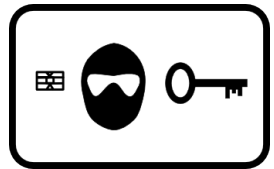


# AnonAccess

Sören Heisrath   Daniel Otte



27. Dezember 2007

# Unser Schlüsselpproblem:

AnonAccess

Sören  
Heisrath,  
Daniel Otte

Schlüsselp-  
problem

Anforderungen

Begrifflichkeiten

ein erster  
Ansatz

Probleme

Ein zweiter  
Ansatz

Probleme 2

AnonAccess

Probleme und  
Lösungen

3 Stufen  
Konzept

EOP

- viele Leute
- wenig Schlüssel
- wenig Geld

# Erste Überlegungen

AnonAccess

Sören  
Heisrath,  
Daniel Otte

Schlüsselproblem

Anforderungen

Begrifflichkeiten

ein erster  
Ansatz

Probleme

Ein zweiter  
Ansatz

Probleme 2

AnonAccess

Probleme und  
Lösungen

3 Stufen  
Konzept

EOP

- Mechanische Schlüssel kann man einfach nachmachen
- Schliesssysteme sind teuer
- $\Rightarrow$  wir müssen was Eigenes machen

AnonAccess

Sören  
Heisrath,  
Daniel Otte

Schlüsselproblem

Anforderungen

Begrifflichkeiten

ein erster  
Ansatz

Probleme

Ein zweiter  
Ansatz

Probleme 2

AnonAccess

Probleme und  
Lösungen

3 Stufen  
Konzept

EOP

- Speicherkarten oder SmartCards
- Microcontroller-Plattform

# Kostenabschätzung

AnonAccess

Sören  
Heisrath,  
Daniel Otte

Schlüsselproblem

Anforderungen

Begrifflichkeiten

ein erster  
Ansatz

Probleme

Ein zweiter  
Ansatz

Probleme 2

AnonAccess

Probleme und  
Lösungen

3 Stufen  
Konzept

EOP

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

# Elegante Lösung

AnonAccess

Sören  
Heisrath,  
Daniel Otte

Schlüsselproblem

Anforderungen

Begrifflichkeiten

ein erster  
Ansatz

Probleme

Ein zweiter  
Ansatz

Probleme 2

AnonAccess

Probleme und  
Lösungen

3 Stufen  
Konzept

EOP

- einfach zu realisieren
- günstig
- sicher

# Anonymität

AnonAccess

Sören  
Heisrath,  
Daniel Otte

Schlüsselpro-  
blem

Anforderungen

Begrifflichkeiten

ein erster  
Ansatz

Probleme

Ein zweiter  
Ansatz

Probleme 2

AnonAccess

Probleme und  
Lösungen

3 Stufen  
Konzept

EOP

Karten sollen anonym wie Schlüssel sein

# Prüfsummen

AnonAccess

Sören  
Heisrath,  
Daniel Otte

Schlüsselproblem

Anforderungen

Begrifflichkeiten

ein erster  
Ansatz

Probleme

Ein zweiter  
Ansatz

Probleme 2

AnonAccess

Probleme und  
Lösungen

3 Stufen  
Konzept

EOP

z.B. eine Quersumme über eine Zahl.



# Problem

AnonAccess

Sören  
Heisrath,  
Daniel Otte

Schlüsselpro-  
blem

Anforderungen

Begrifflichkeiten

ein erster  
Ansatz

Probleme

Ein zweiter  
Ansatz

Probleme 2

AnonAccess

Probleme und  
Lösungen

3 Stufen  
Konzept

EOP

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

# Hashfunktionen

AnonAccess

Sören  
Heisrath,  
Daniel Otte

Schlüsselpro-  
blem

Anforderungen

Begrifflichkeiten

ein erster  
Ansatz

Probleme

Ein zweiter  
Ansatz

Probleme 2

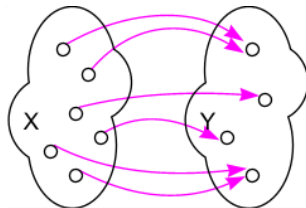
AnonAccess

Probleme und  
Lösungen

3 Stufen  
Konzept

EOP

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



# Hash-MACs

AnonAccess

Sören  
Heisrath,  
Daniel Otte

Schlüsselproblem

Anforderungen

Begrifflichkeiten

ein erster  
Ansatz

Probleme

Ein zweiter  
Ansatz

Probleme 2

AnonAccess

Probleme und  
Lösungen

3 Stufen  
Konzept

EOP

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

$$HMAC_k(msg) = hash((k \oplus opad) \parallel hash((k \oplus ipad) \parallel msg))$$

# Ansatz 1

AnonAccess

Sören  
Heisrath,  
Daniel Otte

Schlüsselproblem

Anforderungen

Begrifflichkeiten

ein erster  
Ansatz

Probleme

Ein zweiter  
Ansatz

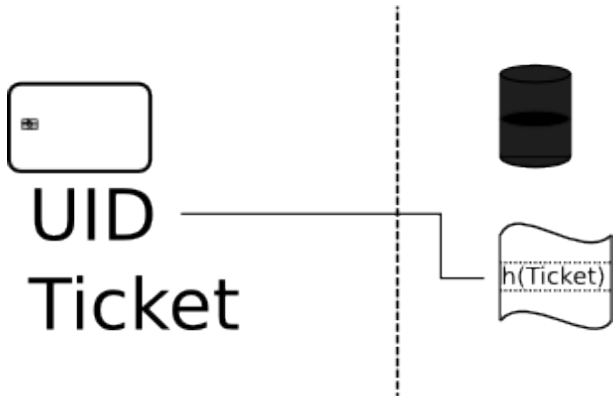
Probleme 2

AnonAccess

Probleme und  
Lösungen

3 Stufen  
Konzept

EOP



# Ansatz 1 – Ablauf

AnonAccess

Sören  
Heisrath,  
Daniel Otte

Schlüsselproblem

Anforderungen

Begrifflichkeiten

ein erster  
Ansatz

Probleme

Ein zweiter  
Ansatz

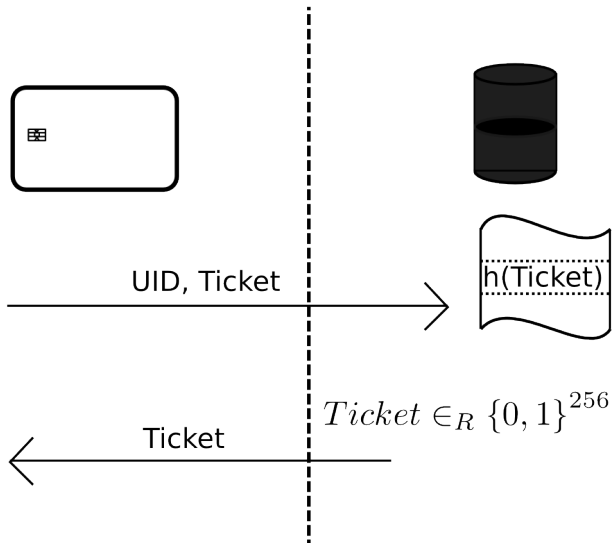
Probleme 2

AnonAccess

Probleme und  
Lösungen

3 Stufen  
Konzept

EOP



# Ticket-DB Struktur

AnonAccess

Sören  
Heisrath,  
Daniel Otte

Schlüsselpro-  
blem

Anforderungen

Begrifflichkeiten

ein erster  
Ansatz

Probleme

Ein zweiter  
Ansatz

Probleme 2

AnonAccess

Probleme und  
Lösungen

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

Sören  
Heisrath,  
Daniel Otte

Schlüsselpro-  
blem

Anforderungen

Begrifflichkeiten

ein erster  
Ansatz

**Probleme**

Ein zweiter  
Ansatz

Probleme 2

AnonAccess

Probleme und  
Lösungen

3 Stufen  
Konzept

EOP

# Ansatz 1 – Probleme

AnonAccess

Sören  
Heisrath,  
Daniel Otte

Schlüsselpro-  
blem

Anforderungen

Begrifflichkeiten

ein erster  
Ansatz

**Probleme**

Ein zweiter  
Ansatz

Probleme 2

AnonAccess

Probleme und  
Lösungen

3 Stufen  
Konzept

EOP

■ nur pseudonym



# Ansatz 1 – Probleme

AnonAccess

Sören  
Heisrath,  
Daniel Otte

Schlüsselpro-  
blem

Anforderungen

Begrifflichkeiten

ein erster  
Ansatz

**Probleme**

Ein zweiter  
Ansatz

Probleme 2

AnonAccess

Probleme und  
Lösungen

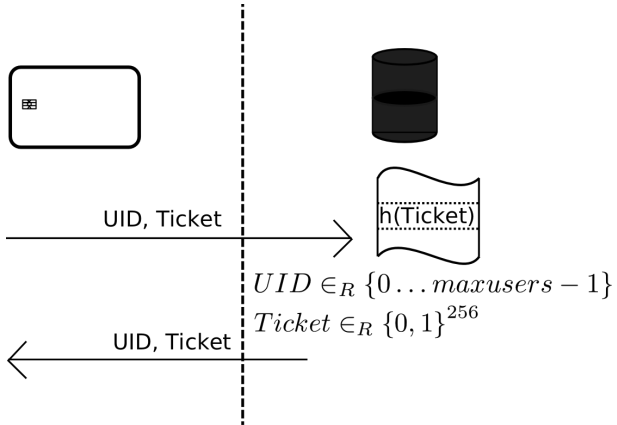
3 Stufen  
Konzept

EOP

- nur pseudonym
- pseudonym schwer merkbar

# Ansatz 2

neue, zufällige UUIDs



# Ansatz 2 – Probleme

AnonAccess

Sören  
Heisrath,  
Daniel Otte

Schlüsselpro-  
blem

Anforderungen

Begrifflichkeiten

ein erster  
Ansatz

Probleme

Ein zweiter  
Ansatz

**Probleme 2**

AnonAccess

Probleme und  
Lösungen

3 Stufen  
Konzept

EOP

# Ansatz 2 – Probleme

AnonAccess

Sören  
Heisrath,  
Daniel Otte

Schlüsselproblem

Anforderungen

Begrifflichkeiten

ein erster  
Ansatz

Probleme

Ein zweiter  
Ansatz

**Probleme 2**

AnonAccess

Probleme und  
Lösungen

3 Stufen  
Konzept

EOP

- keine feste Referenz auf Nutzer

# Ansatz 2 – Probleme

AnonAccess

Sören  
Heisrath,  
Daniel Otte

Schlüsselproblem

Anforderungen

Begrifflichkeiten

ein erster  
Ansatz

Probleme

Ein zweiter  
Ansatz

**Probleme 2**

AnonAccess

Probleme und  
Lösungen

3 Stufen  
Konzept

EOP

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

# AnonAccess

## AnonAccess

Sören  
Heisrath,  
Daniel Otte

Schlüsselproblem

Anforderungen

Begrifflichkeiten

ein erster  
Ansatz

Probleme

Ein zweiter  
Ansatz

Probleme 2

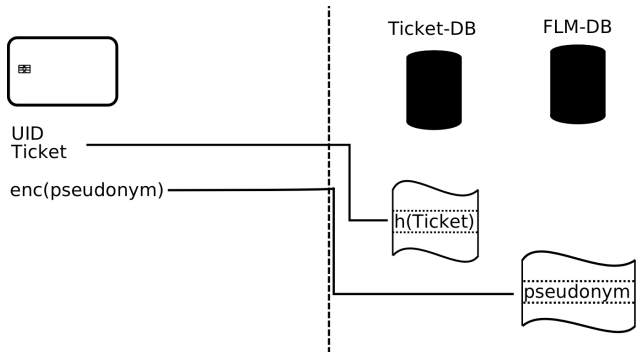
AnonAccess

Probleme und  
Lösungen

3 Stufen  
Konzept

EOP

## Zusätzliche Datenbank für Änderungen



# AnonAccess Ablauf

## AnonAccess

Sören  
Heisrath,  
Daniel Otte

Schlüsselproblem

Anforderungen

Begrifflichkeiten

ein erster  
Ansatz

Probleme

Ein zweiter  
Ansatz

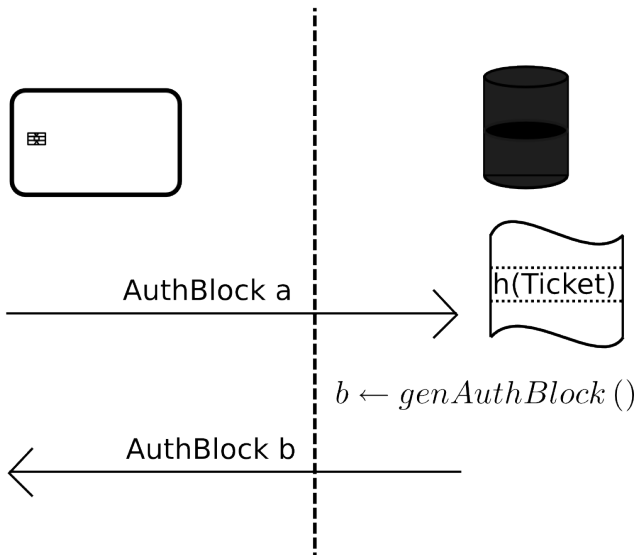
Probleme 2

AnonAccess

Probleme und  
Lösungen

3 Stufen  
Konzept

EOP



# AuthBlock Struktur

AnonAccess

Sören  
Heisrath,  
Daniel Otte

Schlüsselproblem

Anforderungen

Begrifflichkeiten

ein erster  
Ansatz

Probleme

Ein zweiter  
Ansatz

Probleme 2

AnonAccess

Probleme und  
Lösungen

3 Stufen  
Konzept

EOP

## AuthBlock Struktur:

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 vorangegangenen Daten



# FLM-DB Struktur

AnonAccess

Sören  
Heisrath,  
Daniel Otte

Schlüsselproblem

Anforderungen

Begrifflichkeiten

ein erster  
Ansatz

Probleme

Ein zweiter  
Ansatz

Probleme 2

AnonAccess

Probleme und  
Lösungen

3 Stufen  
Konzept

EOP

## FLM-DB Struktur:

active	ist dieser Eintrag aktiviert
permanent	soll der Eintrag nach anwendung gelöscht 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

Schlüsselproblem

Anforderungen

Begrifflichkeiten

ein erster  
Ansatz

Probleme

Ein zweiter  
Ansatz

Probleme 2

AnonAccess

**Probleme und  
Lösungen**

3 Stufen  
Konzept

EOP

Lösung: Datenbank wird verschlüsselt.

# Nutzer entfernen

AnonAccess

Sören  
Heisrath,  
Daniel Otte

Schlüsselproblem

Anforderungen

Begrifflichkeiten

ein erster  
Ansatz

Probleme

Ein zweiter  
Ansatz

Probleme 2

AnonAccess

**Probleme und  
Lösungen**

3 Stufen  
Konzept

EOP

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

# 3 Stufen Konzept

AnonAccess

Sören  
Heisrath,  
Daniel Otte

Schlüsselproblem

Anforderungen

Begrifflichkeiten

ein erster  
Ansatz

Probleme

Ein zweiter  
Ansatz

Probleme 2

AnonAccess

Probleme und  
Lösungen

3 Stufen  
Konzept

EOP

# 3 Stufen Konzept

AnonAccess

Sören  
Heisrath,  
Daniel Otte

Schlüsselproblem

Anforderungen

Begrifflichkeiten

ein erster  
Ansatz

Probleme

Ein zweiter  
Ansatz

Probleme 2

AnonAccess

Probleme und  
Lösungen

3 Stufen  
Konzept

EOP



Namentlich  
bekannter Nutzer

# 3 Stufen Konzept

AnonAccess

Sören  
Heisrath,  
Daniel Otte

Schlüsselproblem

Anforderungen

Begrifflichkeiten

ein erster  
Ansatz

Probleme

Ein zweiter  
Ansatz

Probleme 2

AnonAccess

Probleme und  
Lösungen

3 Stufen  
Konzept

EOP



Namentlich  
bekannter Nutzer



Pseudonym

# 3 Stufen Konzept

AnonAccess

Sören  
Heisrath,  
Daniel Otte

Schlüsselpro-  
blem

Anforderungen

Begrifflichkeiten

ein erster  
Ansatz

Probleme

Ein zweiter  
Ansatz

Probleme 2

AnonAccess

Probleme und  
Lösungen

3 Stufen  
Konzept

EOP



Namentlich  
bekannter Nutzer



Pseudonym



shared  
Pseudonym  
("Anonym")

# Namentlich bekannt

AnonAccess

Sören  
Heisrath,  
Daniel Otte

Schlüsselpro-  
blem

Anforderungen

Begrifflichkeiten

ein erster  
Ansatz

Probleme

Ein zweiter  
Ansatz

Probleme 2

AnonAccess

Probleme und  
Lösungen

3 Stufen  
Konzept

EOP



# Namentlich bekannt

AnonAccess

Sören  
Heisrath,  
Daniel Otte

Schlüsselproblem

Anforderungen

Begrifflichkeiten

ein erster  
Ansatz

Probleme

Ein zweiter  
Ansatz

Probleme 2

AnonAccess

Probleme und  
Lösungen

3 Stufen  
Konzept

EOP

- Name wird in der Ticket-DB hinterlegt

# Namentlich bekannt

AnonAccess

Sören  
Heisrath,  
Daniel Otte

Schlüsselproblem

Anforderungen

Begrifflichkeiten

ein erster  
Ansatz

Probleme

Ein zweiter  
Ansatz

Probleme 2

AnonAccess

Probleme und  
Lösungen

3 Stufen  
Konzept

EOP

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

# Namentlich bekannt

AnonAccess

Sören  
Heisrath,  
Daniel Otte

Schlüsselproblem

Anforderungen

Begrifflichkeiten

ein erster  
Ansatz

Probleme

Ein zweiter  
Ansatz

Probleme 2

AnonAccess

Probleme und  
Lösungen

3 Stufen  
Konzept

EOP

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

# Pseudonym

AnonAccess

Sören  
Heisrath,  
Daniel Otte

Schlüsselpro-  
blem

Anforderungen

Begrifflichkeiten

ein erster  
Ansatz

Probleme

Ein zweiter  
Ansatz

Probleme 2

AnonAccess

Probleme und  
Lösungen

3 Stufen  
Konzept

EOP

# Pseudonym

AnonAccess

Sören  
Heisrath,  
Daniel Otte

Schlüsselproblem

Anforderungen

Begrifflichkeiten

ein erster  
Ansatz

Probleme

Ein zweiter  
Ansatz

Probleme 2

AnonAccess

Probleme und  
Lösungen

3 Stufen  
Konzept

EOP

- es wird kein Name gespeichert

# Pseudonym

AnonAccess

Sören  
Heisrath,  
Daniel Otte

Schlüsselproblem

Anforderungen

Begrifflichkeiten

ein erster  
Ansatz

Probleme

Ein zweiter  
Ansatz

Probleme 2

AnonAccess

Probleme und  
Lösungen

3 Stufen  
Konzept

EOP

- es wird kein Name gespeichert
- anonym-Flag  $\leftarrow 1$

# Pseudonym

AnonAccess

Sören  
Heisrath,  
Daniel Otte

Schlüsselproblem

Anforderungen

Begrifflichkeiten

ein erster  
Ansatz

Probleme

Ein zweiter  
Ansatz

Probleme 2

AnonAccess

Probleme und  
Lösungen

3 Stufen  
Konzept

EOP

- es wird kein Name gespeichert
- anonym-Flag  $\leftarrow 1$
- individuelles Pseudonym

# shared Pseudonym

AnonAccess

Sören  
Heisrath,  
Daniel Otte

Schlüsselproblem

Anforderungen

Begrifflichkeiten

ein erster  
Ansatz

Probleme

Ein zweiter  
Ansatz

Probleme 2

AnonAccess

Probleme und  
Lösungen

3 Stufen  
Konzept

EOP



# shared Pseudonym

AnonAccess

Sören  
Heisrath,  
Daniel Otte

Schlüsselproblem

Anforderungen

Begrifflichkeiten

ein erster  
Ansatz

Probleme

Ein zweiter  
Ansatz

Probleme 2

AnonAccess

Probleme und  
Lösungen

3 Stufen  
Konzept

EOP

- es wird kein Name gespeichert

# shared Pseudonym

AnonAccess

Sören  
Heisrath,  
Daniel Otte

Schlüsselpro-  
blem

Anforderungen

Begrifflichkeiten

ein erster  
Ansatz

Probleme

Ein zweiter  
Ansatz

Probleme 2

AnonAccess

Probleme und  
Lösungen

3 Stufen  
Konzept

EOP

- es wird kein Name gespeichert
- anonym-Flag  $\leftarrow 1$

# shared Pseudonym

AnonAccess

Sören  
Heisrath,  
Daniel Otte

Schlüsselpro-  
blem

Anforderungen

Begrifflichkeiten

ein erster  
Ansatz

Probleme

Ein zweiter  
Ansatz

Probleme 2

AnonAccess

Probleme und  
Lösungen

3 Stufen  
Konzept

EOP

- es wird kein Name gespeichert
- anonym-Flag  $\leftarrow 1$
- Gruppen-Pseudonym

# Probleme

AnonAccess

Sören  
Heisrath,  
Daniel Otte

Schlüsselproblem

Anforderungen

Begrifflichkeiten

ein erster  
Ansatz

Probleme

Ein zweiter  
Ansatz

Probleme 2

AnonAccess

Probleme und  
Lösungen

3 Stufen  
Konzept

EOP

Problem:

Das gezielte Löschen von anonymen Nutzern ist nicht möglich.

AnonAccess

Sören  
Heisrath,  
Daniel Otte

Schlüsselproblem

Anforderungen

Begrifflichkeiten

ein erster  
Ansatz

Probleme

Ein zweiter  
Ansatz

Probleme 2

AnonAccess

Probleme und  
Lösungen

3 Stufen  
Konzept

EOP

## Lokale Policies:

AnonAccess

Sören  
Heisrath,  
Daniel Otte

Schlüsselproblem

Anforderungen

Begrifflichkeiten

ein erster  
Ansatz

Probleme

Ein zweiter  
Ansatz

Probleme 2

AnonAccess

Probleme und  
Lösungen

3 Stufen  
Konzept

EOP

## Lokale Policies:

- Timeouts

AnonAccess

Sören  
Heisrath,  
Daniel Otte

Schlüsselproblem

Anforderungen

Begrifflichkeiten

ein erster  
Ansatz

Probleme

Ein zweiter  
Ansatz

Probleme 2

AnonAccess

Probleme und  
Lösungen

3 Stufen  
Konzept

EOP

## Lokale Policies:

- Timeouts
- Nur Pseudonymisierte Nutzer dürfen Admin sein

AnonAccess

Sören  
Heisrath,  
Daniel Otte

Schlüsselproblem

Anforderungen

Begrifflichkeiten

ein erster  
Ansatz

Probleme

Ein zweiter  
Ansatz

Probleme 2

AnonAccess

Probleme und  
Lösungen

3 Stufen  
Konzept

EOP

# End Of Presentation