AnonAccess

Sören Heisrath Daniel Otte





20. Dezember 2007

- 1 Anforderungen & Beispiele
- 2 Begriffe und Vorraussetzungen
- 3 Aufbau
- 4 Mögliche (alternative) Implementationen
- 5 AnonAccess Konzept

AnonAccess Sören

Heisrath, Daniel Otte

Anforderungen & Beispiele

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative) Implementationen

AnonAccess Konzept

Anforderungen

- Wartbarkeit
- Sicherheit
- Anonymität
- Kostengünstig (Komplette Anlage
- Transparenz

Anforderungen

Anforderungen & Beispiele

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative) Implementationen

AnonAccess Konzept

Wartbarkeit

AnonAccess

Sören Heisrath, Daniel Otte

Anforderungen & Beispiele

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative) Implementationen

AnonAccess Konzept

Anforderungen

- Wartbarkeit
- Sicherheit
- Anonymität
- Kostengünstig (Komplette Anlage 100€)
- Iransparenz

Anforderungen

Anforderungen & Beispiele

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative) Implementationen

- Wartbarkeit
- Sicherheit
- Anonymität
- Kostengünstig (Komplette Anlage 100€)
- Transparenz

Begriffe und

Anforderungen

- Wartbarkeit
- Sicherheit
- Anonymität
- Kostengünstig (Komplette Anlage 100€)

Transparenz

AnonAccess Konzept

Anforderungen

- Wartbarkeit
- Sicherheit
- Anonymität
- Kostengünstig (Komplette Anlage 100€)
- Transparenz

Anforderungen & Beispiele

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative) Implementationen

- Hinzufügen von Nutzern
- Löschen von Nutzern
- Sperren von Nutzern (mit und ohne Karte)
- Privilegien verwalten

Anforderungen & Beispiele

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative) Implementationen

AnonAccess Konzept

• Hinzufügen von Nutzern

- Löschen von Nutzern
- Sperren von Nutzern (mit und ohne Karte)
- Privilegien verwalten

Anforderungen & Beispiele

Begriffe und Vorraussetzungen

Aufbau

tionen

Mögliche (alternative) Implementa-

- Hinzufügen von Nutzern
- Löschen von Nutzern
- Sperren von Nutzern (mit und ohne Karte)
- Privilegien verwalten

Anforderungen & Beispiele

Begriffe und Vorraussetzungen

Aufbau

tionen

Mögliche (alternative) Implementa-

AnonAccess Konzept • Hinzufügen von Nutzern

- Löschen von Nutzern
- Sperren von Nutzern (mit und ohne Karte)
- Privilegien verwalten

AnonAccess

Sören Heisrath, Daniel Otte

Anforderungen & Beispiele

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative) Implementationen

AnonAccess Konzept

Sicherheit

- Zugang beschränken auf berechtigte Personen
- Verhindern des Kopierens der Zugangsberechtigung
- Sicherheit sollte vergleichbar sein mit konventioneller
 Schlägende

Begriffe und Vorraussetzungen

Aufbau

.

Mögliche (alternative) Implementationen

- Zugang beschränken auf berechtigte Personen
- Verhindern des Kopierens der Zugangsberechtigung
- Sicherheit sollte vergleichbar sein mit konventioneller Schlüsseln

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative)

Implementationen

- Zugang beschränken auf berechtigte Personen
- Verhindern des Kopierens der Zugangsberechtigung
- Sicherheit sollte vergleichbar sein mit konventioneller Schlüsseln

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative)

Implementa-

- Zugang beschränken auf berechtigte Personen
- Verhindern des Kopierens der Zugangsberechtigung
- Sicherheit sollte vergleichbar sein mit konventionellen Schlüsseln

Anonymität

Anforderungen & Beispiele

Begriffe und Vorraussetzungen

Aufbau

Autoa

Mögliche (alternative) Implementationen

- Schutz der Persönlichen Daten auch vor starken Angreifern
- Ein Angreifer soll nicht von der Karte auf die Zugehörigkeit zu einem System schließen könner
- Ein Angreifer soll nicht von der Analyse des Systems auf den Nutzerkreis schließen dürfen
- Anonymität sollte vergleichbar sein mit konventionellen Schlüsseln

Anonymität

Anforderungen & Beispiele

Begriffe und Vorraussetzungen

Aufbau

Mäaliol

Mögliche (alternative) Implementationen

- Schutz der Persönlichen Daten auch vor starken Angreifern
- Ein Angreifer soll nicht von der Karte auf die Zugehörigkeit zu einem System schließen können
- Ein Angreifer soll nicht von der Analyse des Systems auf den Nutzerkreis schließen dürfen
- Anonymität sollte vergleichbar sein mit konventionellen Schlüsseln

Begriffe und Vorraussetzungen

Aufbau

Autba

Mögliche (alternative) Implementationen

AnonAccess Konzept

Anonymität

- Schutz der Persönlichen Daten auch vor starken Angreifern
- Ein Angreifer soll nicht von der Karte auf die Zugehörigkeit zu einem System schließen können
- Ein Angreifer soll nicht von der Analyse des Systems auf den Nutzerkreis schließen dürfen
- Anonymität sollte vergleichbar sein mit konventionellen Schlüsseln

Aufbau

Mögliche (alternative) Implementationen

AnonAccess Konzept

Anonymität

- Schutz der Persönlichen Daten auch vor starken. Angreifern
- Ein Angreifer soll nicht von der Karte auf die Zugehörigkeit zu einem System schließen können
- Ein Angreifer soll nicht von der Analyse des Systems auf den Nutzerkreis schließen dürfen

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative)

(alternative) Implementationen

- Schutz der Persönlichen Daten auch vor starken Angreifern
- Ein Angreifer soll nicht von der Karte auf die Zugehörigkeit zu einem System schließen können
- Ein Angreifer soll nicht von der Analyse des Systems auf den Nutzerkreis schließen dürfen
- Anonymität sollte vergleichbar sein mit konventionellen Schlüsseln

AnonAccess

Sören Heisrath, Daniel Otte

Anforderungen & Beispiele

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative)

(alternative) Implementationen

AnonAccess Konzept

Kostengünstig

- geringe Kosten f
 ür die Hardware des Systems
- geringe Kosten je Nutzer
- einfache Herstellung (für den Nachbau geeignet)

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative)

Implementationen

AnonAccess Konzept

Kostengünstig

- geringe Kosten für die Hardware des Systems
- geringe kosten je Nutzer
- einfache Herstellung (für den Nachbau geeignet)

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative)

(alternative) Implementationen

AnonAccess Konzept

Kostengünstig

- geringe Kosten für die Hardware des Systems
- geringe Kosten je Nutzer

einfache Herstellung (für den Nachbau geeignet)

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative)

Implementationen

AnonAccess Konzept

Kostengünstig

- geringe Kosten für die Hardware des Systems
- geringe Kosten je Nutzer
- einfache Herstellung (für den Nachbau geeignet)

Begriffe und Vorraussetzungen

Aufbau

- -----

Mögliche (alternative) Implementationen

- Software ist OpenSource (GPLv3)
- Schaltpläne für die Hardware liegen offen
- Keine "Security by Obscurity"
- Die Sicherheit hangt von der Geheimhaltung des Schlüssels ab nicht von der Geheimhaltung des
- Verfahrens (Kerkhofs Gesetz)

Begriffe und Vorraussetzungen

Aufbau

Mögliche

(alternative) Implementationen

AnonAccess Konzept

• Software ist OpenSource (GPLv3)

- Schaltpläne für die Hardware liegen offen
- Keine "Security by Obscurity"
- Die Sicherheit h\u00e4ngt von der Geheimhaltung des Schl\u00fcssels ab, nicht von der Geheimhaltung des Verfahrens. (Kerkhofs Gesetz)

Transparenz

Anforderungen & Beispiele

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative) Implementationen

- Software ist OpenSource (GPLv3)
- Schaltpläne für die Hardware liegen offen
- Keine "Security by Obscurity"
- Die Sicherheit hängt von der Geheimhaltung des Schlüssels ab, nicht von der Geheimhaltung des Verfahrens. (Kerkhofs Gesetz)

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative)

(alternative) Implementationen

AnonAccess Konzept

Transparenz

- Software ist OpenSource (GPLv3)
- Schaltpläne für die Hardware liegen offen
- Keine "Security by Obscurity"
- Die Sicherheit hängt von der Geheimhaltung des Schlüssels ab, nicht von der Geheimhaltung des Verfahrens. (Kerkhofs Gesetz)

Begriffe und Vorraussetzungen

& Beispiele

Aufbau

Mögliche

(alternative) Implementationen

AnonAccess Konzept Einmal verwendbarer Datensatz zur Authentifikation. Das Ticket wird vom System überprüft und bei erfolgreiche Prüfung (Authentifikation) wird ein neues Ticket ausgegeben

Hash-Funktion

& Beispiele

Begriffe und

Vorraussetzungen

Aufbau

Mögliche (alternative) Implementationen

AnonAccess Konzept Eine Hashfunktion bildet eine beliebig große Datenmenge eindeutig auf eine Datenmenge fester Größe ab (Message-Digest oder Fingerprint).

Eine wichtige Anforderung an eine derartig Funktion ist die sogenannte Kollisionsfreiheit, d.h. obwohl es prinzipiell mehrere Nachrichten gibt die den gleichen Fingerprint haben ist es schwierig zwei derartige Nachrichten zu finden.

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative) Implementationen

AnonAccess Konzept Verwendung einer Speicherkarte zum speichern der Authentifizierungsdaten.

Aufteilung in **Master** und **Terminal** um:

- Aufgaben Verteilung
- Besondere Sicherung der Master Unit

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative) Implementationen

AnonAccess Konzept Verwendung einer Speicherkarte zum speichern der Authentifizierungsdaten.

Aufteilung in Master und Terminal um:

- Aufgaben Verteilung
- Besondere Sicherung der Master Unit

System

Anforderungen & Beispiele Begriffe und

Vorraussetzungen

Aufbau

Mögliche (alternative) Implementationen

AnonAccess Konzept Verwendung einer Speicherkarte zum speichern der Authentifizierungsdaten.

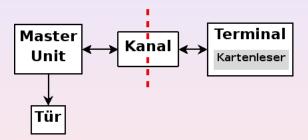
Aufteilung in Master und Terminal um:

- Aufgaben Verteilung
- Besondere Sicherung der Master Unit

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative) Implementationen



Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative) Implementationen

- Speicherung der Datenbank
- Authentifizierung der Nutzer
- Löschung der Schlüssel & Datenbank bei physikalischen Angriffen
- Unterbrechungsfrei Stromversorgung (USV)

Anforderungen & Beispiele

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative) Implementationen

- Speicherung der Datenbank
- Authentifizierung der Nutzer
- Loschung der Schlüssel & Datenbank bei physikalischen Angriffen
- Unterbrechungsfrei Stromversorgung (USV)

Anforderungen & Beispiele

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative) Implementationen

- Speicherung der Datenbank
- Authentifizierung der Nutzer
- Löschung der Schlüssel & Datenbank bei physikalischen Angriffen
- Unterbrechungsfrei Stromversorgung (USV)

Anforderungen & Beispiele Begriffe und

Vorraussetzungen Aufbau

Auibu

Mögliche (alternative) Implementationen

AnonAccess Konzept

- Speicherung der Datenbank
- Authentifizierung der Nutzer
- Löschung der Schlüssel & Datenbank bei physikalischen Angriffen

Unterbrechungsfrei Stromversorgung (USV)

Anforderungen & Beispiele

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative) Implementationen

- Speicherung der Datenbank
- Authentifizierung der Nutzer
- Löschung der Schlüssel & Datenbank bei physikalischen Angriffen
- Unterbrechungsfrei Stromversorgung (USV)

AnonAccess Sören

Sören Heisrath, Daniel Otte

Terminal/Panel

Anforderungen & Beispiele

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative) Implementationen

- Weitergabe der Kartendaten
- Ein- und Ausgabe (Master Unit <-> Mensch)
- Loschung des Schlussels bei physikalischen Angriffen

Terminal/Panel

Anforderungen & Beispiele

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative) Implementationen

- Weitergabe der Kartendaten
- Ein- und Ausgabe (Master Unit <-> Mensch)
- Löschung des Schlüssels bei physikalischen Angritter

Terminal/Panel

Anforderungen & Beispiele

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative) Implementationen

- Weitergabe der Kartendaten
- Ein- und Ausgabe (Master Unit <-> Mensch)
- Löschung des Schlüssels bei physikalischen Angriffen

Terminal/Panel

Anforderungen & Beispiele

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative) Implementationen

- Weitergabe der Kartendaten
- Ein- und Ausgabe (Master Unit <-> Mensch)
- Löschung des Schlüssels bei physikalischen Angriffen

AnonAccess Sören

Heisrath, Daniel Otte

Kanal (logisch)

Anforderungen & Beispiele

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative) Implementationen

AnonAccess Konzept Verbindung über kryptografisch sicheren Kanal

- Integritat
- Authentizität
- Vertraulichkeit

Kanal (logisch)

Anforderungen & Beispiele

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative) Implementationen

AnonAccess Konzept Verbindung über kryptografisch sicheren Kanal

- Integrität
- Authentizität
- Vertraulichkeit

Kanal (logisch)

Anforderungen & Beispiele

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative) Implementationen

AnonAccess Konzept Verbindung über kryptografisch sicheren Kanal

- Integrität
- Authentizität

Vertraulichkeit

Kanal (logisch)

Anforderungen & Beispiele Begriffe und

Vorraussetzungen

Autba

Mögliche (alternative) Implementationen

AnonAccess Konzept Verbindung über kryptografisch sicheren Kanal

- Integrität
- Authentizität
- Vertraulichkeit

Kanal (physikalisch)

Anforderungen & Beispiele

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative) Implementationen

AnonAccess Konzept Galvanische Trennung zwischen Master Unit und Panel, z.B.

Funk

LWL / Optokoppler

AnonAccess Sören

Heisrath, Daniel Otte

Kanal (physikalisch)

Anforderungen & Beispiele

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative) Implementationen

AnonAccess Konzept Galvanische Trennung zwischen Master Unit und Panel, z.B.

Funk

LWL / Optokoppler

Kanal (physikalisch)

& Beispiele Begriffe und Vorrausset-

Aufbau

zungen

Mögliche

(alternative) Implementationen

AnonAccess Konzept

Galvanische Trennung zwischen Master Unit und Panel, z.B.

- Funk
- LWL / Optokoppler

Speicherkarte

Anforderungen & Beispiele

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative) Implementationen

AnonAccess Konzept

- Chipkartenformat: handlich
- Günstig: ¡ 1 € pro Stück
- Transparent: Daten können von jedem nach belieben ausgelesen werden.

Speicherkarte

Anforderungen & Beispiele Begriffe und

Vorraussetzungen

Aufbau

Mögliche (alternative) Implementationen

AnonAccess Konzept

- Chipkartenformat: handlich
- Günstig: ¡ 1 € pro Stück
- Transparent: Daten können von jedem nach belieben ausgelesen werden.

Speicherkarte

Anforderungen & Beispiele Begriffe und

Vorraussetzungen

Aufbau

Mögliche (alternative) Implementationen

AnonAccess Konzept

- Chipkartenformat: handlich
- Günstig: ¡ 1 € pro Stück
- Transparent: Daten können von jedem nach belieben ausgelesen werden.

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative) Implementationen

AnonAccess Konzept

- Chipkartenformat: handlich
- Günstig: ¡ 1 € pro Stück
- Transparent: Daten können von jedem nach belieben ausgelesen werden.

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative) Implementationen

AnonAccess Konzept Daten auf der Karte:

• User ID

Licket

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative) Implementationen

AnonAccess Konzept Daten auf der Karte:

• User ID

Ticket

Daten im System für jeden Nutzer:

Licket (oder Fingerprint des Lickets)

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative)

Implementationen

AnonAccess Konzept

Daten auf der Karte:

- User ID
- Ticket

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative) Implementationen

AnonAccess Konzept

Daten auf der Karte:

- User ID
- Ticket

- Ticket (oder Fingerprint des Tickets)
- Berechtigungen (sog. Flags)

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative) Implementationen

AnonAccess Konzept

Daten auf der Karte:

- User ID
- Ticket

- Ticket (oder Fingerprint des Tickets)
- Berechtigungen (sog. Flags)

Anforderungen & Beispiele

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative

(alternative) Implementationen

AnonAccess Konzept

- Auslesen der User ID und des Tickets von der Karte
- 2 Auslesen der des Tickets aus der Nutzerdatenbank
- 3 Uberprüfen des Tickets
- 4 Generieren eines neuen Tickets
- 5 Schreiben des neuen Tickets auf die Karte

Anforderungen & Beispiele

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative) Implementationen

AnonAccess Konzept

- 1 Auslesen der User ID und des Tickets von der Karte
- 2 Auslesen der des Tickets aus der Nutzerdatenbank
- 3 Uberprüfen des Tickets
- 4 Generieren eines neuen Tickets
- 5 Schreiben des neuen Tickets auf die Karte

Anforderungen & Beispiele

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative) Implementationen

AnonAccess Konzept

- 1 Auslesen der User ID und des Tickets von der Karte
- 2 Auslesen der des Tickets aus der Nutzerdatenbank
- 3 Uberprüfen des Tickets
- 4 Generieren eines neuen Tickets
- 5 Schreiben des neuen Tickets auf die Karte

Anforderungen & Beispiele

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative) Implementationen

AnonAccess Konzept

- 1 Auslesen der User ID und des Tickets von der Karte
- 2 Auslesen der des Tickets aus der Nutzerdatenbank
- 3 Überprüfen des Tickets
- 4 Generieren eines neuen Tickets
- Schreiben des neuen Tickets auf die Karte

Anforderungen & Beispiele

Begriffe und Vorraussetzungen

Aufbau

tionen

Mögliche (alternative) Implementa-

AnonAccess Konzept

- 1 Auslesen der User ID und des Tickets von der Karte
- 2 Auslesen der des Tickets aus der Nutzerdatenbank
- 3 Überprüfen des Tickets
- 4 Generieren eines neuen Tickets
- 5 Schreiben des neuen Tickets auf die Karte

Anforderungen & Beispiele

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative) Implementationen

AnonAccess Konzept

- 1 Auslesen der User ID und des Tickets von der Karte
- 2 Auslesen der des Tickets aus der Nutzerdatenbank
- 3 Überprüfen des Tickets
- 4 Generieren eines neuen Tickets
- 5 Schreiben des neuen Tickets auf die Karte

Variante 1 - Nachteile

Anforderungen & Beispiele

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative) Implementationen

AnonAccess Konzept

Nachteil:

- Zugriff ist nur Pseudonym
- Pseudonym ist relativ schwer zu merken

Variante 1 - Nachteile

Anforderungen & Beispiele

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative) Implementationen

AnonAccess Konzept

Nachteil:

- Zugriff ist nur Pseudonym
- Pseudonym ist relativ schwer zu merken

Variante 1 - Nachteile

& Beispiele

Begriffe und

Vorrausset
zungen

Aufbau Mögliche

(alternative) Implementa-

tionen

AnonAccess Konzept

Nachteil:

- Zugriff ist nur Pseudonym
- Pseudonym ist relativ schwer zu merken

Variante 2

Anforderungen & Beispiele Begriffe und

Vorraussetzungen

Aufbau

Mögliche (alternative) Implementationen

AnonAccess Konzept

Wie Variante 1, mit folgender Änderungen:

 Es wird zusatzlich zu dem Ticket auch eine neue User ID generiert.

Variante 2

Anforderungen & Beispiele

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative) Implementationen

AnonAccess Konzept Wie Variante 1, mit folgender Änderungen:

 Es wird zusätzlich zu dem Ticket auch eine neue User ID generiert.

AnonAccess Sören

Sören Heisrath, Daniel Otte

Variante 2 - Nachteil

Anforderungen & Beispiele
Begriffe und

Vorraussetzungen

Aufbau

Mögliche (alternative) Implementationen

AnonAccess Konzept

Nachteil:

Nicht wartbar, da Nutzer nicht mehr "adressierbar" sind

Variante 2 - Nachteil

Anforderungen & Beispiele Begriffe und

Vorraussetzungen

Aufbau

Mögliche (alternative) Implementationen

AnonAccess Konzept

Nachteil:

• Nicht wartbar, da Nutzer nicht mehr "adressierbar" sind.

Neue Problemstellungen

Anforderungen & Beispiele

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative)

(alternative) Implementationen

AnonAccess Konzept

Das Problem der Wartbarkeit

- Nutzer müssen adressierbar sein.
- Lösungsidee: Nutzer müssen nicht die ganze Zeit adressierbar sein.

Neue Problemstellungen

Anforderungen & Beispiele

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative) Implementa-

Implementationen

AnonAccess Konzept

Das Problem der Wartbarkeit

- Nutzer müssen adressierbar sein.
- Lösungsidee: Nutzer müssen nicht die ganze Zeit adressierbar sein.

Neue Problemstellungen

Anforderungen & Beispiele

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative) Implementationen

AnonAccess Konzept Das Problem der Wartbarkeit

- Nutzer müssen adressierbar sein.
- Lösungsidee: Nutzer müssen nicht die ganze Zeit adressierbar sein.

Anforderungen & Beispiele Begriffe und

Vorraussetzungen

Aufbau

Mögliche (alternative)

(alternative) Implementationen

AnonAccess Konzept Änderungen an einem Benutzerkonto werden erst dann angewendet wenn sich der Benutzer anmeldet. Die Adressierung findet über einen sogenannten Nickname statt.

Dieser Nickname wird jedoch nirgwendwo im Klartext gespeichert.

Auf der Karte wird ein verschlüsselter Fingerprint des Nicknames gespeichert.

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative)

Implementationen

AnonAccess Konzept Sollen die Eigenschaften eines Kontos modifiziert werden, dann wird ein Eintrag in der Flag-Modify-Database erstellt.

Fingerprint des Nicknames

Anderungsanweisungen

Lösung

& Beispiele

Begriffe und

Vorraussetzungen

Aufbau Mögliche

(alternative) Implementationen

AnonAccess Konzept Sollen die Eigenschaften eines Kontos modifiziert werden, dann wird ein Eintrag in der Flag-Modify-Database erstellt.

Fingerprint des Nicknames

Anderungsanweisungen

Lösung

& Beispiele

Begriffe und

Vorraussetzungen

Aufbau Mögliche

(alternative)

tionen

AnonAccess Konzept Sollen die Eigenschaften eines Kontos modifiziert werden, dann wird ein Eintrag in der Flag-Modify-Database erstellt.

- Fingerprint des Nicknames
- Änderungsanweisungen

Begriffe und Vorraussetzungen

Aufbau

Mögliche (alternative) Implementationen

AnonAccess Konzept

Nun wird der Ablauf der Authentifizierung erweitert um:

- Entschlüsseln des Nickname Fingerprints
- Suche in der Datenbank nach Anderungen für dieses Konto

Lösung

& Beispiele

Begriffe und
Vorrausset-

zungen Aufbau

7101100

Mögliche (alternative) Implementationen

AnonAccess Konzept Nun wird der Ablauf der Authentifizierung erweitert um:

- Entschlüsseln des Nickname Fingerprints
- Suche in der Datenbank nach Anderungen für dieses Konto

Anforderungen & Beispiele Begriffe und

Vorraussetzungen

Aufbau

Mögliche (alternative)

(alternative) Implementationen

AnonAccess Konzept Nun wird der Ablauf der Authentifizierung erweitert um:

- Entschlüsseln des Nickname Fingerprints
- Suche in der Datenbank nach Änderungen für dieses Konto