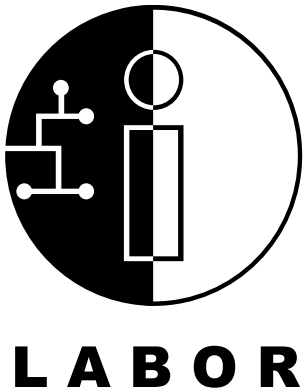
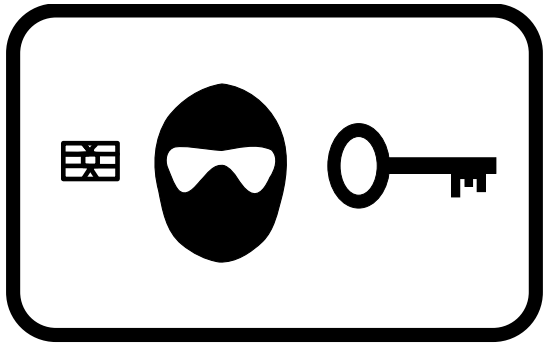
AnonAccess

Sören Heisrath Daniel Otte





27. Dezember 2007

Unser Schlüsselproblem:

- viele Leute
- wenig Schlüssel
- wenig Geld

Erste Überlegungen

- Mechanische Schlüssel kann man einfach nachmachen
- Schliesssysteme sind teuer
- $\Rightarrow$ wir müssen was Eigenes machen

Mittel & Wege

- Speicherkarten oder SmartCards
- Microcontroller-Plattform

Kostenabschätzung

- Speicherkarten kosten $\leq$ 1 Euro pro Stück
- (geeigneter) Microcontroller $\leq$ 10 Euro
- Restliche elektronik ca. 10 Euro

Elegante Lösung

- einfach zu realisieren
- günstig
- sicher

Anonymität

Karten sollen anonym wie Schlüssel sein

Prüfsummen

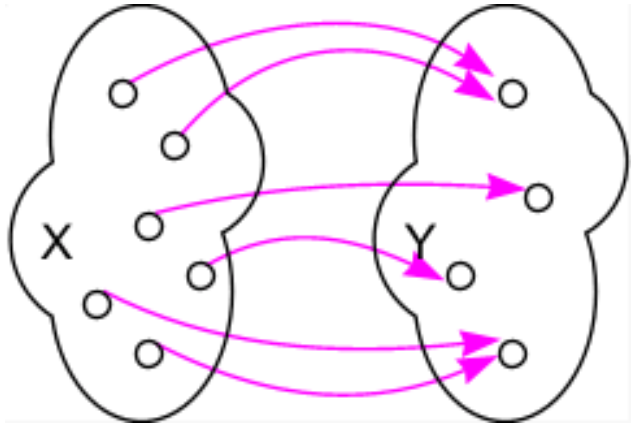
z.B. eine Quersumme üeber eine Zahl.

Problem

Zu einer gegebenen Prüfsumme kann jeder eine valide andere Zahl generieren.

Hashfunktionen

Hashfunktionen sind Einweg-Funktionen
die eine beliebig grosse Datenmenge
auf eine kleinere Datenmenge abbilden.

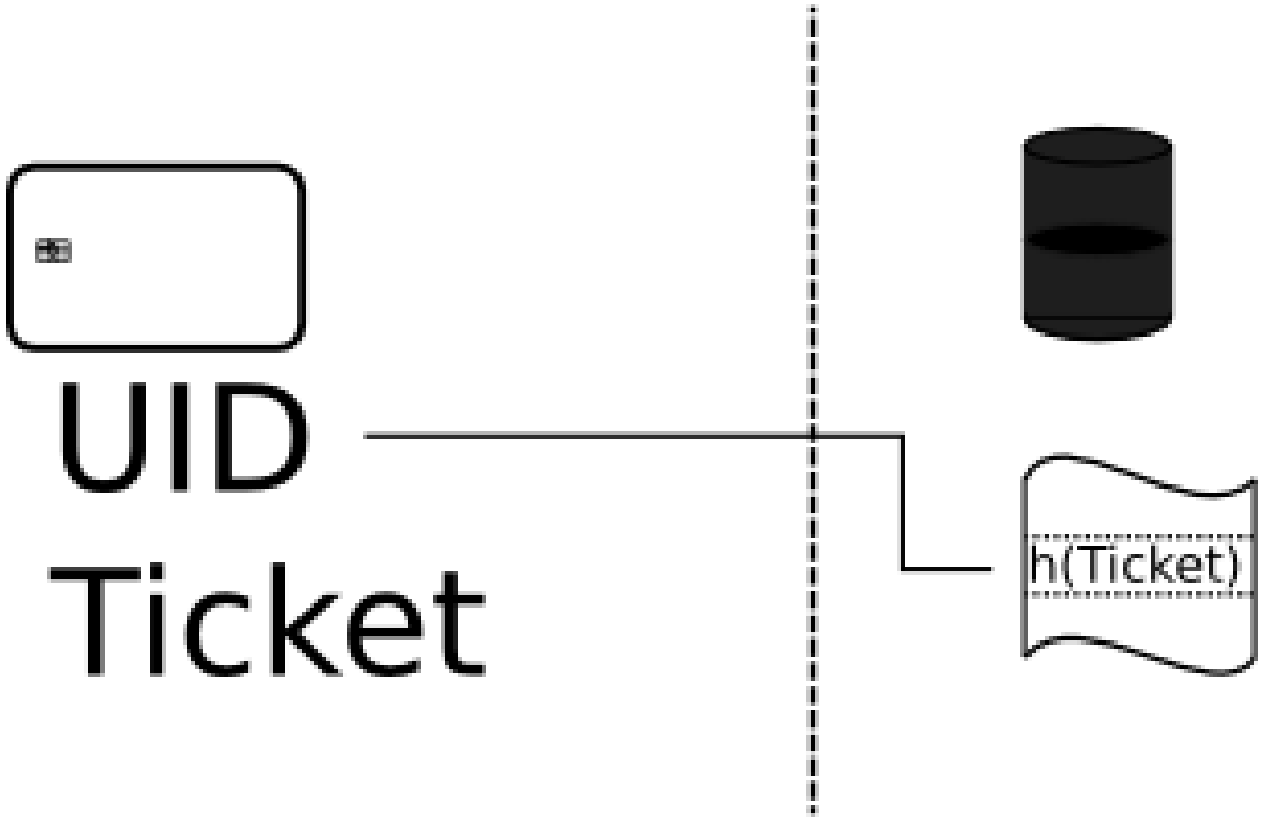


Hash-MACs

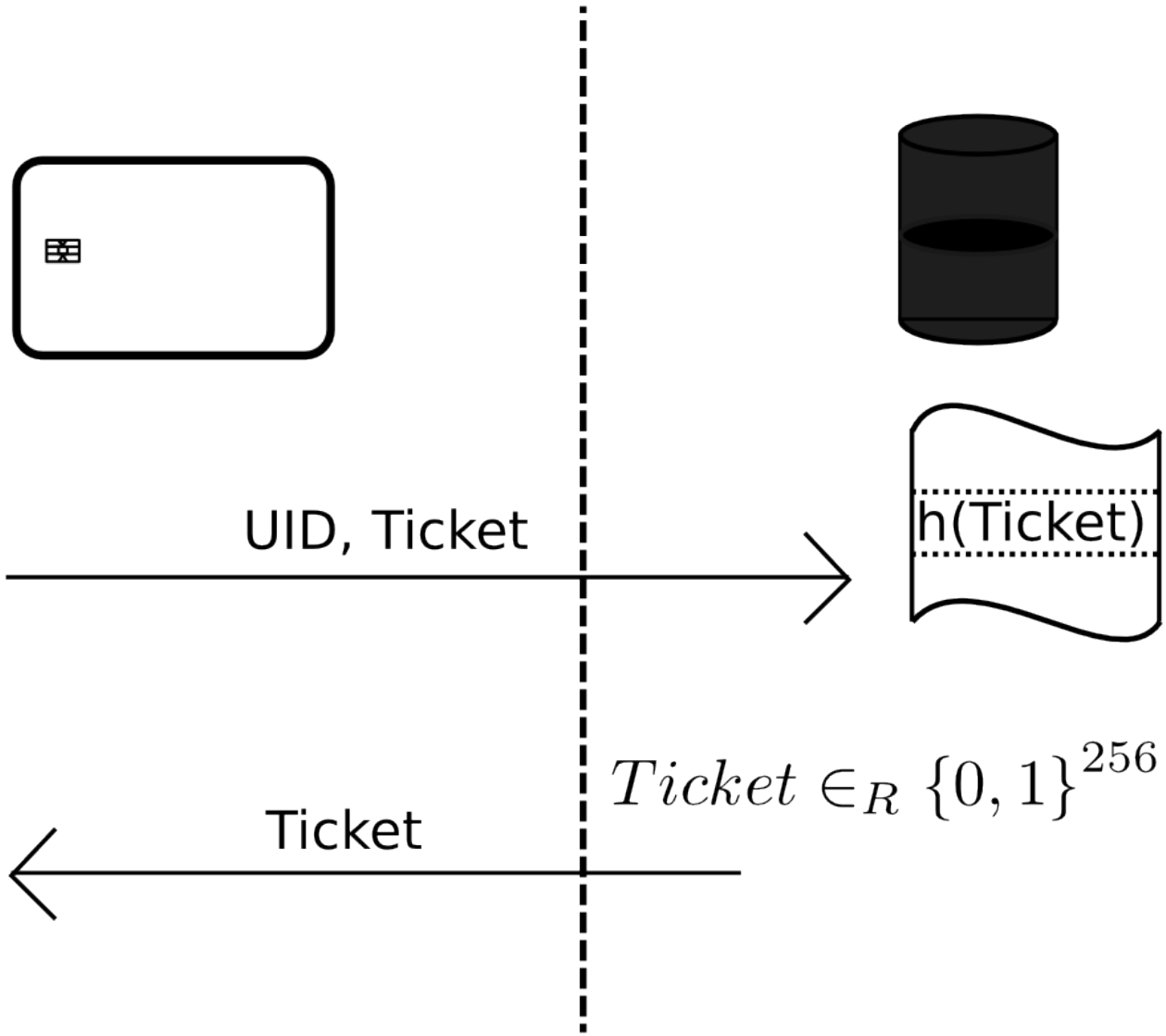
Hash-MACs sind Hash-funktionen zur Authenfikation von Nachrichten.

$$HMAC_k(msg) = hash((k \oplus opad) \parallel hash((k \oplus ipad) \parallel msg))$$

Ansatz 1



Ansatz 1 – Ablauf



Ticket-DB Struktur

Struktur eines Eintrags in der Ticket-DB:

flags	Flags (siehe unten)
nickname	Nickname (wenn Speicherung gewünscht)
ticketmac	MAC vom Ticket

Struktur der Flags:

exist	Benutzer existiert
admin	Benutzer hat Admin Status
locked	Benutzer ist gesperrt
notify_lostadmin	Benutzer hat Admin Status verloren
anonymous	Benutzer hat keinen Namen hinterlegt

Ansatz 1 – Probleme

Ansatz 1 – Probleme

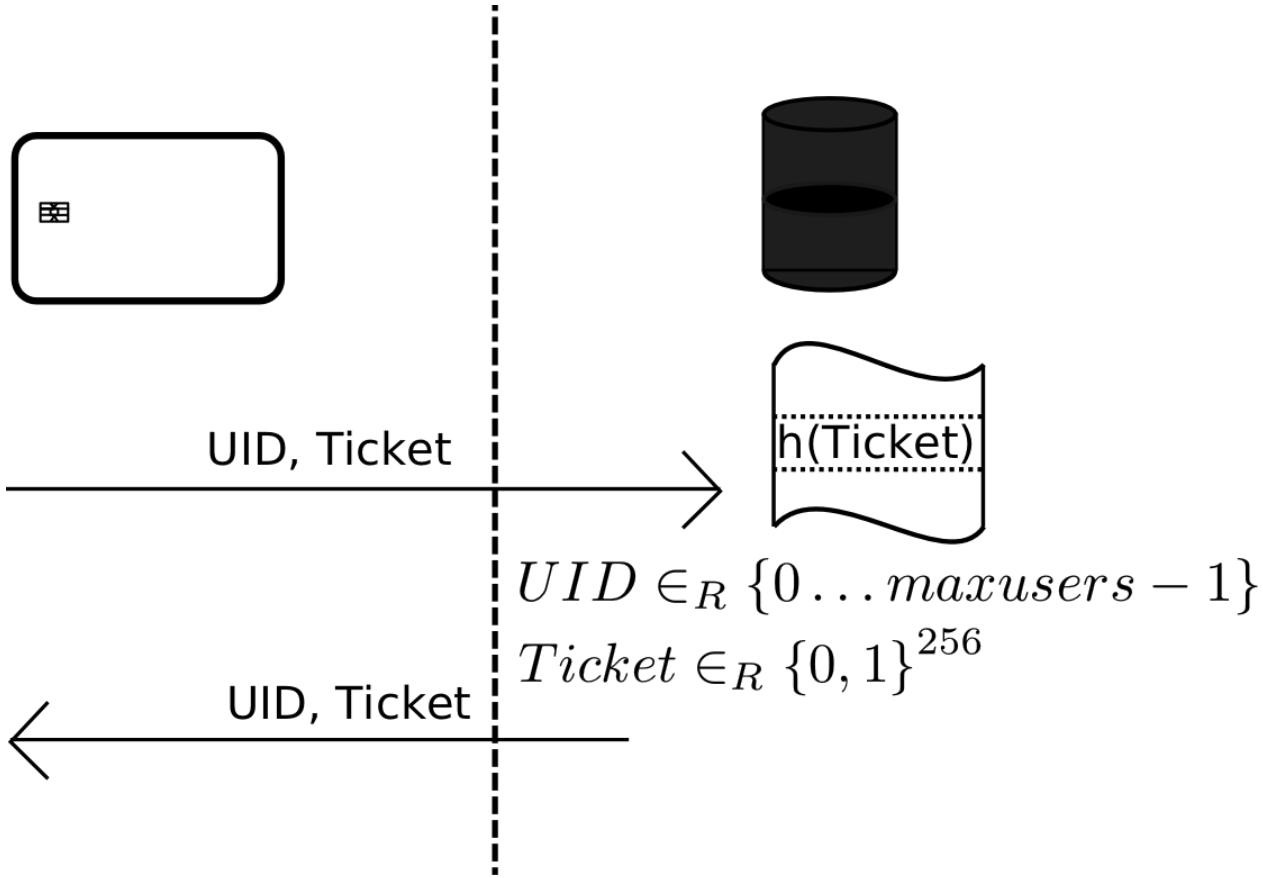
- nur pseudonym

Ansatz 1 – Probleme

- nur pseudonym
- pseudonym schwer merkbar

Ansatz 2

neue, zufällige UIDs



Ansatz 2 – Probleme

Ansatz 2 – Probleme

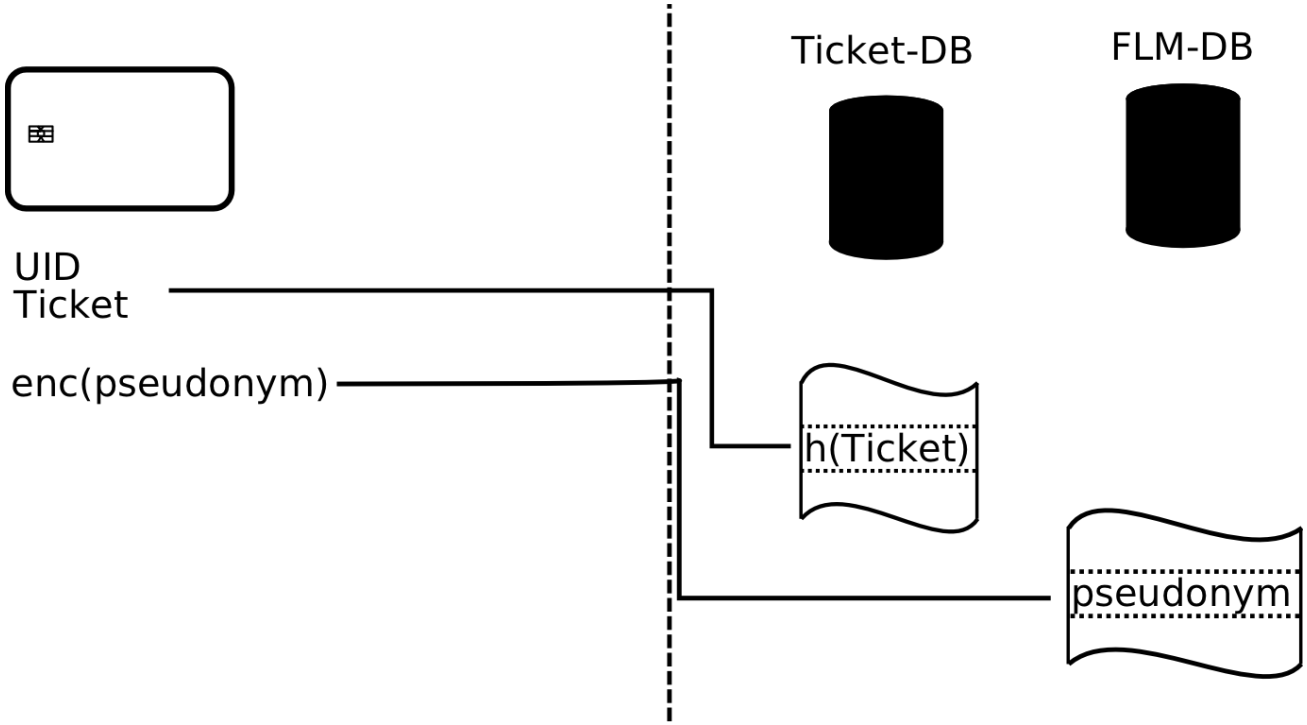
- keine feste Referenz auf Nutzer

Ansatz 2 – Probleme

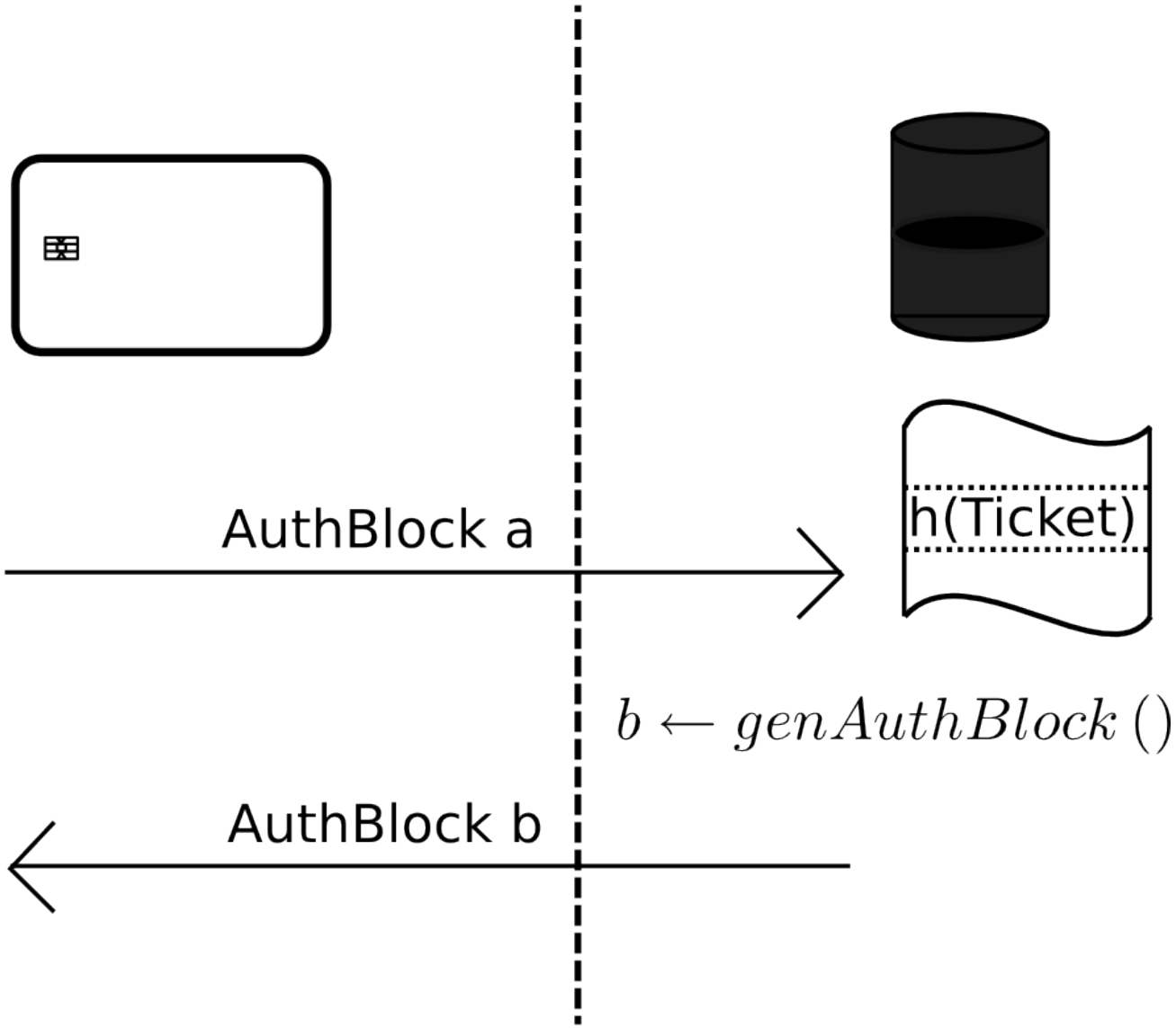
- keine feste Referenz auf Nutzer
- nicht mehr ”wartbar”

AnonAccess

Zusätzliche Datenbank für Änderungen



AnonAccess Ablauf



AuthBlock Struktur

AuthBlock Struktur:

UID	User ID; Index in die Ticket-DB
Ticket	$enc_{TicketKey}(24ByteZufall \parallel 8ByteZeitstempel)$
rkey	32 Byte zufälliger Schlüssel
rid	$enc_{ridKey}\left(enc_{rkey}\left(h\left(Pseudonym\right)\right)\right)$
HMAC	HMAC über die vorrangegangenen Daten

FLM-DB Struktur

FLM-DB Struktur:

active	ist dieser Eintrag aktiviert
permanent	soll der Eintrag nach anwendung glöscht werden
last	letzter Eintrag in der Datenbank
setflags	Flags die gesetzt werden sollen
clearflags	Flags die zu löschen sind
timestamp	Zeitstempel zur Erstellung des Eintrags
hnick	Hash des Pseudonyms

Anwendung von Modifizierungen

Änderungen können nicht zwangsläufig unmittelbar angewendet werden.

3 Stufen Konzept

3 Stufen Konzept

Namentlich

bekannter Nutzer

3 Stufen Konzept

Namentlich

Pseudonym

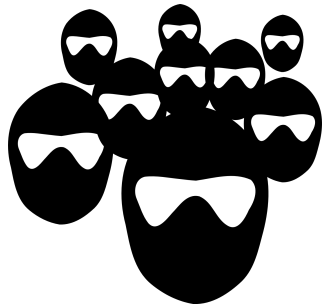
bekannter Nutzer

3 Stufen Konzept

Namentlich

bekannter Nutzer

Pseudonym



shared Pseudonym (”Anonym”)

Namentlich bekannt

Namentlich bekannt

- Name wird in der Ticket-DB hinterlegt

Namentlich bekannt

- Name wird in der Ticket-DB hinterlegt
- anonym-Flag $\leftarrow$ 0

Namentlich bekannt

- Name wird in der Ticket-DB hinterlegt
- anonym-Flag $\leftarrow$ 0
- Name ist auch Pseudonym

Pseudonym

Pseudonym

- es wird kein Name gespeichert

Pseudonym

- es wird kein Name gespeichert
- anonym-Flag $\leftarrow$ 1

Pseudonym

- es wird kein Name gespeichert
- anonym-Flag $\leftarrow$ 1
- individuelles Pseudonym

shared Pseudonym

shared Pseudonym

- es wird kein Name gespeichert

shared Pseudonym

- es wird kein Name gespeichert
- anonym-Flag $\leftarrow$ 1

shared Pseudonym

- es wird kein Name gespeichert
- anonym-Flag $\leftarrow$ 1
- Gruppen-Pseudonym

Probleme

Problem:
Das gezielte Löschen von Nutzern des *shared pseudonym*-Features ist nicht möglich.

Lösung

Lokale Policies (Beispiele):

Lösung

Lokale Policies (Beispiele):

- Timeouts

Lösung

Lokale Policies (Beispiele):

- Timeouts
- Nur Pseudonymisierte Nutzer dürfen Admin sein

Lösung

Lokale Policies (Beispiele):

- Timeouts
- Nur Pseudonymisierte Nutzer dürfen Admin sein
- Nickname muss der Realname sein

End Of Presentation