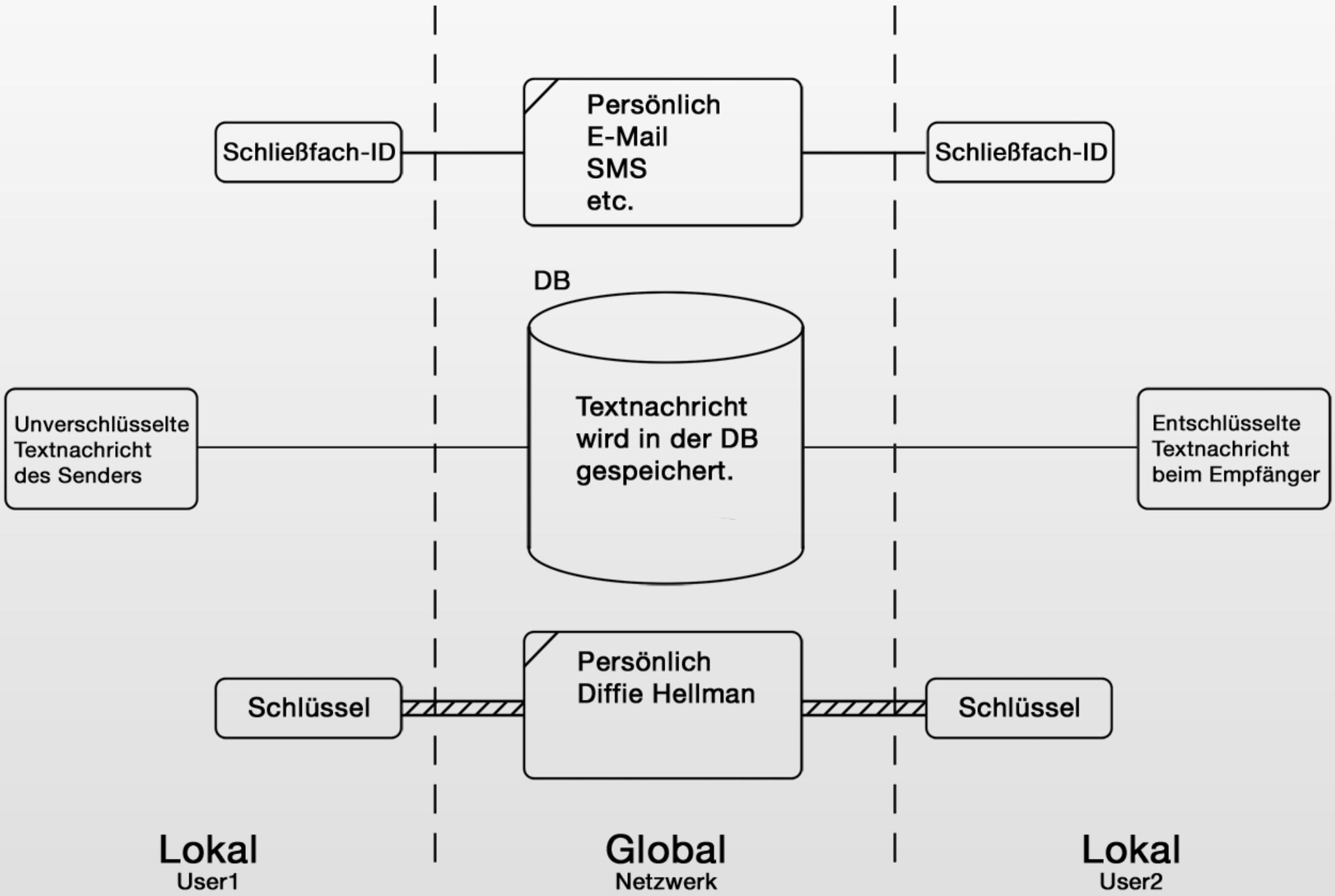
Datenaustausch



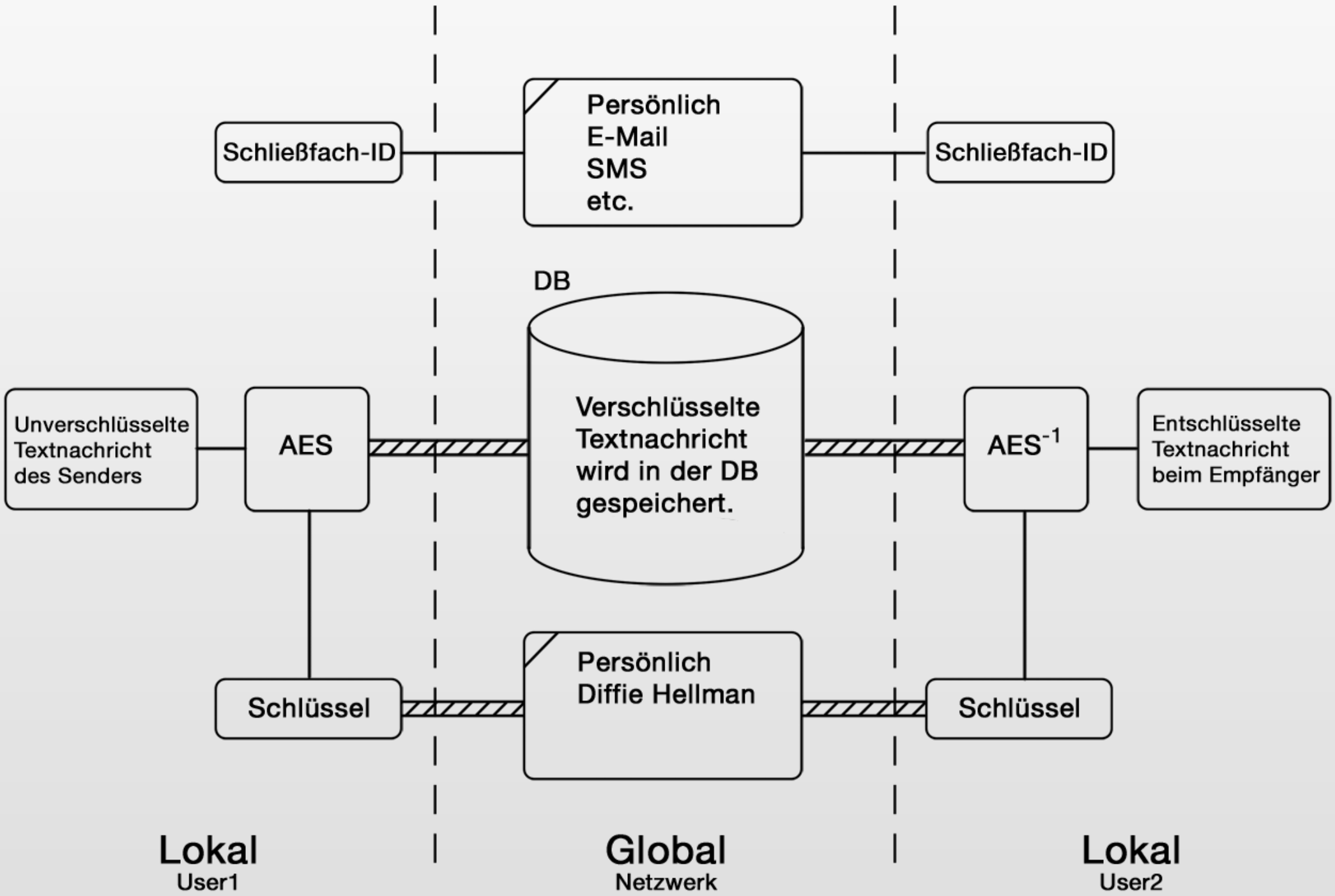
Datenaustausch



Datenaustausch



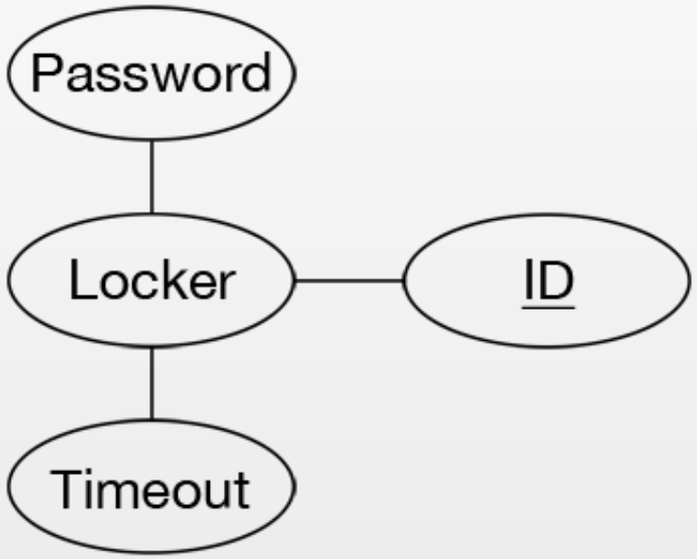
Datenaustausch



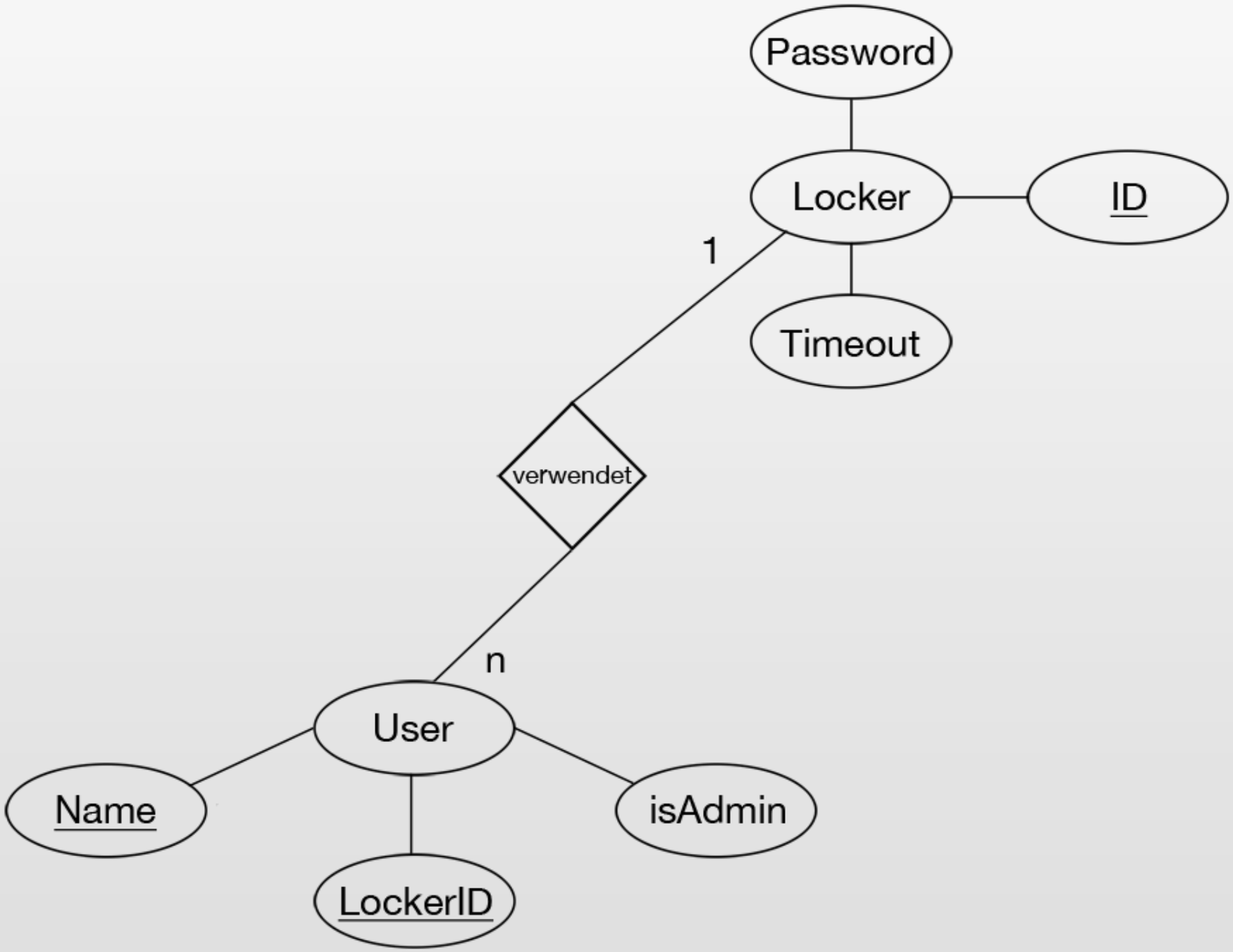
Implementierung

- Datenbank
  - ER - Modell
  - Timeout - Funktion
- Schlüsselstellen
  - Diffie-Hellman
  - Weitere Funktionen

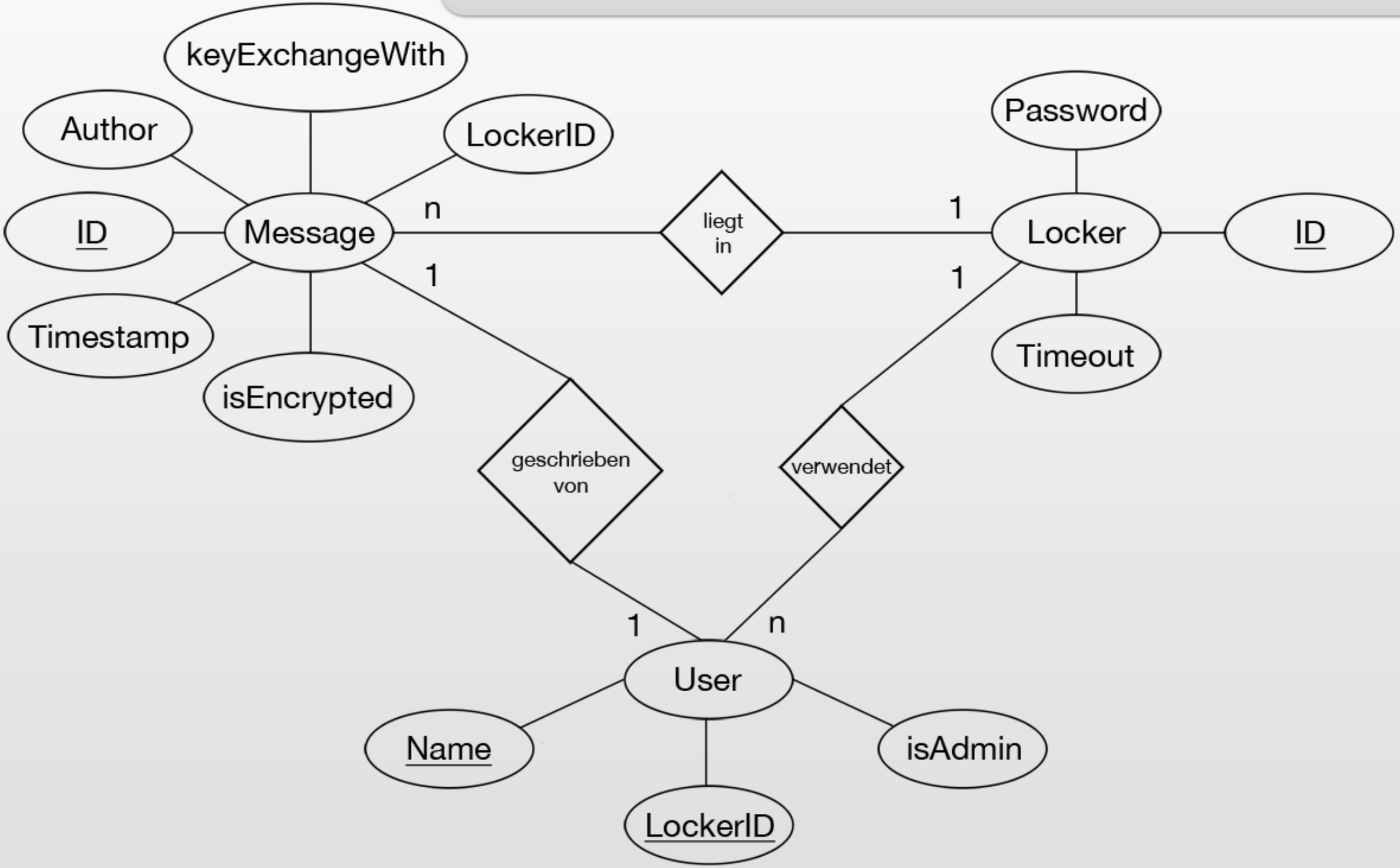
ER - Modell



ER - Modell


Password
Locker
ID
1
Timeout
verwendet
n
User
Name
isAdmin
LockerID

ER - Modell


keyExchangeWith
Author
LockerID
Password
ID
Message
n
liegt
in
1
Locker
ID
1
1
Timestamp
Timeout
isEncrypted
geschrieben
von
verwendet
1
n
User
Name
isAdmin
LockerID

Timeout-Funktion

- MySQL
  - Events

```
CREATE EVENT myevent
    ON SCHEDULE AT CURRENT_TIMESTAMP + INTERVAL 1 HOUR
    DO
        UPDATE myschema.mytable SET mycol = mycol + 1;
```

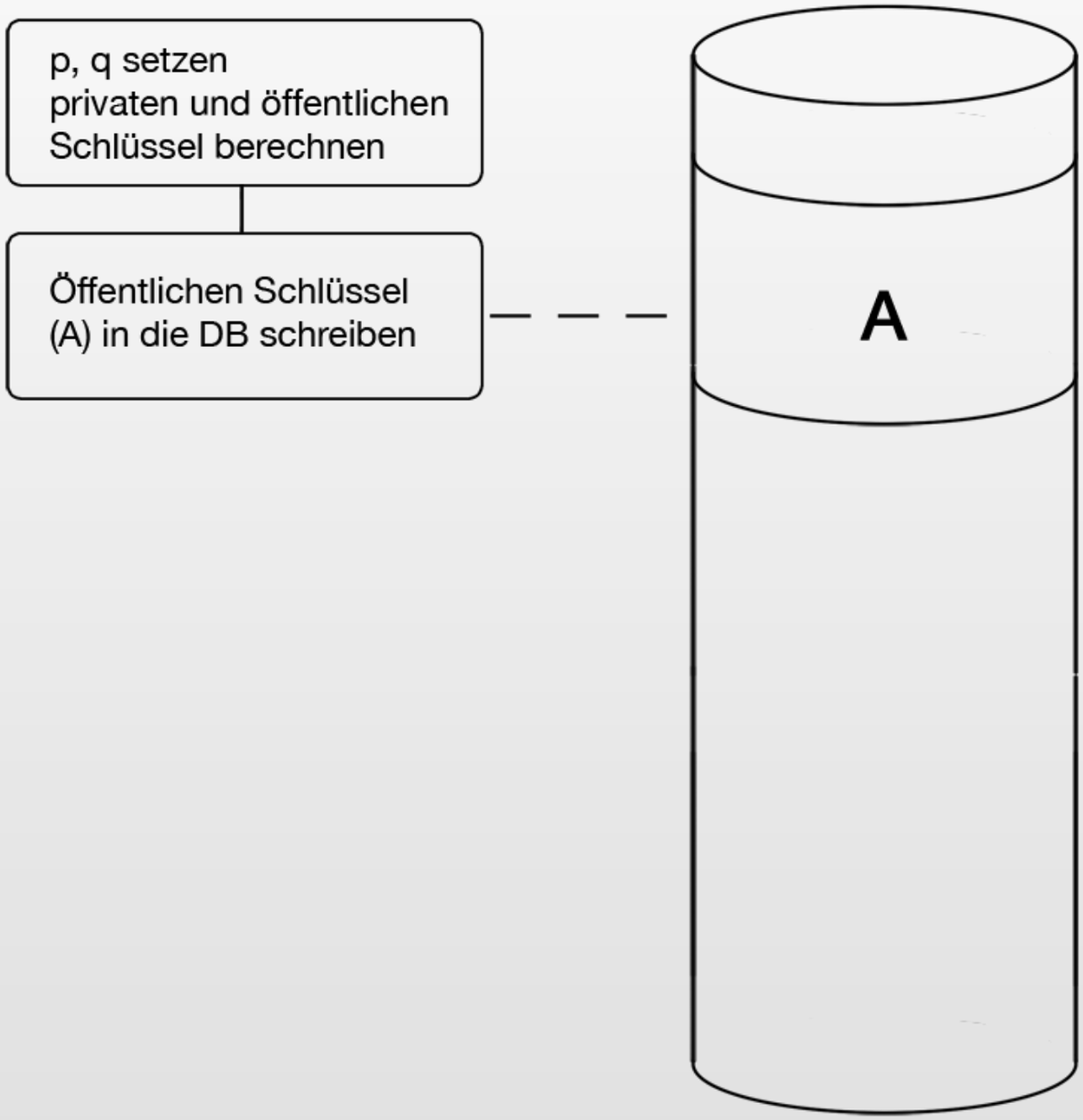
Diffie-Hellman

Benutzer A
Admin

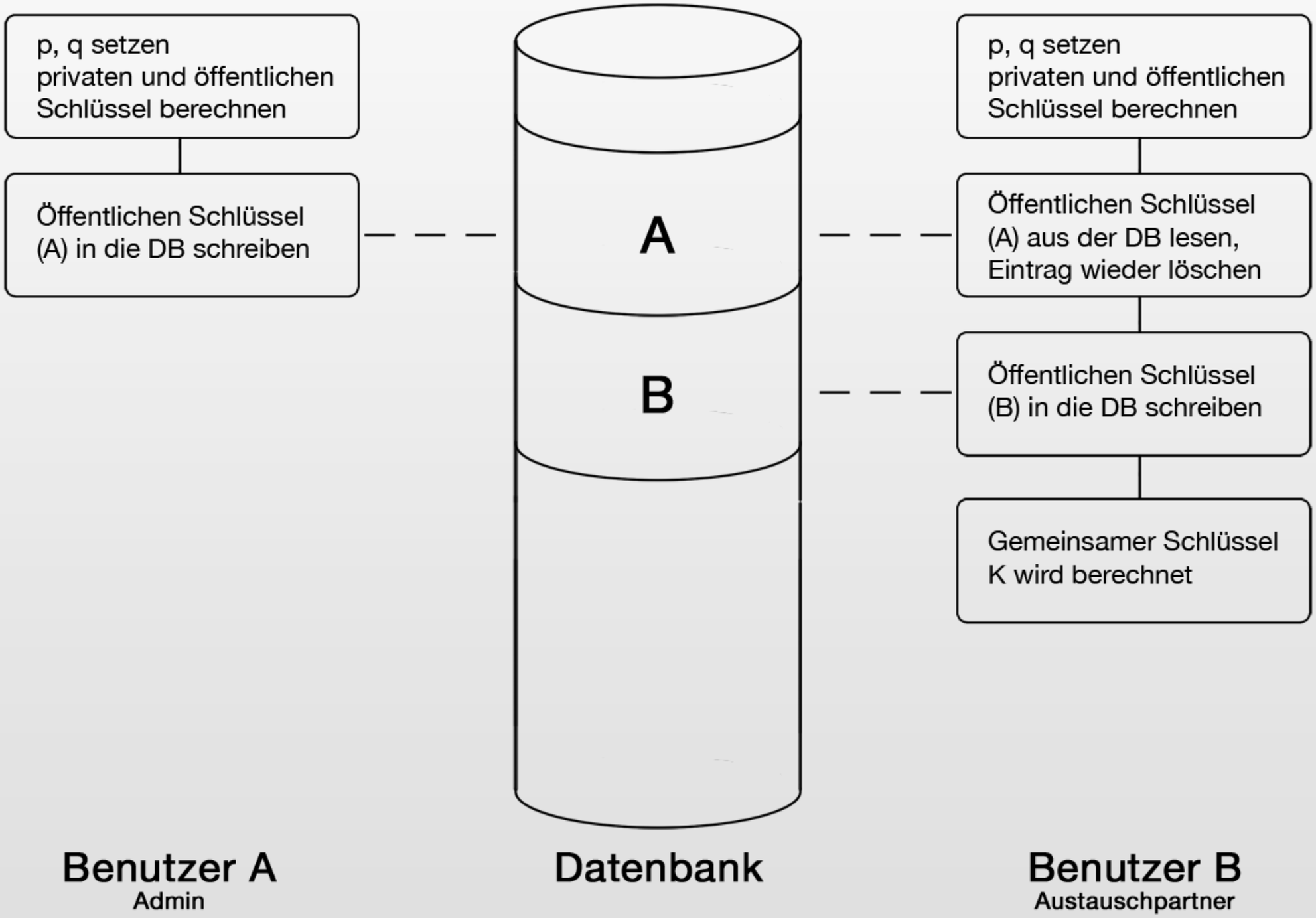
Datenbank

Benutzer B
Austauschpartner

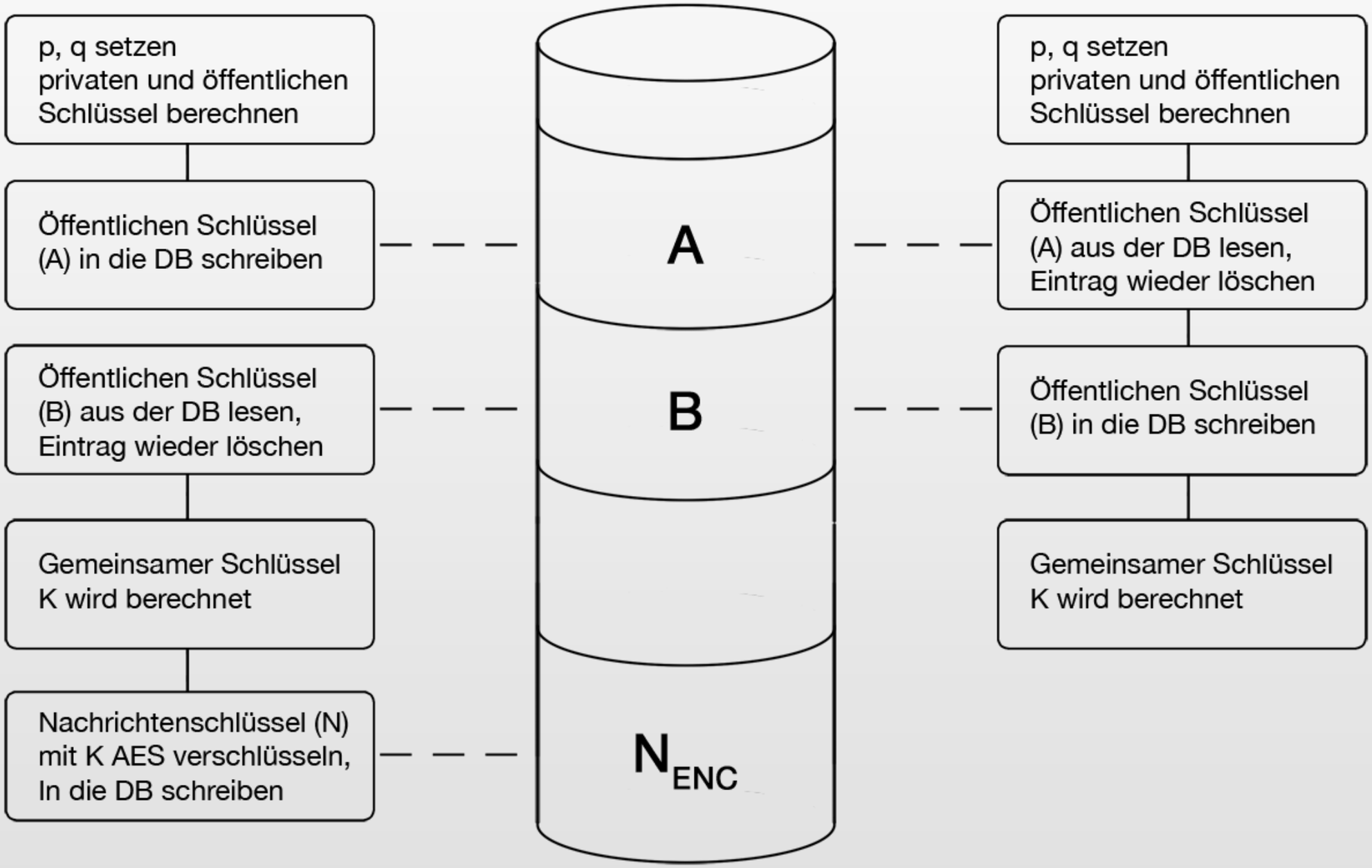
Diffie-Hellman



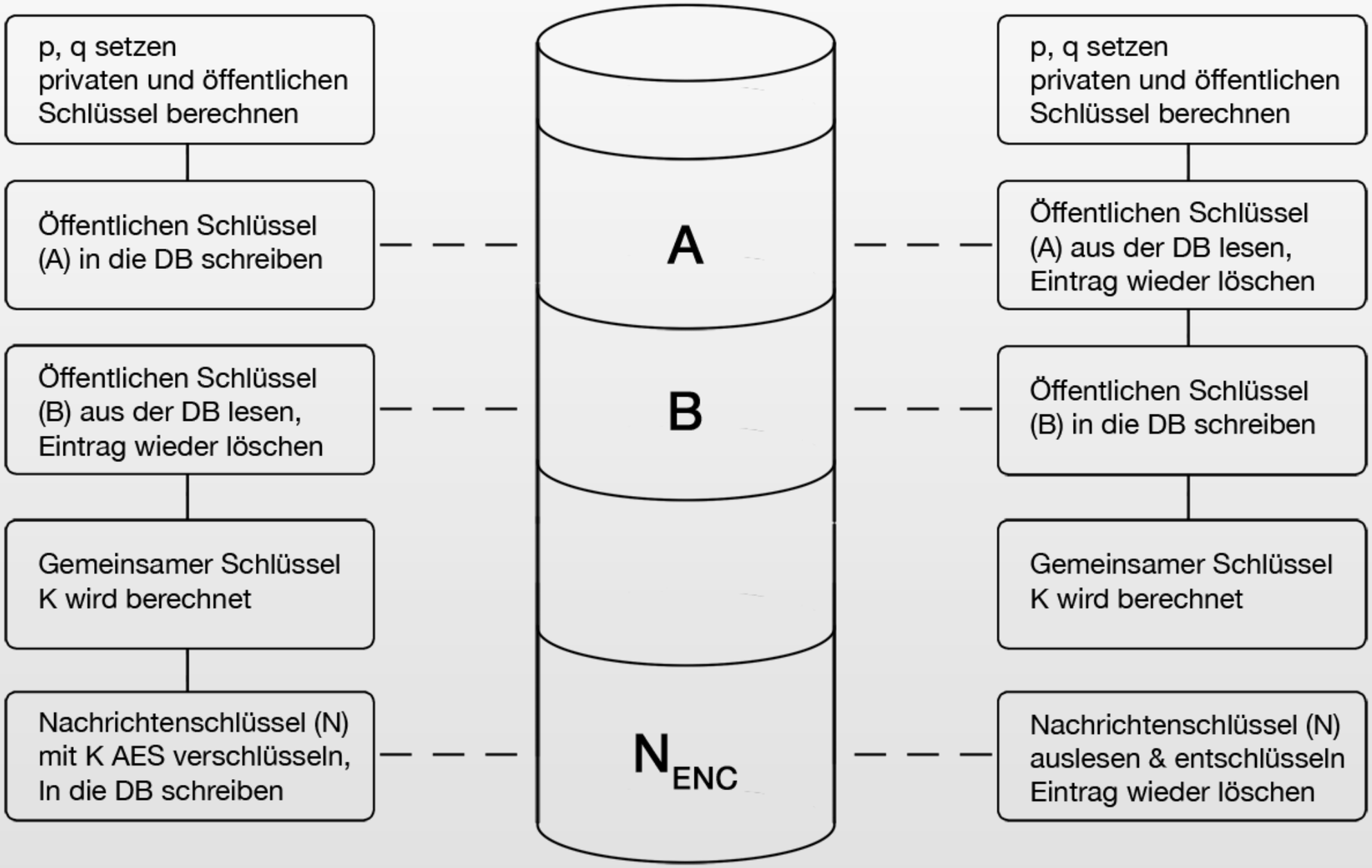
Diffie-Hellman



Diffie-Hellman



Diffie-Hellman



Weitere Funktionen

- Adminfunktionen
  - Schlüsselaustausch
  - Schließfach löschen
  - Nachrichtenverlauf löschen
- Nachrichtenabfrage
  - Polling
- Datenerhaltung
  - POST Übergabe
  - HTTPS

Verwendete Software

- jQuery
- jQuery Mobile
- Zend
  - Diffie-Hellman
- Movable-Type
  - AES
  - SHA 256
- XAMPP
  - Apache Webserver
  - MySQL

LIVE DEMO

Vielen Dank!

Haben Sie noch Fragen?