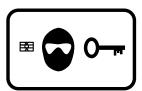
AnonAccess

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

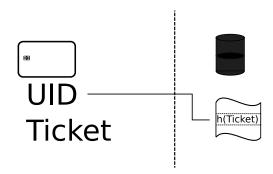
Probleme 2

AnonAccess

Probleme ur Lösungen

3 Stufer

FOP



Ansatz 1 – Ablauf

AnonAccess

Sören Heisrath,

Schlüsselproblem

Anforderunge

ein erster Ansatz

- ----

Ein zweite

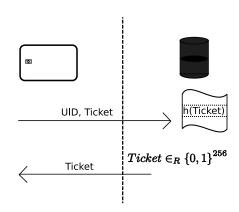
1 TODICITIC L

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 ui

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

_

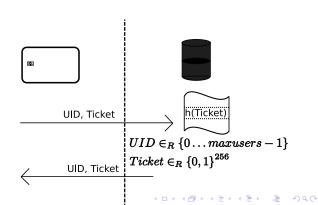
AnonAccoss

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

FIODIETTI

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

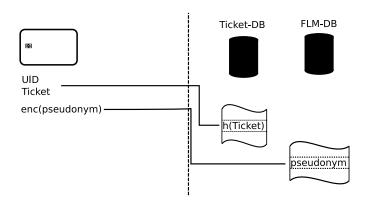
AnonAccess

Probleme un

3 Stufer

EOP

Zusätzliche Datenbank für Änderungen



AuthBlock Struktur

AnonAccess

Soren Heisrath, Daniel Otte

Schlüsselproblem

Anforderungen

Ansatz

Droblome

Fin zweit

Ansatz

Probleme 2

AnonAccess

Probleme ur

3 Stufen

EOP

UID	User ID; Index in die Ticket-DB
Ticket	enc _{TicketKey} (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

AnonAccess

Sören Heisrath,

Schlüsselproblem

Anforderunger

ein erster

Droblomo

Ein zweite

Probleme 2

AnonAccess

Probleme un Lösungen

3 Stufen Konzept

FOP

AnonAccess

Heisrath, Daniel Otte

Schlüsselproblem

Anforderungei

ein erste

Ansatz

Ein zweite

Ansatz

Probleme 2

AnonAccess

Probleme ur

3 Stufen Konzept

EOE

Namentlich bekannter Nutzer

AnonAccess

Heisrath,
Daniel Otte

Schlüsselproblem

Anforderunge

oin orotor

Problem

Ein zweite

Probleme 2

ΔησηΔοσρεί

_ ..

Lösunger

3 Stufen Konzept

- Namentlich bekannter Nutzer
- Pseudonym

AnonAccess

Soren Heisrath, Daniel Otte

Schlüsselproblem

Antorderunge

ein erster

_ ...

Problem

Ein zweite Ansatz

Probleme 2

AnonAccess

Probleme u

3 Stufen Konzept

FOR

- Namentlich bekannter Nutzer
- Pseudonym
- shared Pseudonym ("Anonym")

Namentlich bekannt

AnonAccess

Sören Heisrath, Paniel Otte

Schlüsselproblem

Anforderunger

ein erster

Droblomo

Ein zweite

Probleme 2

AnonAccess

Probleme un

3 Stufen Konzept

FOR

Namentlich bekannt

AnonAccess

Heisrath,
Daniel Otte

Schlüsselproblem

Anforderunge

ein erster

Ansatz

Ein zweite

Dualdania

. .

Anonacces

Lösungen

3 Stufen Konzept

EOE

■ Name wird in der Ticket-DB hinterlegt

Namentlich bekannt

AnonAccess

Heisrath,
Daniel Otte

Schlüsselproblem

Anforderunge

ein erstei Ansatz

7 11 10 CKL

Ein zweite

Ansatz

Probleme 2

AnonAccess

Probleme u

3 Stufen Konzept

ГОГ

- Name wird in der Ticket-DB hinterlegt
- anonym-Flag ← 0

AnonAccess

Sören Heisrath,

Schlüsselproblem

Anforderunger

ein erster

Broblomo

Ein zweite

Probleme 2

AnonAccess

Probleme un

3 Stufen Konzept

EOE

AnonAccess

Heisrath, Daniel Otte

Schlüsselproblem

Anforderunge

ein erste

Ansatz

F:-- -----:

Ein zweite Ansatz

Probleme 2

AnonAccess

Probleme ur

3 Stufen Konzept

EOB

es wird kein Name gespeichert

AnonAccess

Heisrath, Daniel Otte

Schlüsselproblem

Anforderunge

oin orotor

, ...oc.

Problem

Ein zweite

Probleme S

ΔησηΔοσος

Probleme ui

3 Stufen Konzept

EOE

- es wird kein Name gespeichert
- anonym-Flag ← 1

AnonAccess

Heisrath,
Daniel Otte

Schlüsselproblem

Antorderunge

ein erster

Problem

Ein zweite

Probleme 2

AnonAccess

Probleme u

3 Stufen Konzept

FOR

- es wird kein Name gespeichert
- anonym-Flag ← 1
- individuelles Pseudonym

AnonAccess

Sören Heisrath,

Schlüsselproblem

Anforderungen

ein erster

Droblomo

Ein zweiter

Probleme 2

AnonAccess

Probleme un Lösungen

3 Stufen Konzept

FOP

AnonAccess

Heisrath,

Schlüsselproblem

Anforderungei

ein erster

Ansatz

Ein zweite

Ansatz

Probleme 2

AnonAccess

Probleme ur

3 Stufen Konzept

EOP

es wird kein Name gespeichert

AnonAccess

Heisrath,
Daniel Otte

Schlüsselproblem

Antorderunge

..........

Problem

Ein zweite

Probleme S

A A

_ ..

Lösungen

3 Stufen Konzept

EOB

- es wird kein Name gespeichert
- anonym-Flag ← 1

AnonAccess

Heisrath,
Daniel Otte

Schlüsselproblem

Antorderunge

ein erster

Problem

Ein zweite Ansatz

Probleme 2

AnonAccess

Probleme u

3 Stufen Konzept

- es wird kein Name gespeichert
- anonym-Flag ← 1
- Gruppen-Pseudonym

EOP

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselproblem

Antorderunge

ein erster

_ ...

1 TODICITI

Ein zweite Ansatz

Probleme 2

AnonAccess

AHOHACCESS

3 Stufen

EOP

End Of Presentation