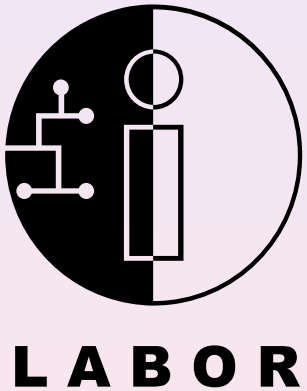
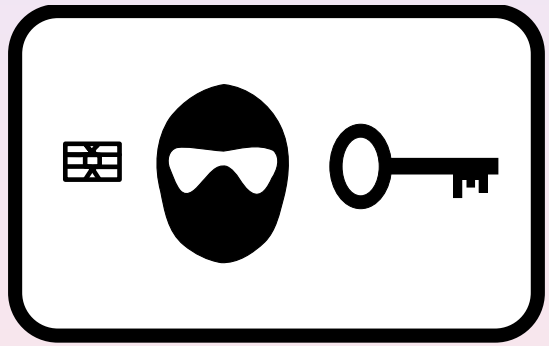
AnonAccess

Sören Heisrath Daniel Otte





20. Dezember 2007

Anforderungen

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

Anforderungen

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

Anforderungen

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

Anforderungen

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

Anforderungen

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

Anforderungen

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

Wartbarkeit

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

Wartbarkeit

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

Wartbarkeit

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

Wartbarkeit

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

Sicherheit

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

Sicherheit

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

Sicherheit

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

Sicherheit

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

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

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

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

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

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

Kostengünstig

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

Kostengünstig

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

Kostengünstig

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

Kostengünstig

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

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)

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)

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)

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)

Ticket

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

Hash-Funktion

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.

System

Verwendung einer Speicherkarte zum speichern der Authentifizierungsdaten.
Aufteilung in **Master** und **Terminal** um:

- Aufgaben Verteilung
- Besondere Sicherung der Master Unit

System

Verwendung einer Speicherkarte zum speichern der Authentifizierungsdaten.
Aufteilung in **Master** und **Terminal** um:

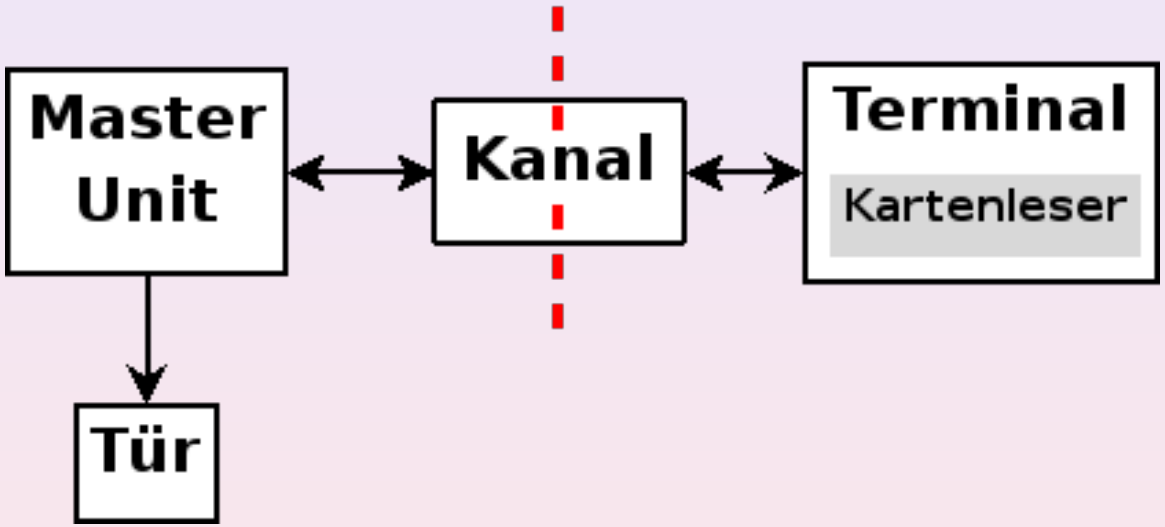
- Aufgaben Verteilung
- Besondere Sicherung der Master Unit

System

Verwendung einer Speicherkarte zum speichern der Authentifizierungsdaten.
Aufteilung in **Master** und **Terminal** um:

- Aufgaben Verteilung
- Besondere Sicherung der Master Unit

Grundaufbau



Master Unit

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

Master Unit

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

Master Unit

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

Master Unit

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

Master Unit

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

Terminal/Panel

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

Terminal/Panel

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

Terminal/Panel

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

Terminal/Panel

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

Kanal (logisch)

Verbindung über kryptografisch sicheren Kanal

- Integrität
- Authentizität
- Vertraulichkeit

Kanal (logisch)

Verbindung über kryptografisch sicheren Kanal

- Integrität
- Authentizität
- Vertraulichkeit

Kanal (logisch)

Verbindung über kryptografisch sicheren Kanal

- Integrität
- Authentizität
- Vertraulichkeit

Kanal (logisch)

Verbindung über kryptografisch sicheren Kanal

- Integrität
- Authentizität
- Vertraulichkeit

Kanal (physikalisch)

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

- Funk
- LWL / Optokoppler

Kanal (physikalisch)

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

- Funk
- LWL / Optokoppler

Kanal (physikalisch)

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

- Funk
- LWL / Optokoppler

Speicherkarte

Speicherung der zur Authentifierung nötigen Daten (z.B. Ticket).

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

Speicherkarte

Speicherung der zur Authentifierung nötigen Daten (z.B. Ticket).

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

Speicherkarte

Speicherung der zur Authentifierung nötigen Daten (z.B. Ticket).

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

Speicherkarte

Speicherung der zur Authentifierung nötigen Daten (z.B. Ticket).

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

Variante 1

Daten auf der Karte:

- User ID
- Ticket

Daten im System für jeden Nutzer:

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

Variante 1

Daten auf der Karte:

- User ID
- Ticket

Daten im System für jeden Nutzer:

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

Variante 1

Daten auf der Karte:

- User ID
- Ticket

Daten im System für jeden Nutzer:

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

Variante 1

Daten auf der Karte:

- User ID
- Ticket

Daten im System für jeden Nutzer:

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

Variante 1

Daten auf der Karte:

- User ID
- Ticket

Daten im System für jeden Nutzer:

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

Variante 1 - Anwendung

Normale Authentifizierung:

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 - Anwendung

Normale Authentifizierung:

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 - Anwendung

Normale Authentifizierung:

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 - Anwendung

Normale Authentifizierung:

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 - Anwendung

Normale Authentifizierung:

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 - Anwendung

Normale Authentifizierung:

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

Nachteil:

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

Variante 1 - Nachteile

Nachteil:

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

Variante 1 - Nachteile

Nachteil:

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

Variante 2

Wie Variante 1, mit folgender Änderungen:

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

Variante 2

Wie Variante 1, mit folgender Änderungen:

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

Variante 2 - Nachteil

Nachteil:

- Nicht wartbar, da Nutzer nicht mehr ”adressierbar” sind.

Variante 2 - Nachteil

Nachteil:

- Nicht wartbar, da Nutzer nicht mehr ”adressierbar” sind.

Neue Problemstellungen

Das Problem der Wartbarkeit

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

Neue Problemstellungen

Das Problem der Wartbarkeit

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

Neue Problemstellungen

Das Problem der Wartbarkeit

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

Lösung

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.

Lösung

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

- Fingerprint des Nicknames
- Änderungsanweisungen

Lösung

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

- Fingerprint des Nicknames
- Änderungsanweisungen

Lösung

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

- Fingerprint des Nicknames
- Änderungsanweisungen

Lösung

Nun wird der Ablauf der Authentifizierung erweitert um:

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

Lösung

Nun wird der Ablauf der Authentifizierung erweitert um:

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

Lösung

Nun wird der Ablauf der Authentifizierung erweitert um:

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