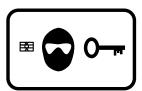
AnonAccess

Sören Heisrath, Daniel Otte

AnonAccess

Sören Heisrath Daniel Otte





27. Dezember 2007

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

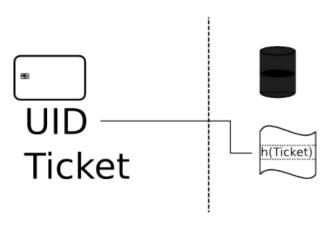
Probleme:

AnonAccess

Probleme und Lösungen

3 Stufer

=OP



Ansatz 1 – Ablauf

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpro

Anforderunge

ein erster Ansatz

Problem

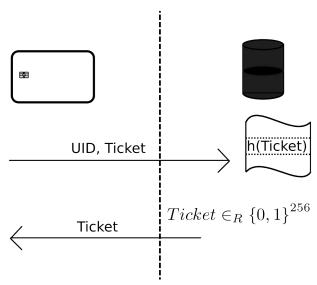
Ein zweite

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

Probleme

nur pseudonym

Ansatz 1 – Probleme

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselproblem

Anforderunge

ein erste Ansatz

Probleme

Ansatz

Probleme 2

AnonAccess

Probleme ui Lösungen

3 Stufei Konzen

EOP

- nur pseudonym
- pseudonym schwer merkbar

Ansatz 2

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpro

Anforderunge

ein erste Ansatz

Probleme

Ein zweiter Ansatz

Probleme 2

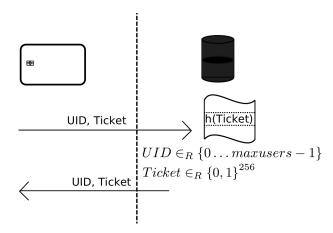
AnonAcces

Probleme und Lösungen

3 Stufer Konzept

=OB

neue, zufällige UIDs



Ansatz 2 – Probleme

AnonAccess

Soren Heisrath, Daniel Otte

Schlüsselpro

Anforderunge

ein erste

Problems

Ein zweite

Probleme 2

AnonAccess

Probleme und

3 Stufer

Ansatz 2 – Probleme

AnonAccess

Probleme 2

keine feste Referenz auf Nutzer

Ansatz 2 – Probleme

AnonAccess

Probleme 2

keine feste Referenz auf Nutzer

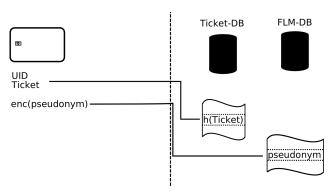
nicht mehr "wartbar"

AnonAccess

AnonAccess

AnonAccess

Zusätzliche Datenbank für Änderungen



AnonAccess Ablauf

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpro

Anforderung:

ein erste Ansatz

Probleme

Ein zweiter

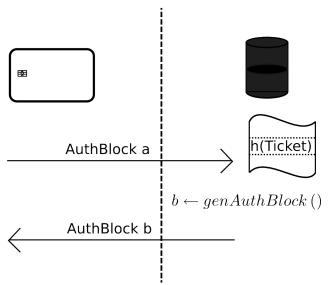
Probleme:

AnonAccess

Probleme und Lösungen

3 Stufer Konzept

=OP



AuthBlock Struktur

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpro blem

Anforderunge

ein erster Ansatz

7110012

Ein zweite

Probleme 2

AnonAccess

Probleme und Lösungen

3 Stufei Konzep

AuthBlock Struktur:

, tati Biook of artar		
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

DIGITI

Antoraerunge

Ansatz

Fin zweit

Ansatz

Probleme 2

AnonAccess

Probleme und Lösungen

3 Stufeı Konzep

FOP

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	

Datenbank wird "kopiert"

AnonAccess

Probleme und Lösungen

Lösung: Datenbank wird verschlüsselt.

Nutzer entfernen

AnonAccess

Heisrath, Daniel Ott

blem

Anforderunge

ein erste Ansatz

TODICTIE

Ein zweit

Probleme

AnonAcces

Probleme und Lösungen

3 Stufer 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

Probleme

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

3 Stufen Konzept

Name wird in der Ticket-DB hinterlegt

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpro

Anforderunge

ein erste Ansatz

Problem

Ein zwoi

Droblomo

AnonAcces

AHOHACCES

3 Stufen

Konzept

Name wird in der Ticket-DB hinterlegt

■ anonym-Flag \leftarrow 0

AnonAccess

Sören Heisrath, Daniel Otte

blem

Antorderunge

ein erste Ansatz

Problem

Ein zweit

Probleme 2

AnonAcces

Probleme un

3 Stufen Konzept

EOP

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

AnonAccess

Soren Heisrath, Daniel Otte

Schlüsselproblem

Anforderunge

ein erste

Probleme

Ein zweite

Probleme

AnonAcces

Probleme und

3 Stufen Konzept

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpro

Anforderunge

ein erste Ansatz

Probleme

Ein zweite

Probleme:

AnonAcces

Probleme un

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

Anforderunae

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

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

EOP

End Presentation