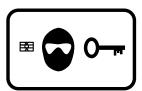
AnonAccess

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 Ansatz

Problema

Problem

Ansatz

AnonAcces

Probleme u Lösungen

3 Stufer

=OP

- viele Leute
- wenig Schlüssel
- wenig Geld

Erste Überlegungen

AnonAccess

Schlüsselproblem

- 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 Ansatz

Probleme

Probleme

Ansatz

1 TODICTIC 2

AnonAcces

Probleme und Lösungen

3 Stufen

Konzep

=OP

- Speicherkarten oder SmartCards
- Microcontroller-Plattform

Kostenabschätzung

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselproblem

Anforderunge

ein erste

FIODIEITIE

Ein zweite Ansatz

Probleme 2

AnonAcces

Probleme und

3 Stufer

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

Elegante Lösung

AnonAccess

Sören Heisrath, Daniel Otte

chlüsselpro

Anforderungen

ein erste Ansatz

Probleme

Probleme

. . .

AnonAccess

AHUHACCES

Losunger 3 Stufen

3 Stuter Konzep

=OP

- einfach zu realisieren
- günstig
- sicher

Anonymität

AnonAccess

Sören Heisrath, Daniel Otte

chlüsselpro

Anforderungen

ein erste

Problem

Ein zweite

Probleme

AnonAcces

Probleme und

3 Stufen

EOP

Karten sollen anonym wie Schlüssel sein



Ansatz 1

AnonAccess

Soren Heisrath, Daniel Otte

Schlüsselpr

Anforderunge

ein erster Ansatz

Probleme

Ein zweite

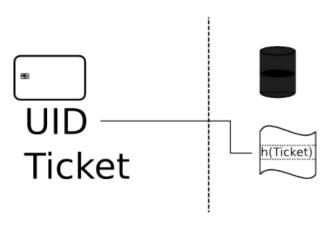
Probleme:

AnonAccess

Probleme und Lösungen

3 Stufer

=OP



Ansatz 1 – Ablauf

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpro

Anforderunge

ein erster Ansatz

Problem

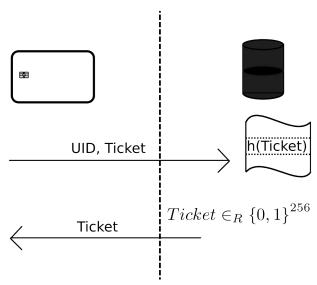
Ein zweite

Probleme

AnonAcces

Probleme u Lösungen

3 Stufen



Ticket-DB Struktur

AnonAccess

ein erster Ansatz

Struktur eines Fintrags 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 olem

Anforderunge

ein erste

Probleme

Ein zweite

Probleme :

AnonAccess

Probleme und

3 Stufer

Ansatz 1 – Probleme

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpro

Anforderunge

ein erste Ansatz

Probleme

Ein zweite Ansatz

Probleme 2

AnonAcces

Probleme und Lösungen

3 Stufen

EOP

nur pseudonym

Ansatz 1 – Probleme

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselproblem

Anforderunge

ein erste Ansatz

Probleme

Ansatz

Probleme 2

AnonAcces

Probleme un Lösungen

3 Stufer

EOP.

- nur pseudonym
- pseudonym schwer merkbar

Ansatz 2

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpro

Anforderunge

ein erste Ansatz

Probleme

Ein zweiter Ansatz

Probleme :

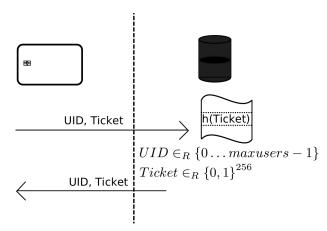
AnonAcces

Probleme und Lösungen

3 Stufer Konzept

=OB

neue, zufällige UIDs



Ansatz 2 – Probleme

AnonAccess

Soren Heisrath, Daniel Otte

Schlüsselpro

Anforderunge

ein erste

Probleme

Ein zweite

Probleme 2

AnonAccess

Probleme und

3 Stufer

Ansatz 2 - Probleme

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpro

Anforderunge

ein erste

Probleme

Ein zweite

Probleme 2

AnonAcces

Probleme und

3 Stufen

Konzep

EOP

keine feste Referenz auf Nutzer

Ansatz 2 - Probleme

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpro

Anforderunge

ein erste Ansatz

Probleme

TODICITIO

Probleme 2

AnonAcces

Anonacces

Probleme un Lösungen

3 Stufer

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

AnonAccess

AnonAccess

Sören Heisrath, Daniel Otte

7 illioraciang

Ansatz

Problem

Droblomo

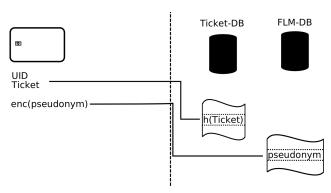
AnonAccess

Probleme und Lösungen

3 Stufen Konzept

FOP

Zusätzliche Datenbank für Änderungen



AuthBlock Struktur

AnonAccess

Sören Heisrath, Daniel Otte

blem

Anforderunge

ein erster Ansatz

Probleme

Ein zweite

Probleme 2

AnonAccess

Probleme und Lösungen

3 Stufe Konzep

UID	User ID; Index in die Ticket-DB
Ticket	$enc_{TicketKey}(24ByteZufall \parallel 8ByteZeitstempel)$
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

A ... f - ... l -

7 illioraciange

eın erster Ansatz

Probleme

Ansatz

Probleme 2

AnonAccess

Probleme und Lösungen

3 Stufei Konzep

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	

Datenbank wird "kopiert"

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpro

nforderunge

ein erste Ansatz

Problem

Fin zwei

robleme

AnonAcces

Probleme und Lösungen

3 Stufen

FOP

Lösung: Datenbank wird verschlüsselt.

Nutzer entfernen

AnonAccess

Heisrath, Daniel Otte

Schlüsselpr blem

Anforderunge

ein erste Ansatz

TODICTIE

Ein zweit

Probleme

AnonAccess

Probleme und Lösungen

3 Stufei Konzep

FOP

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

AnonAccess

Soren Heisrath, Daniel Otte

Schlüsselpro blem

Anforderunge

ein erste

Problems

Ein zweite

Probleme :

AnonAccess

Probleme und

3 Stufen Konzept

AnonAccess

Soren Heisrath, Daniel Otte

blem

Amoraciange

ein erste Ansatz

Probleme

. . . .

AnonAoooo

Probleme und

3 Stufen Konzept

=OP



Namentlich

bekannter Nutzer

AnonAccess

Soren Heisrath, Daniel Otte

blem

Amoraerang

Ansatz

Probleme

. .

Probleme un

3 Stufen Konzept

EOP.





Pseudonym

bekannter Nutzer

AnonAccess

Soren Heisrath, Daniel Otte

DICITI

7 il llor dor drige

Ansatz

Cin munito

Ansatz

Froblettie 2

AnonAccess

Lösungen

3 Stufen Konzept

FOP







bekannter Nutzer

shared Pseudonym ("Anonym")

AnonAccess

Soren Heisrath, Daniel Otte

chlüsselpro

Anforderunge

ein erste

Probleme

Ein zweite

Probleme:

AnonAccess

Probleme und

3 Stufen Konzept

AnonAccess

Sören Heisrath, Daniel Ott

Schlüsselpro

Anforderunge

ein erste

Probleme

Ein zweite

Probleme

AnonAcces

Probleme un

3 Stufen Konzept

FOP

Name wird in der Ticket-DB hinterlegt

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpro

Anforderunge

ein erste Ansatz

Problem

Ein zwoit

Droblomo

AnonAcces

Probleme ur

3 Stufen Konzept

Konze

=OP

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

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpr blem

Antorderunge

ein erste Ansatz

Problem

Ein zweite

Probleme 2

AnonAcces

Probleme un

3 Stufen Konzept

EOP

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

AnonAccess

Soren Heisrath, Daniel Otte

Schlüsselpro olem

Anforderunge

ein erste

Problems

Ein zweite

Probleme :

AnonAccess

Probleme und

3 Stufen Konzept

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpro

Anforderunge

ein erste Ansatz

Probleme

Ein zweite

Probleme

AnonAcces

Probleme ur

3 Stufen Konzept

EOP

es wird kein Name gespeichert

AnonAccess

3 Stufen

Konzept

es wird kein Name gespeichert

anonym-Flag ← 1

AnonAccess

Heisrath,
Daniel Otte

Schlusselpi

Antorderunge

ein erste Ansatz

Problem

Ein zweite

Probleme 2

AnonAcces

Probleme un

3 Stufen Konzept

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

AnonAccess

Soren Heisrath, Daniel Otte

Schlüsselpro olem

Anforderunge

ein erste

Problems

Ein zweiter

Probleme:

AnonAccess

Probleme und

3 Stufen Konzept

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpro

Anforderunge

ein erste

Probleme

Ein zweite

Probleme

AnonAcces

D 11

3 Stufen Konzept

EOP

es wird kein Name gespeichert

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpro

Anforderunge

ein erste

Problem

Ein zweit

Drablama

AnonAcces

AnonAcces

3 Stufen

Konzept

es wird kein Name gespeichert

■ anonym-Flag ← 1

AnonAccess

3 Stufen Konzept

es wird kein Name gespeichert

■ anonym-Flag ← 1

Gruppen-Pseudonym

EOP

AnonAccess

Soren Heisrath, Daniel Otte

Schlüsselpro

Anforderunge

ein erste

Probleme

Fin zweit

Probleme

AnonAcces

Probleme un

3 Stufer

Konzep

EOP

Fragen?