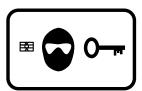
AnonAccess

Sören Heisrath, Daniel Otte

AnonAccess

Sören Heisrath Daniel Otte





27. Dezember 2007

Unser Schlüsselproblem:

AnonAccess

Sören Heisrath,

Schlüsselproblem

Anforderunge

Regrifflichk

ein erster

Ansatz

Problem

Ein zweite Ansatz

Probleme 2

Figenschafte

3 Stufer

EOB

- viele Leute
- wenig Schlüssel
- wenig Geld

Erste Überlegungen

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselproblem

Anforderunge

Dogwiffliable

ein erste

Probleme

Ein zweite

Probleme 2

Figenschafte

3 Stufer

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

Mittel & Wege

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselproblem

Anforderunge

Begrifflichkeite

ein erster

Problem

Ein zweite

Probleme 2

Figenschafte

3 Stufen

EOD

- Speicherkarten oder SmartCards
- Microcontroller-Plattform

Kostenabschätzung

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselproblem

Anforderunge

Dagwiffliable

ein erster

Problem

Ein zweite

Probleme 2

Eigeneeheft

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

B

ein erster

Ansatz

Problem

Ein zweite

Probleme 2

Eigeneehefte

3 Stufer

- einfach zu realisieren
- günstig
- sicher

Anonymität

AnonAccess

Sören Heisrath, Daniel Otte

chlüsselpro-

Anforderungen

Begrifflichkeite

ein erster

Droblom

Ein zweite

Probleme 2

Figenschafte

2 Stufan

3 Stuter Konzept

FOP

Karten sollen anonym wie Schlüssel sein



Prüfsummen

AnonAccess

Sören Heisrath, Daniel Otte

chlüsselpro

Anforderunge

Begrifflichkeiten

ein erstei

Problem

Ein zweite

Probleme 2

Figenschafte

3 Stufer

FOP

z.B. eine Quersumme üeber eine Zahl.

Problem

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpro

Anforderunge

Begrifflichkeiten

ein erste

Ansatz

Probleme 2

Eigenechefte

Ligeriscriant

3 Stufer Konzept

FOP

Zu einer gegebenen Prüfsumme kann jeder eine valide andere Zahl generieren.



Hashfunktionen

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpi blem

Antorderunge

Begrifflichkeiten

ein erste

Problem

Ein zweite Ansatz

Probleme 2

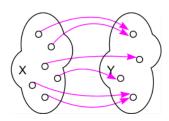
. .

Eigenschafte

3 Stufer

FOP

Hashfunktionen sind Einweg-Funktionen die eine beliebig grosse Datenmenge auf eine kleinere Datenmenge abbilden.



Hash-MACs

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpro

Anforderunge

Begrifflichkeiten

ein erste

Problem

Ein zweite

Probleme 2

A A

Eigenschafte

3 Stufer

FOP

Hash-MACs sind Hash-funktionen zur Authenfikation von Nachrichten.

$$\mathit{HMAC}_k(\mathit{msg}) = \mathit{hash}((\mathit{k} \oplus \mathit{opad}) \parallel \mathit{hash}((\mathit{k} \oplus \mathit{ipad}) \parallel \mathit{msg}))$$

Ansatz 1

AnonAccess

Heisrath,
Daniel Otte

Schlüsselpr blem

Anforderunge

Begrifflichkei

ein erster Ansatz

Problem

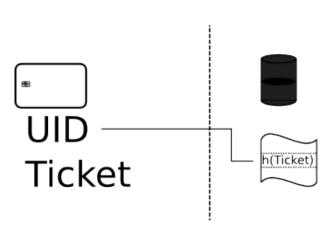
Ein zweite Ansatz

Probleme 2

. .

Eigenschafte

3 Stufen



Ansatz 1 – Ablauf

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpro

Anforderunge

Begrifflichkeit

ein erster Ansatz

Problem

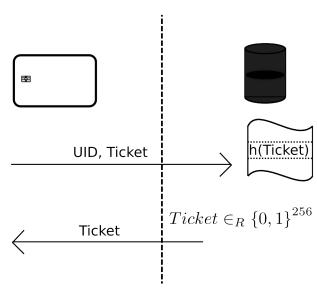
Ein zweite

Probleme 2

Eigenschafte

3 Stufen Konzept

EOB



Ticket-DB Struktur

AnonAccess

Sören Heisrath, Daniel Otte

blem

Dagwiffliablesita

Begrifflichkeite

ein erster Ansatz

Problem

Ansatz

Probleme :

Eigeneehefte

2 Ctuton

3 Stufen Konzept

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

Anforderunger

Begrifflichkeite

oin oretor

Probleme

Ein zweite

Probleme 3

Finenschafte

3 Stufen

Ansatz 1 – Probleme

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpro

Anforderunge

Begrifflichkeite

ein erster

Probleme

Ein zweite

Probleme 2

Eigenechefte

3 Stufen

-05

nur pseudonym

Ansatz 1 – Probleme

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpro

Anforderunge

Begrifflichkeite

ein erster Ansatz

Probleme

Ein zweite Ansatz

Probleme 2

Figenschafte

3 Stufen

FOR

- nur pseudonym
- pseudonym schwer merkbar

Ansatz 2

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpre

Anforderunge

Begrifflichkei

ein erste Ansatz

Problem

Ein zweiter Ansatz

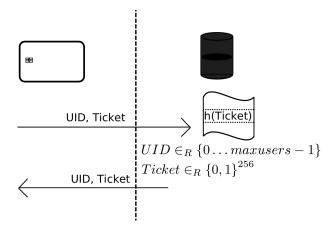
Probleme 2

AHOHAGGGSS

Eigonschafto

3 Stufer Konzept





Ansatz 2 – Probleme

AnonAccess

Soren Heisrath, Daniel Otte

ichlüsselpro

Anforderunge

Begrifflichkeite

ein erster

Ein zweite

Probleme 2

ΔησηΔοσος

Figenschafte

3 Stufen

Ansatz 2 – Probleme

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpro-

Anforderunge

ein erstei

Ansatz

Problem

Ein zweite

Probleme 2

Figenschafte

3 Stufen

Konzep

EOP

keine feste Referenz auf Nutzer



Ansatz 2 – Probleme

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpro

Anforderunge

Begrifflichkeite

ein erster

Problem

Ein zweite

Probleme 2

A A . . .

Ligeriscriant

3 Stufer Konzept

EOP

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

AnonAccess

AnonAccess

Sören Heisrath, Daniel Otte

bioiii

Begrifflichkei

ein erste

Allsalz

Ansatz

Probleme 2

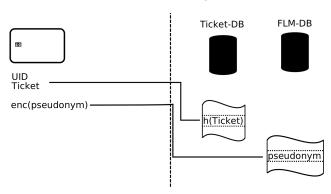
AnonAccess

Eigenschafte

3 Stufer Konzept

FOP

Zusätzliche Datenbank für Änderungen



AnonAccess Ablauf

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpro

Anforderunge

Begrifflichkeit

ein erste Ansatz

Problem

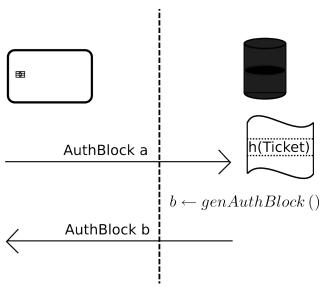
Ansatz

Probleme 2

AnonAccess

Eigenschafte

3 Stufen Konzept



AuthBlock Struktur

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselproblem

Anforderunger

Begrifflichkeite

ein erster

Problem

Ein zweite

Probleme 2

AnonAccess

Eigenschaft

3 Stufen Konzept

FOP

AuthBlock Struktur:

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

DIEITI

D

Бединісткене

ein erster

Problem

Ein zweiter Ansatz

Probleme 2

AnonAccess

Eigenschafte

3 Stufer Konzept

FOP

FLM-DB Struktur:

I LIVI-DD GITUKIUI.		
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	

Anwendung von Modifizierungen

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpro

Anforderunge

ein erster

Problem

Ein zweite Ansatz

Probleme 2

Eigenschaften

3 Stufen

3 Stufer Konzept

FOP

Änderungen können nicht zwangsläufig unmittelbar angewendet werden.



AnonAccess

Heisrath, Daniel Otte

Schlüsselpro

Anforderungei

Begrifflichkeit

ein erstei

Ansatz

Problem

Ein zweite

Probleme 2

Figenschafte

3 Stufen Konzept

AnonAccess

3 Stufen

Konzept



bekannter Nutzer

AnonAccess

Soren Heisrath, Daniel Otte

Schlüsselpr blem

Anforderunge

Regrifflichke

ein erste

. ...-

Fin zweit

.

Eigeneehefte

Eigenschafte

3 Stufen Konzept

EOP





Pseudonym

bekannter Nutzer

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpro

Anforderunge

Degriillerik

ein erster

1 TODICII

Ansatz

Probleme 2

F:-----

Eigenschafter

3 Stufen Konzept

EOP







bekannter Nutzer

Pseudonym

shared Pseudonym ("Anonym")

AnonAccess

Heisrath, Daniel Otte

Schlüsselpro

Anforderunge

Begrifflichkeit

ein erstei

Probleme

Ein zweite

Probleme 2

Figenschafte

3 Stufen Konzept

FOF

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpro

Anforderunge

Dagwiffliable

ein erste

Problem

Ein zweite

Probleme 2

Figenschafte

2 Stufon

3 Stufen Konzept

FOP

Name wird in der Ticket-DB hinterlegt

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpro

Antorderung

Boarifflioble

ein erste Ansatz

Problem

Ein zweite

Probleme 2

Finenschafte

3 Stufen Konzept

- Name wird in der Ticket-DB hinterlegt
- anonym-Flag \leftarrow 0

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpr blem

Anforderunge

Regrifflichk

ein erste Ansatz

Problem

Ein zweiter Ansatz

Probleme 2

Finenschafte

3 Stufen Konzept

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

Pseudonym

AnonAccess

Soren Heisrath, Daniel Otte

Schlüsselpro

Anforderunge

Begrifflichkeit

ein erster

_ ...

Ein zweite

Drahlama C

1 TobleThe 2

Electrical and

3 Stufen Konzept

EOE

Pseudonym

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselproblem

Inforderunge

_

ein erste

Doobless

Ein zweite

Probleme 2

Figenschafte

3 Stufen Konzept

FOP

es wird kein Name gespeichert

Pseudonym

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpro blem

Anforderunge

Degwifflighte

ein erstei

Problem

Ein zweite

Probleme 2

Figenschafte

3 Stufen Konzept

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

Pseudonym

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpr blem

Antorderunge

Pogrifflioble

ein erste

Problem

Ein zweite Ansatz

Probleme 2

Figenschafte

3 Stufen Konzept

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

AnonAccess

Soren Heisrath, Daniel Otte

chlüsselpro

Anforderunge

Begrifflichkeit

ein erster

Ansatz

Probleme

Ein zweite

Probleme 2

Figenschafte

3 Stufen Konzept

FOF

AnonAccess

Sören Heisrath, Daniel Otte

chlüsselpro

Anfordorung

ein erste

. . .

Ein zweite Ansatz

Probleme 2

Eigenschafte

3 Stufen Konzept

FOP

es wird kein Name gespeichert

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpro

Anforderunge

Dogwifffiolole

ein erstei

Problem:

Ein zweite

Probleme 2

Figenschafte

3 Stufen Konzept

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

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpr blem

Anforderung

Boariffliobke

ein erste

Problem

Ein zweite Ansatz

Probleme 2

Figenschafte

3 Stufen Konzept

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

Probleme

AnonAccess

Heisrath, Daniel Otte

blem

Amorderunge

Begrifflichkeite

ein erster

Duablana

Ein zweite

Probleme 2

_. . . .

Ligeriscriant

3 Stufen Konzept

FOP

Problem:

Das gezielte Löschen von Nutzern des *shared pseudonym*-Features ist nicht möglich.

AnonAccess

Soren Heisrath, Daniel Otte

chlüsselpro

Anforderungei

_

Begrifflichkei

Ansatz

Problem

Ein zweite Ansatz

Probleme 2

--inenschafter

3 Stufen

3 Stufen Konzept

EOP

Lokale Policies (Beispiele):

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpre blem

Anforderunge

Ŭ

ein erster

Ansatz

Problem

Ein zweite Ansatz

Probleme 2

A A . . .

Finenschafte

3 Stufen Konzept

FOP

Lokale Policies (Beispiele):

Timeouts

AnonAccess

Soren Heisrath, Daniel Otte

Schlüsselpri blem

Anforderungei

Begrifflichkeit

ain avatav

Ansatz

TODICITI

Ein zweite Ansatz

Probleme 2

AnonAcce

Eigenschafte

3 Stufen Konzept

EOP

Lokale Policies (Beispiele):

- Timeouts
- Nur Pseudonymisierte Nutzer dürfen Admin sein

AnonAccess

Sören Heisrath, Daniel Otte

blem

Anforderungei

Begrifflichkeite

ain avatav

Problem

Ein zweiter

Probleme 2

AnanAaaa

Eigenschafte

3 Stufen Konzept

FOP

Lokale Policies (Beispiele):

- Timeouts
- Nur Pseudonymisierte Nutzer dürfen Admin sein
- Nickname muss der Realname sein

EOP

AnonAccess

Soren Heisrath Daniel Ot

Schlüsselpr blem

Anforderunge

Begrifflichkeit

ein erster Ansatz

Problem

Ein zweite Ansatz

Probleme 2

A A

Eigenschafte

3 Stufer

EOP

End Of Presentation