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

Schlüsselproblem

Anforderunge

ein erste

Problem

Ein zweiter

Probleme:

AnonAcces

Probleme un Lösungen

3 Stufer

=OP

- viele Leute
- wenig Schlüssel
- wenig Geld

Erste Überlegungen

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselproblem

Anforderunge

ein erste

Droblom

Ein zweite

Probleme 2

AnonAcces

Lösungen

3 Stufer Konzep

EOD

- Mechanische Schlüssel kann man einfach nachmachen
- Schliesssysteme sind teuer
- ⇒ wir müssen was Eigenes machen

Mittel & Wege

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselproblem

Anforderunge

ein erste

Probleme

Ein zwoit

. . .

AnonAccos

AnonAcces

Lösungen

3 Stufen

EOD

- Speicherkarten oder SmartCards
- Microcontroller-Plattform

Kostenabschätzung

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselproblem

Anforderunge

ein erste

. . .

Ein zweite

Probleme (

AnonAcces

Probleme und Lösungen

3 Stufer

EOB

■ Speicherkarten kosten ≤ 1 Euro pro Stück

■ geeigneter Microcontroller ≤ 10 Euro

Restliche elektronik ca. 10 Euro

Elegante Lösung

AnonAccess

Anforderungen

- einfach zu realisieren
- günstig
- sicher

Anonymität

AnonAccess

Anforderungen

Karten sollen anonym wie Schlüssel sein

Ansatz 1

AnonAccess

Soren Heisrath, Daniel Otte

Schlüsselpi

Anforderunge

ein erster Ansatz

Problem

Ein zweite Ansatz

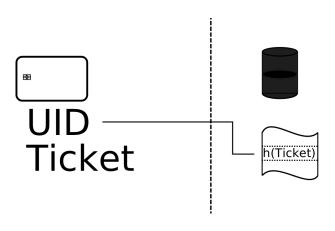
Probleme

AnonAccess

Probleme und Lösungen

3 Stufer Konzept

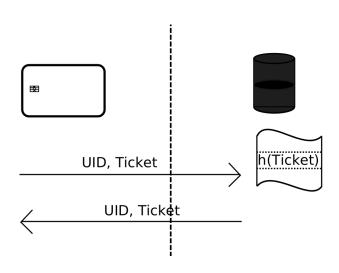
=OB



Ansatz 1 – Ablauf

AnonAccess

ein erster Ansatz



Ticket-DB Struktur

AnonAccess

Sören Heisrath, Daniel Otte

Anfordorungo

ein erster Ansatz

Probleme

Ein zweite Ansatz

Probleme

AnonAcces

Probleme und Lösungen

EOP

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

AnonAccess

Soren Heisrath, Daniel Otte

Schlüsselpro

Anforderunge

ein erste Ansatz

Probleme

Ein zweite

Probleme :

AnonAccess

Probleme und

3 Stufer

Ansatz 1 – Probleme

AnonAccess

Probleme

nur pseudonym

Ansatz 1 – Probleme

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpro blem

Anforderunge

ein erste Ansatz

Probleme

Ansatz

1 TobleThe 2

AnonAcces

Lösungen

3 Stufe

=OP

- nur pseudonym
- pseudonym schwer merkbar

Ablauf

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpro

Anforderunge

ein erste Ansatz

Probleme

Ein zweiter Ansatz

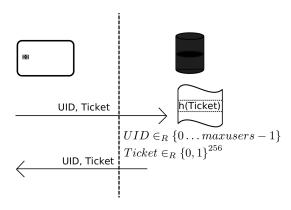
Probleme

AnonAcces

Probleme und Lösungen

3 Stufen Konzept

=OP



Ansatz 2 – Probleme

AnonAccess

Soren Heisrath, Daniel Otte

Schlüsselpro

Anforderunge

ein erste

Probleme

Ein zweite

Probleme 2

AnonAccess

Probleme und

3 Stufer Konzent

Ansatz 2 – Probleme

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpro

Anforderunae

ein erste

Probleme

Ein zweite

Probleme 2

AnonAcces

Probleme un

3 Stufen

Konzep

EOP

keine feste Referenz auf Nutzer

Ansatz 2 – Probleme

AnonAccess

Probleme 2

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

AnonAccess

AnonAccess

Soren Heisrath, Daniel Otte

bieiii

Amoraerunge

ein erstei Ansatz

Problem

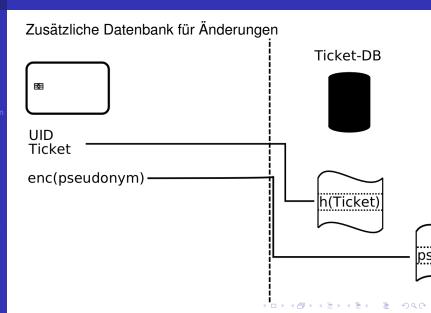
Ein zweite Ansatz

robleme 2

AnonAccess

Probleme und Lösungen

3 Stufer Konzept



AuthBlock Struktur

AnonAccess

Sören Heisrath, Daniel Otte

biem

Amoraerunge

Ansatz

Probleme

Ansatz

Probleme 2

AnonAccess

Probleme und Lösungen

3 Stufe

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

Sören Heisrath, Daniel Otte

blem

Anforderunge

ein erster Ansatz

Probleme

Ein zweite

Probleme 2

AnonAccess

Probleme un Lösungen

3 Stufe Konzep

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

Datenbank wird "kopiert"

AnonAccess

Probleme und Lösungen

Lösung: Datenbank wird verschlüsselt.

Nutzer entfernen

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpr blem

Anforderunge

ein erste Ansatz

TODICTIE

Ein zweite

Probleme

AnonAcces

Probleme und Lösungen

3 Stufer Konzept

FOP

Problem: Wie findet man die Nutzer wieder? Lösung: Garnicht - Man arbeitet mit timeouts.

AnonAccess

Soren Heisrath, Daniel Otte

Schlüsselpro Nem

Anforderunge

ein erste

Probleme

Ein zweite

Probleme :

AnonAccess

Probleme und

3 Stufen Konzept

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpro

Anforderunge

ein erste

Probleme

Ein zweite

Probleme

AnonAccess

AllollAcces.

3 Stufen

Konzept

FOP

Namentlich bekannter Nutzer

AnonAccess

Heisrath,
Daniel Otte

Schlüsselpr blem

Anforderung

ein erste Ansatz

Problem

Ein zwei

Droblomo

AnonAcces

7 100000

3 Stufen

Konzept

EOP

- Namentlich bekannter Nutzer
- Pseudonym

AnonAccess

Heisrath,
Daniel Otte

blem

Antorderung

ein erste Ansatz

Problem

Ein zweiter

Probleme 2

AnonAcces

Probleme un

3 Stufen Konzept

=OP

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

AnonAccess

Soren Heisrath, Daniel Otte

Schlüsselpro Nem

Anforderunge

ein erste

Problems

Ein zweite

Probleme:

AnonAccess

Probleme und

3 Stufen Konzept

AnonAccess

3 Stufen Konzept

Name wird in der Ticket-DB hinterlegt

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpro

Anforderunge

ein erste Ansatz

Problem

Ein zwoit

Problomo

AnonAcces

Anonacces

3 Stufen

Konzept

EOP

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

AnonAccess

Soren Heisrath, Daniel Otte

blem

Antorderung

ein erste Ansatz

Problem

Fin zweit

Probleme :

AnonAcces

Probleme un

3 Stufen Konzept

EOP

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

AnonAccess

Heisrath, Daniel Otte

Schlüsselpro Jem

Anforderunge

ein erste

Problems

Ein zweite

Probleme :

AnonAccess

Probleme und

3 Stufen Konzept

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpro

Anforderunge

ein erste

Probleme

Ein zweite

Probleme

AnonAccess

AllollAcces.

3 Stufen Konzept

101120

FOP

es wird kein Name gespeichert

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpro

Anforderunge

ein erste Ansatz

Problem

Ein zweit

Probleme

AnonAcces

Probleme un

3 Stufen Konzept

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

AnonAccess

Heisrath,
Daniel Otte

blem

Antorderunge

ein erste Ansatz

Problem

Ein zweiter

Probleme 2

AnonAcces

Probleme und

3 Stufen Konzept

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

AnonAccess

Soren Heisrath, Daniel Otte

Schlüsselpro

Anforderunge

ein erste

Problems

Ein zweite

Probleme :

AnonAccess

Probleme und

3 Stufen Konzept

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpro

Anforderunge

ein erste

Probleme

Ein zweite

Probleme

AnonAccess

AHOHACCES

3 Stufen

3 Stuten Konzept es wird kein Name gespeichert

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpro

Anforderunge

ein erste

Problem

Probleme

Ansatz

Probleme :

AnonAcces

Probleme un

3 Stufen Konzept

EOP

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

AnonAccess

3 Stufen Konzept

es wird kein Name gespeichert

■ anonym-Flag ← 1

Gruppen-Pseudonym

EOP

AnonAccess

Heisrath Daniel Ott

Schlüsselpr blem

Anforderunge

ein erste Ansatz

Probleme

Ein zweiter

Probleme 2

AnonAccess

Probleme und Lösungen

3 Stufer Konzept

EOP

End Of Presentation