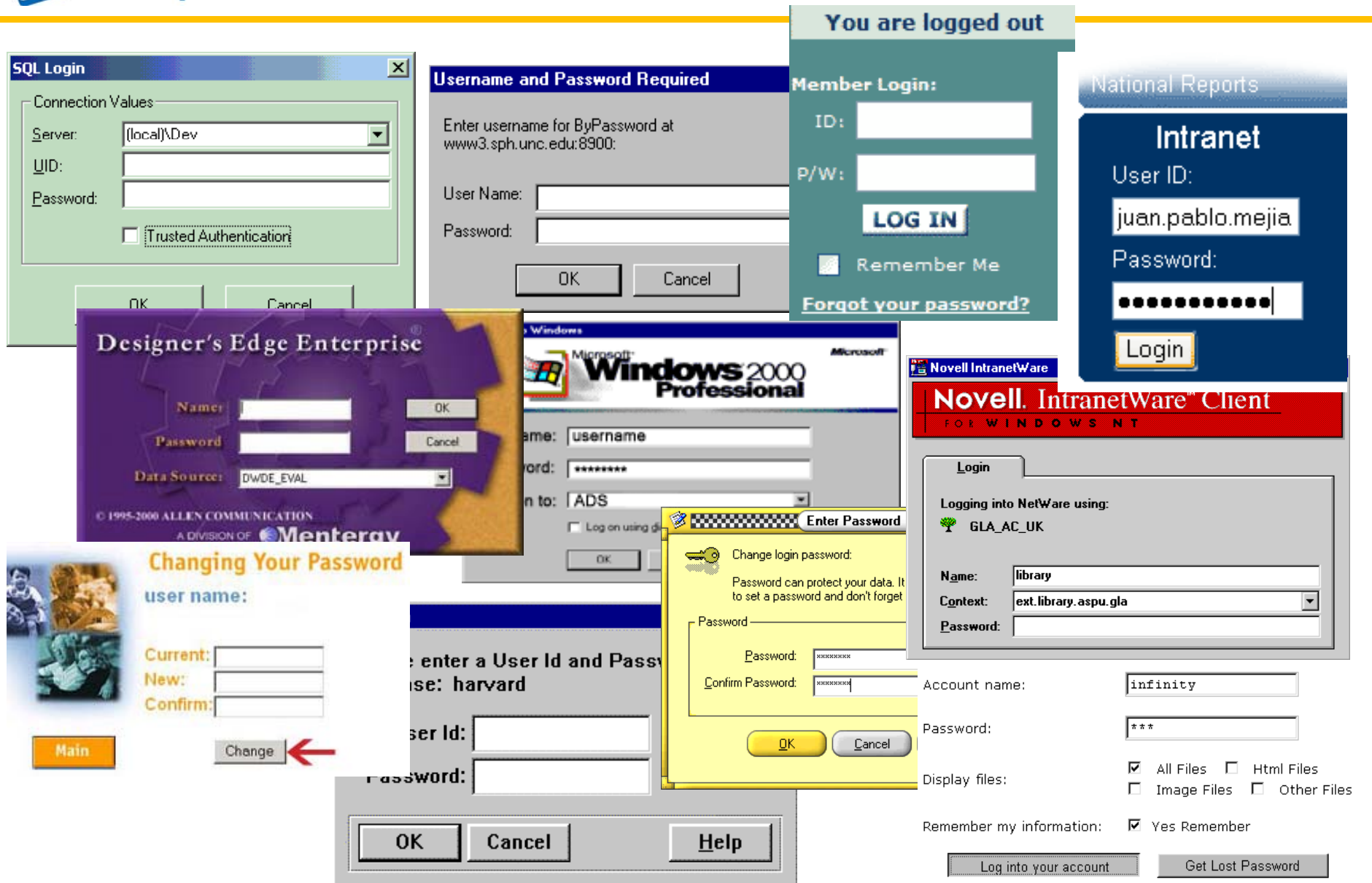


# **Easy Single Sign-On - Lösung der Passwortproblematik**

**Leif Hager, Sales Mgr EMEA  
HMK DKEY Europe GmbH  
2009**



# Viele Passwörter?



The collage features several overlapping windows and forms:

- SQL Login**: A dialog box with fields for Server (set to (local)\Dev), UID, Password, and a checkbox for Trusted Authentication.
- Username and Password Required**: A dialog box asking for a username and password for ByPassword at www3.sph.unc.edu:8900.
- You are logged out**: A teal dialog box with Member Login fields for ID and P/W, a LOG IN button, and a Remember Me checkbox.
- National Reports Intranet**: A web form with fields for User ID (filled with 'juan.pablo.mejia') and Password, and a Login button.
- Designer's Edge Enterprise**: A purple dialog box with fields for Name, Password, and Data Source (set to DWDE\_EVAL).
- Windows 2000 Professional**: A Windows login screen with fields for username and password.
- Novell IntranetWare Client**: A red header for a client application.
- Novell IntranetWare Login**: A login form for NetWare with fields for Name (library), Context (ext.library.aspu.gla), and Password.
- Changing Your Password**: A web form with fields for Current, New, and Confirm passwords, and a Change button with a red arrow pointing to it.
- Enter a User Id and Password**: A dialog box with fields for User Id and Password, and a Help button.
- Change login password**: A yellow dialog box with fields for Password and Confirm Password.
- Account name: infinity**: A form field for an account name.
- Password: \*\*\***: A form field for a password.
- Display files:** A section with checkboxes for All Files, Image Files, Html Files, and Other Files.
- Remember my information:** A checkbox for Yes Remember.
- Log into your account** and **Get Lost Password**: Two buttons at the bottom right.

**Die steigende Verlässlichkeit auf e-Business erfordert bei Unternehmen einen Bedarf um:**

- 1. Anwender zu identifizieren um damit den Zugang der Informationsressourcen zu kontrollieren**
- 2. die Sicherheit der Zugangskontrolle zu erhöhen und für den Anwender den Zugang zu erleichtern**

**Bisherige Lösungen waren nicht ausreichend weil:**

- Verwaltung von vielfachen Zugangsknoten ist nicht einfach
  - steigende Anforderungen für schnellen und einfachen Zugang zu Informationen für Angestellte, Kunden und Partner
  - Sicherheit für Anwender und Administratoren zu erleichtern
  - Bedürfnis die Vertraulichkeit und Integrität der Informationskommunikation zu gewährleisten
  - Bedürfnis der sicheren Authentifizierung der Anwender
-

## Viele verschiedene Zugangskontrollpunkte

- Applikationen
- Web-Seiten
- Geräte
- Netzwerke

## Verschiedene Arten der Authentifizierung

- Passwörter
  - Zertifikate
  - Proprietäre Lösungen
-



**Weil Passwörter Teil unserer  
sozialen und unternehmerischen  
Kultur geworden ist**

**Passwörter bieten die meist übliche Methode um sich bei Computern, Web-Seiten, Netwerke, VPNs, Applikationen, usw. einzuloggen**

**Passwörter sind:**

- zu viele - die Anzahl vermehrt sich sehr schnell
- schwer sich zu merken (zu viele, kompliziert, selten genutzt)
- Administration ist teuer ("Ich habe mein Password vergessen")
- verwundbar gegen Angriffe (leicht zu stehlen, einfach zu verteilen)
- unsicher – Sicherheitsrichtlinien für ein starkes Passwort werden nicht eingehalten

## Sicherheitslücken:

- Passwörter werden vom Anwender niedergeschrieben und heben den Zettel sichtbar auf
  - Anwender teilen Kollegen ihre Passwörter mit
  - Einfache Passwörter werden gewählt
  - “Die Stärke eines Passwortes wird verringert weil Menschen im Prozess beteiligt sind”
-

**Wir Anwender werden mit  
Passwörter konfrontiert**

**ABER**

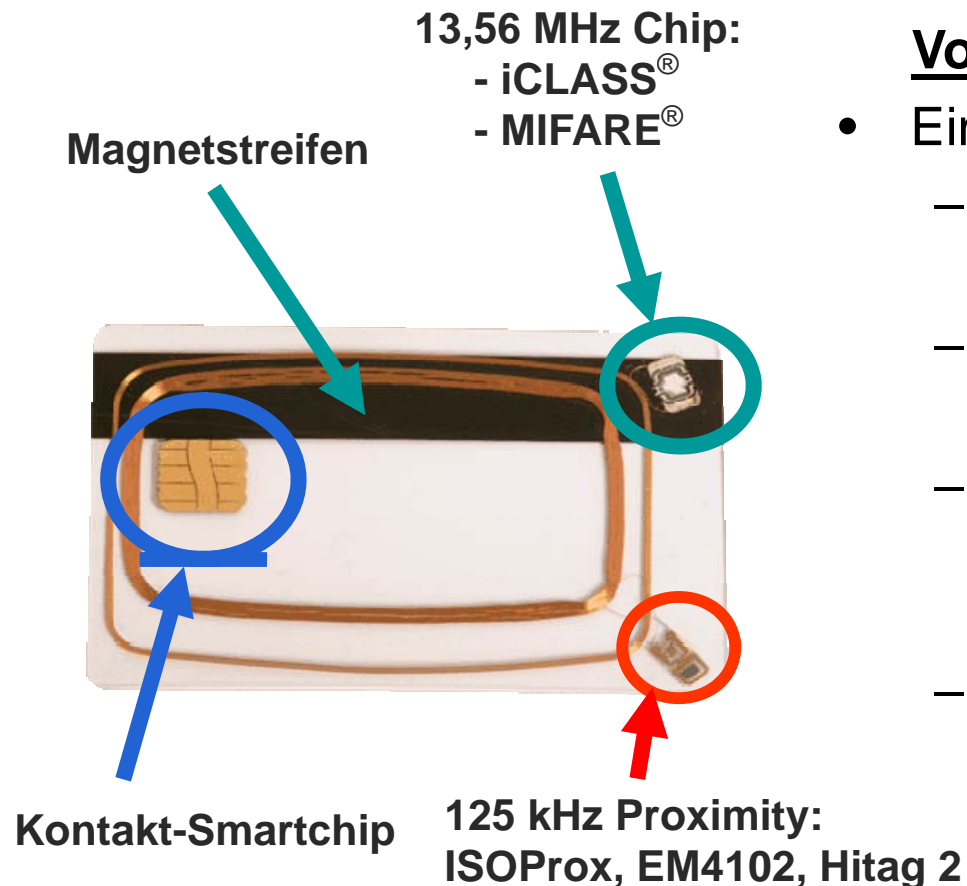
**wie gewährleisten wir eine sichere  
Authentifizierung?**

---

- **Komplettes System um Einloggen mittels Passwörter zu verwalten**
  - ersetzt die Anwendung von Passwörtern mit einer Smartcard und das dazu gehörende Passwort oder Fingerabdruck
- **Verwaltet alle Passwörter des Anwenders**
  - keine Passwörter mehr im Gedächtnis behalten
  - keine Passwörter müssen geändert werden
- **Produktivitätssteigerung der IT-Abteilung**
  - weniger Anfragen wegen Zurücksetzen des PWs
  - betriebsfähig wenige Stunden nach der Installation
  - automatische Integration in der MS-Umgebung
  - kein "IT-Projekt" wird benötigt
- **Integrierte Unterstützung für PKI**
  - sofortiger Einsatz von PKI-Zertifikaten



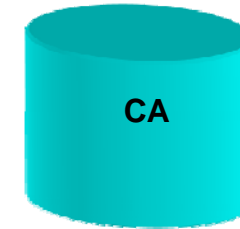
Hybridkarten können für sowohl logische als auch physische Zugangskontrollanwendungen eingesetzt werden.



## Vorteile multifunktionaler Smartcards:

- Ein Unternehmen => eine Sicherheit
  - Gleichzeitige Sperrung von Zugang & Zugriff
  - Reduzierter Missbrauch: enge Verbindung von Mitarbeiter - Karte
  - Einführung von IT-Sicherheits-services (Schutz vor unerlaubten Datenzugriff)
  - Reduzierte Authentisierungsfehler

## Installation



Mit Hilfe von SMS oder  
GPO Technologie

Rapid client soft-  
ware deployment

Client Software

Client Software

Client Software

Anwender mit Karten  
und Lesegeräten  
versehen

