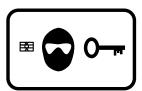
#### **AnonAccess**

Sören Heisrath, Daniel Otte

### **AnonAccess**

Sören Heisrath Daniel Otte





27. Dezember 2007

- 1 Schlüsselproblem
- 2 Anforderungen
- 3 ein erster Ansatz
- 4 Probleme
- 5 Ein zweiter Ansatz
- 6 Probleme 2
- 7 AnonAccess

## Unser Schlüsselproblem

#### AnonAccess

Sören Heisrath, Daniel Otte

#### Schlüsselproble

Anforderunge

ain aretar

\_ ...

Ein zweite Ansatz

Probleme 2

AnonAccess

Probleme ui

3 Stufer

ГОГ

- viele Leute
- wenig Schlüssel
- wenig Geld

# Unsere Anforderungen

#### AnonAccess

Heisrath,
Daniel Otte

Schlüsselproblem

#### Anforderungen

Ansatz

Problem

Ein zweite

Probleme 2

ΔησηΔοσρες

Probleme u

3 Stufer

ГОГ

- einfach zu realisieren
- günstig
- sicher

### Ansatz 1

#### AnonAccess

Heisrath,

Schlüsselproblem

Anforderunge

#### ein erster Ansatz

Droblomo

Ein zweite

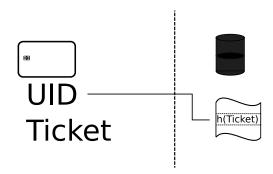
Probleme 2

AnonAccess

Probleme ur Lösungen

3 Stufer

FOP



### Ansatz 1 – Ablauf

#### AnonAccess

Sören Heisrath,

Schlüsselproblem

Anforderunge

ein erster Ansatz

- ----

Ein zweite

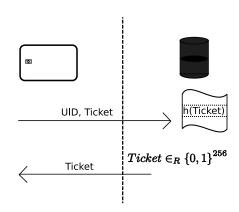
1 TODICITIC L

Anonaccess

Lösungen

3 Stufer

FOP



### Ticket-DB Struktur

#### AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselproblem

Struktur eines Eintrags in der Ticket-DB:

	<u> </u>
flags	Flags (siehe unten)
nickname	Nickname (wenn Speicherung gewünscht)
ticketmac	MAC vom Ticket

ein erster

Ansatz

i iobieiiii

Ansatz

Probleme 2

AnonAccess

Losungen

3 Stufen

Konzep

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

#### AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselproblem

Anforderunger

ein erster

#### Probleme

Ein zweiter

Probleme 2

ΔησηΔοσρες

Probleme un

3 Stufer

### Ansatz 1 – Probleme

#### AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselproblem

Anforderungei

ein erster

Ansatz Probleme

Ein zweite

Droblomo C

AnonAccess

Probleme ur

3 Stufer

F00

nur pseudonym

### Ansatz 1 – Probleme

#### AnonAccess

Schlüsselproblem

Probleme

- nur pseudonym
- pseudonym schwer merkbar

### Ein zweiter Ansatz

#### AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselproblem

Anforderunge

ein erster

Ansatz

Ein zweiter Ansatz

\_ ... .

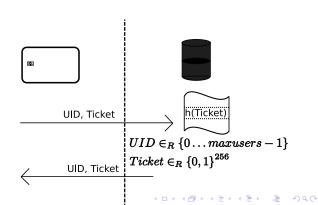
AnonAccoss

Probleme un

3 Stufen

EOP

dynamische UIDs



### Ansatz 2 - Probleme

#### AnonAccess

Sören Heisrath,

Schlüsselproblem

Anforderungen

ein erster

Broblome

Ein zweite

#### Probleme 2

AnonAccess

Probleme ur

3 Stufe

FOR

### Ansatz 2 - Probleme

#### AnonAccess

Heisrath, Daniel Otte

Schlüsselproblem

Anforderunge

ein erstei

Alisalz

Ein zweit

Ein zweit ∆neatz

Probleme 2

AnonAccess

Probleme ui

3 Stufen

keine feste Referenz auf Nutzer

### Ansatz 2 – Probleme

#### AnonAccess

Heisrath,
Daniel Otte

Schlüsselproblem

Anforderunge

ein erstei Ansatz

FIODIEITI

Ein zweite

Probleme 2

AnonAccess

Probleme ui

3 Stufer

FOR

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

### **AnonAccess**

#### AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselproblem

Anforderunger

ein erster

\_ ...

\_.

Ansatz

Probleme 2

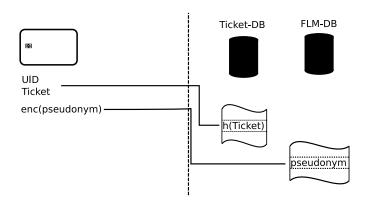
AnonAccess

Probleme un

3 Stufer

EOP

### Zusätzliche Datenbank für Änderungen



### **AuthBlock Struktur**

AnonAccess

Soren Heisrath, Daniel Otte

Schlüsselproblem

Anforderungen

ein erster

Problem

Ein zweite

Probleme 2

AnonAccess

Probleme ur

3 Stufen

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

### AuthBlock Struktur

AnonAccess

Soren Heisrath, Daniel Otte

Schlüsselproblem

Anforderungen

Ansatz

Probleme

Ein zweite Ansatz

Probleme 2

AnonAccess

Probleme ur

3 Stufen

FOP

UID	User ID; Index in die Ticket-DB
Ticket	enc <sub>TicketKey</sub> (24ByteZufall    8ByteZeitstempel)
rkey	32 Byte zufälliger Schlüssel
rid	$enc_{ridKey} (enc_{rkey} (h(Pseudonym)))$
HMAC	HMAC über die vorrangegangenen Daten

### FLM-DB Struktur

AnonAccess

Heisrath,
Daniel Otte

Schlüsselproblem

Anforderungen

ein erster

Allbalz

Probleme

Ein zweite Ansatz

Probleme :

AnonAccess

Probleme ur Lösungen

3 Stufen

FOF

active	ist dieser Eintrag aktiviert
permanent	soll der Eintrag nach anwendung glöscht werder
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

# EOP

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselproblem

Antorderunge

ein erster

Probleme

1 TODICITI

Ein zweite Ansatz

Probleme 2

AnonAccess

7 (1101)/ (00000

3 Stufen

EOP

# End Of Presentation