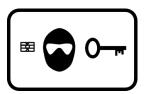
AnonAccess

Soren Heisrath, Daniel Otte

AnonAccess

Sören Heisrath Daniel Otte





27. Dezember 2007

Unser Schlüsselproblem:

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselproblem

Anforderunge

Pagrifflioble

ein erster

Ansatz

TTODICITI

Ein zweite Ansatz

Probleme 2

AnonAccess

Probleme ur

3 Stufe

Konzep^{*}

- 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

Schlüsselproblem

- Speicherkarten oder SmartCards
- Microcontroller-Plattform

Kostenabschätzung

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselproblem

Anforderunge

Begrifflichk

ein erster

Problem

Ein zweiter Ansatz

Probleme 2

AnonAccess

Probleme u

3 Stufe

Konzep

Konze

- 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 erster

Ansatz

Problem

Ein zweite Ansatz

Probleme 2

AnonAccess

_ ..

Lösungen

3 Stufer

Konzep

- einfach zu realisieren
- günstig
- sicher

Anonymität

AnonAccess

Soren Heisrath, Daniel Otte

chlüsselpro

Anforderungen

Begrifflichkeite

ein erster

_ ...

Ein zweite

Probleme 2

A A

Probleme un

Lösungen

3 Stufer

Konzep

FOP

Karten sollen anonym wie Schlüssel sein



Prüfsummen

AnonAccess

Sören Heisrath, Daniel Otte

chlüsselpro

Anforderunge

Begrifflichkeiten

ein erstei

Problem

Ein zweite

Probleme 2

Probleme un

3 Stufer

o oluiei Konzen

z.B. eine Quersumme üeber eine Zahl.

Problem

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpro

Inforderunge

Begrifflichkeiten

ein erste

Ansatz

-roblem

Ein zweite Ansatz

Probleme 2

AnonAccess

Probleme u

3 Stufen

Konzen

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

Hashfunktionen

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpr blem

Antorderunge

Begrifflichkeiten

ein erste

Problem

Ein zweite Ansatz

Probleme 2

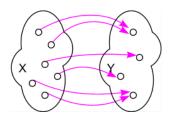
AnonAccess

Probleme un

3 Stufe

Konzep

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

Droblem

Ein zweite

Probleme 2

AnonAccess

Probleme ui

3 Stufer

Konzep

EOP

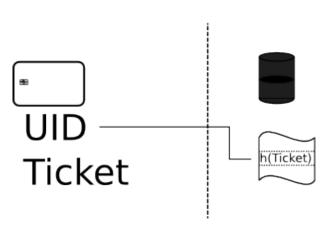
Hash-MACs sind Hash-funktionen zur Authenfikation von Nachrichten.

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

Ansatz 1

AnonAccess

ein erster Ansatz



Ansatz 1 – Ablauf

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpro

Anforderunge

Begrifflichkeit

ein erster Ansatz

Problem

Ein zweite Ansatz

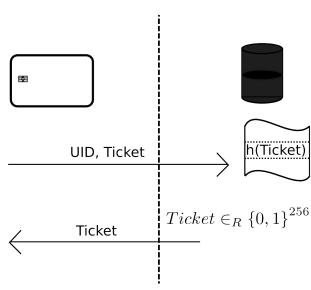
Probleme 2

Probleme und

3 Stufen

Konzepi

=OB



Ticket-DB Struktur

AnonAccess

Sören Heisrath, Daniel Otte

blem

Regrifflichkeite

ein erster

Ansatz

Problem

Ein zweite Ansatz

Probleme 2

- ...

Probleme und Lösungen

3 Stufen Konzept 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

Sören Heisrath, Daniel Otte

Schlüsselpro

Anforderunger

Begrifflichkeite

ein erster

Probleme

Ein zweite

Probleme 2

A ... - .. A - - - -

Probleme ui

Lösungen

3 Stutei Konzen

FOP

Ansatz 1 – Probleme

AnonAccess

Sören Heisrath, Daniel Otte

chlüsselpro

Anforderunge

Begrifflichkeit

ein erster

Probleme

Ein zweite

Probleme 2

Probleme ur

Probleme ul Lösungen

3 Stufe

Konzer

FOP

nur pseudonym

Ansatz 1 – Probleme

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpro

Anforderunge

Begrifflichkeite

ein erster Ansatz

Probleme

Ein zweite Ansatz

Probleme 2

AnonAccess

Probleme ui

Lösungen

3 Stufe

Konzep

EOD.

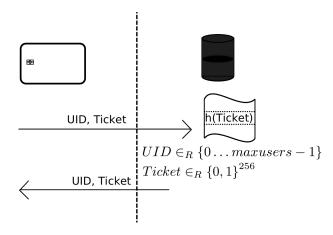
- nur pseudonym
- pseudonym schwer merkbar

Ansatz 2

AnonAccess

Ein zweiter Ansatz

neue, zufällige UIDs



Ansatz 2 – Probleme

AnonAccess

Soren Heisrath, Daniel Otte

Schlüsselpro

Anforderunger

Begrifflichkeite

ein erster

_ ...

Ein zweite

Probleme 2

AnonAcces

Probleme und

Losurige

3 Stulei Konzen

FOP

Ansatz 2 – Probleme

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpro

nforderunge

B

ein erster

Ansatz

Problem

Ein zweite

Probleme 2

AnonAccess

Lösungen

3 Stufer

Konzer

FOP

■ keine feste Referenz auf Nutzer

Ansatz 2 – Probleme

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpro

Anforderunge

Begrifflichkeit

ein erster

Problem

Ein zweite

Probleme 2

AnonAccess

Lösungen

3 Stufe

Konzep

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

AnonAccess

AnonAccess

Sören Heisrath, Daniel Otte

. . .

Begrifflichkeit

ein erster

Ansatz

TTODIETT

Ansatz

Probleme 2

AnonAccess

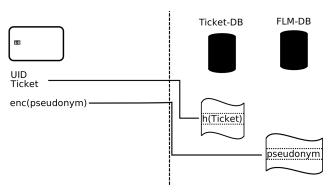
Probleme u Lösungen

3 Stufe

Konzep

=OB

Zusätzliche Datenbank für Änderungen



AnonAccess Ablauf

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpro

Anforderunge

Begrifflichkeit

ein erste Ansatz

Problem

Ansatz

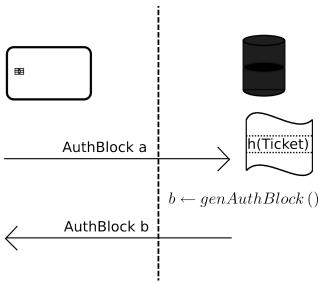
Probleme 2

AnonAccess

Probleme un Lösungen

Konzept

=OP



AuthBlock Struktur

AnonAccess

AnonAccess

AuthBlock Struktur:

, tati Biook of artar		
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

AnonAccess

ELM DB Strukture

FLIVI-DE STUKTUT.		
ist dieser Eintrag aktiviert		
soll der Eintrag nach anwendung glöscht		
werden		
letzter Eintrag in der Datenbank		
Flags die gesetzt werden sollen		
Flags die zu löschen sind		
Zeitstempel zur Erstellung des Eintrags		
Hash des Pseudonyms		

Datenbank wird "kopiert"

AnonAccess

Soren Heisrath, Daniel Otte

Schlüsselpro

Anforderunge

Dogrillionik

ein erster

Ansatz

Ein zweite Ansatz

Probleme 2

Probleme und Lösungen

3 Stufer

Konzep

Lösung: Datenbank wird verschlüsselt.

Nutzer entfernen

AnonAccess

Soren Heisrath, Daniel Ott

Schlüsselpro blem

Anforderung

......

ein erster

Problem -

Ein zweite Ansatz

Probleme 2

ΛησηΛοσο

Probleme und Lösungen

3 Stufer

Konzep

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



AnonAccess

Soren Heisrath, Daniel Otte

Schlüsselpro

Anforderunge

Begrifflichkeite

ein erster

Alisalz

1 TODICITI

Ein zweite Ansatz

Probleme 2

AnonAcces

Probleme und

3 Stufen

Konzept



AnonAccess

Heisrath,
Daniel Otte

blem

, unorabiang

Бединістк

Ansatz

Problem

Ein zweite Ansatz

Probleme 2

Probleme und

3 Stufen

Konzept

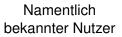


Namentlich bekannter Nutzer

AnonAccess

3 Stufen

Konzept



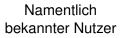


Pseudonym

AnonAccess

Konzept

3 Stufen





Pseudonym



shared Pseudonym ("Anonym")



AnonAccess

3 Stufen

Konzept



AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpro

Anforderunge

_

ein erste

Problem

Ein zweite

Probleme 2

Probleme un

Lösungen

3 Stufen Konzept

EOP

Name wird in der Ticket-DB hinterlegt

AnonAccess

3 Stufen

Konzept

Name wird in der Ticket-DB hinterlegt

anonym-Flag ← 0

AnonAccess

3 Stufen

Konzept

Name wird in der Ticket-DB hinterlegt

anonym-Flag ← 0

Name ist auch Pseudonym

Pseudonym

AnonAccess

Soren Heisrath, Daniel Otte

ichlüsselpro

Anforderunger

Begrifflichkeit

ein erster

71110012

Ein zweite

Droblomo !

AnonAcces

Probleme un

3 Stufen

Konzept

EOP

Pseudonym

AnonAccess

Sören Heisrath, Daniel Otte

Schlüsselpro

Anforderunge

D

ein erste

Ansatz

Problem

Ein zweite Ansatz

Probleme 2

Probleme und

Lösungen

3 Stufen Konzept

EOB

es wird kein Name gespeichert

Pseudonym

AnonAccess

3 Stufen Konzept

es wird kein Name gespeichert

anonym-Flag ← 1

Pseudonym

AnonAccess

3 Stufen

Konzept

es wird kein Name gespeichert

■ anonym-Flag ← 1

individuelles Pseudonym

AnonAccess

3 Stufen Konzept



AnonAccess

3 Stufen Konzept

es wird kein Name gespeichert

AnonAccess

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

Probleme

AnonAccess

3 Stufen

Konzept

Problem:

Das gezielte Löschen von anonymen Nutzern ist nicht möglich.

Lösung

AnonAccess

3 Stufen

Konzept

Lokale Policies:

Lösung

AnonAccess

Soren Heisrath, Daniel Ott

Schlüsselpro

Anforderunge

ein erster Ansatz

Problem

Ein zweite

Probleme 2

ΛησηΛοσο

Probleme ur

3 Stufen Konzept

Lokale Policies:

Timeouts

Lösung

AnonAccess

3 Stufen

Konzept

Lokale Policies:

- Timeouts
- Nur Pseudonymisierte Nutzer dürfen Admin sein

EOP

AnonAccess

Heisrath Daniel Ot

Schlüsselpro blem

Anforderunge

Begrifflichkei

Ansatz

Problem

Ein zweite Ansatz

Probleme 2

AnonAccess

Probleme u

3 Stufer Konzent

EOP

End Of Presentation