

Single Sign-On

---

Einführung und Überblick

Dipl.-Inf. Rolf Negri

Copyright Trivadis AG 1



Agenda

---



- **Einführung**
- **Technologie und Funktionalität**
- **Installation und Konfiguration**
- **Ausblick**

Single Sign-On Copyright Trivadis AG 2

## Passworte

Rechner

Mailserver

Smartcards

Netzwerk

Single Sign-On

Copyright Trivadis AG

3

## Umgang mit Passwörtern

### Zahlreiche Passwörter:

- ➔ schwierig zu merken
- ➔ leichte Passwörter werden gewählt

### Zwang zu komplexen Passwörtern:

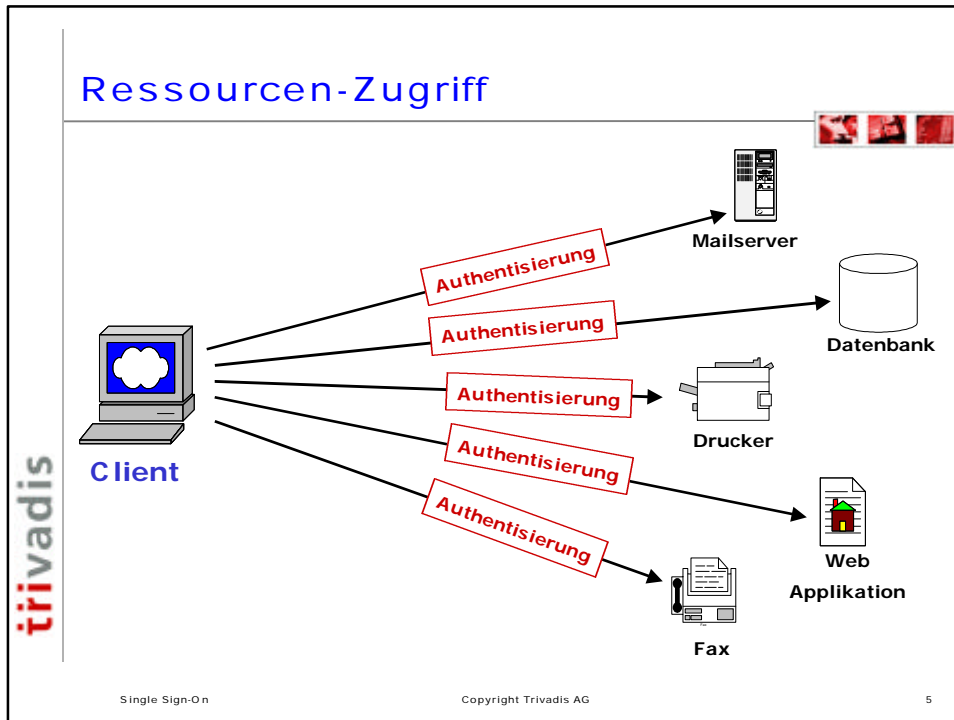
- ➔ werden aufgeschrieben und an Monitor geheftet

**Passwörter sind ein Sicherheitsrisiko!**

Single Sign-On

Copyright Trivadis AG

4



- ## Passwortprobleme
- Mitlesen übers Netz möglich
  - Knacken
  - Passwortfallen
  - Social Engineering
  - Hohe Supportkosten
    - ◆ 40% aller Anfragen bei Help Desk beziehen sich auf vergessene Passwörter
    - ◆ Eine Anfrage kostet im Durchschnitt 80 Dollar
  - Administrationsaufwand
    - ◆ Verteilung / Entzug von Berechtigungen (über ganze Firma)
    - ◆ Autorisierungen durch verschiedene Stellen welche nicht die gleichen Policies unterhalten
- The Trivadis logo is on the left, and the text 'Single Sign-On' and 'Copyright Trivadis AG' are at the bottom.
- Single Sign-On
- Copyright Trivadis AG
- 6

## Ausweg SSO - Anwendersicht

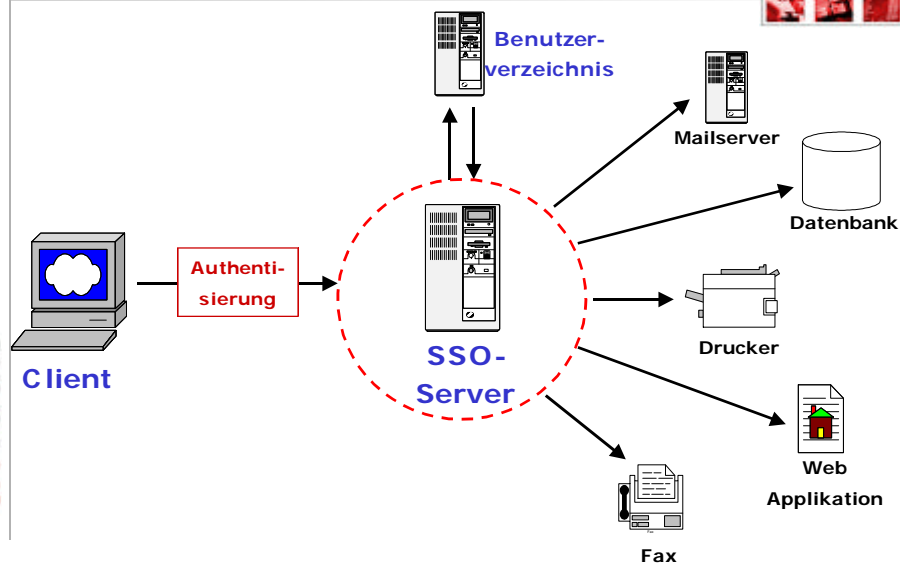
- Vereinfachte Authentisierung:
  - ◆ Nur noch ein Passwort zu merken
  - ◆ Passwort kann ausreichend sicher gewählt werden
  - ◆ Speicherung auf Hardware-Token möglich
- Effizientes Arbeiten:
  - ◆ Alle erlaubten Ressourcen stehen automatisch zur Verfügung
  - ◆ Einfache Interoperabilität zwischen den einzelnen Anwendungen möglich
- Zertifikatsmanagement
  - ◆ Automatische CRL-Prüfung
  - ◆ Automatische Schlüssel- und Zertifikatserneuerung

Single Sign-On

Copyright Trivadis AG

7

## Ressourcen-Zugriff mit SSO



Single Sign-On

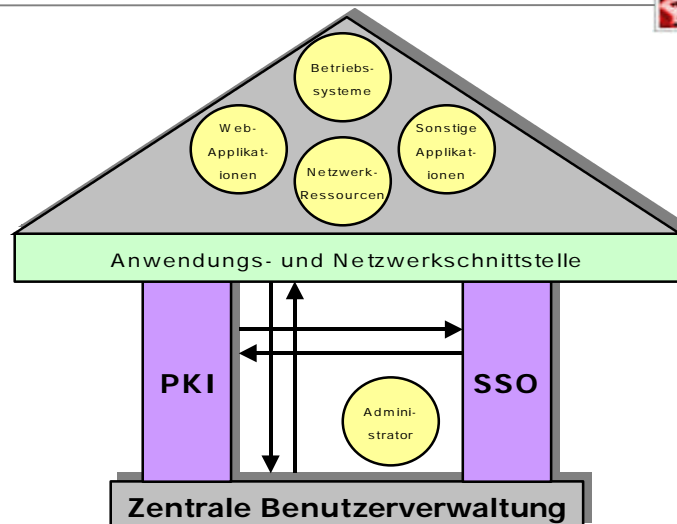
Copyright Trivadis AG

8

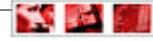
## Voraussetzungen für Single Sign-On

- Zentrales Benutzerverzeichnis
  - ◆ User-Informationen
  - ◆ Passwörter, Zertifikate
  - ◆ Rechte, Privilegien und Rollenprofile
- Public Key Infrastruktur
  - ◆ Authentisierung über Zertifikate
  - ◆ SSL-Verbindung zwischen allen Komponenten
  - ◆ Privilegien mit Zertifikaten verknüpfbar (Attribut-Zertifikate)

## Architekturmodell



## Aufgaben von SSO-Systemen



- **Authentisierung:**
  - ◆ Einmalige Authentisierung des Nutzers
  - ◆ Mapping der Authentisierungsinformationen auf User-Accounts (Account-Management)
- **Autorisierung:**
  - ◆ Auslesen von Privilegien und Berechtigungsinformationen aus Verzeichnis
  - ◆ Weiterleiten der Informationen zu Ressourcen
- **Session-Management:**
  - ◆ Generierung von Session-Tickets
  - ◆ Zuordnung der User zu Sessions

## Ausweg SSO - Administratorsicht



- **Reduzierung des administrativen Aufwandes:**
  - ◆ Benutzerverwaltung geschieht einmalig und zentral
  - ◆ Weniger Supportanfragen wegen vergessener Passwörter
- **Erhöhung der Sicherheit**
  - ◆ kryptographisch starke Passwörter für Netzwerk-Ressourcen
  - ◆ Sperrung von Nutzern an zentraler Stelle hat Auswirkung auf alle Systeme
  - ◆ Verschlüsselte Verbindungen zu allen Ressourcen

## Anpassungen auf Client-Seite

- Einheitliche Applikations-Schnittstelle für Authentisierung
- SSO-Client-Software für Kommunikation mit Authentisierungs- und Autorisierungsserver
- Zugriff auf Authentisierungsdatenbank zur Änderung und Synchronisation von Benutzerinformationen

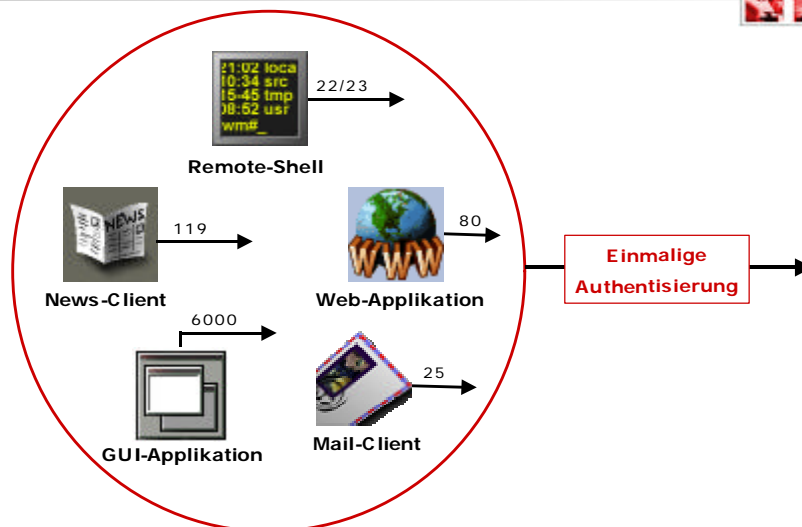
trivadis

Single Sign-On

Copyright Trivadis AG

13

## Client-Schnittstelle



trivadis

Single Sign-On

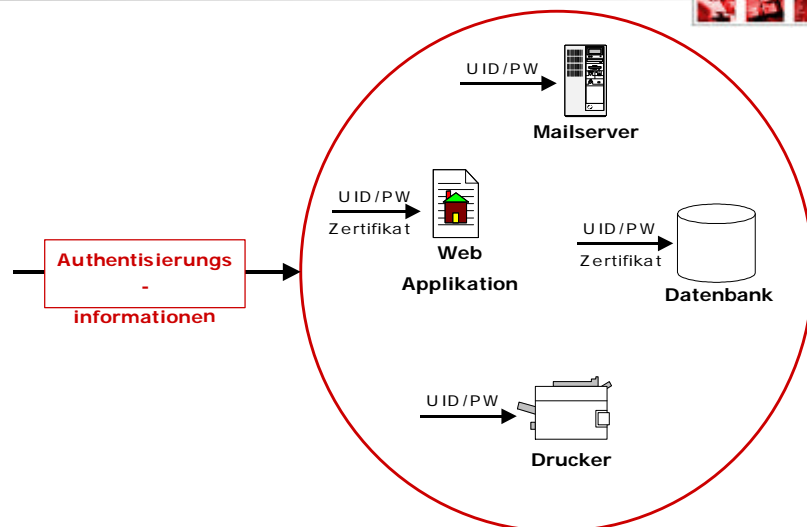
Copyright Trivadis AG

14

## Anpassungen auf Server-Seite

- Gemeinsame Programm-Schnittstelle aller Applikationen für Authentisierung
- Schnittstelle zum Autorisierungs- und Authentisierungsserver für die Validierung der Benutzerinformationen
- Gemeinsame Schnittstelle zum Auslesen von Privilegien und Rechten (einheitliches Rollenkonzept)

## Server-Schnittstelle



## Lösungsansätze



- Zentralisiert, komplex, vollständig:
  - ◆ Einheitliche APIs und SP Is aller Anwendungen und Ressourcen
  - ◆ Zentrales Sessionmanagement
  - ◆ Durch Verwendung offener Standards auch plattformübergreifend in heterogenen Systemen
  
- Aufgesetzt, angepasst, proprietär
  - ◆ SSO nur auf Anwendungsebene
  - ◆ Bedingt einheitliche APIs (nachträglich angepasst)
  - ◆ Proprietäre Schnittstellen

trivadis

Single Sign-On

Copyright Trivadis AG

17

## Zentralisierte Systeme



- Integration in Betriebssystem
- Anmeldung bei zentralem Autorisierungsserver
- Verwaltung der gesamten Session über Autorisierungsserver und Session-Tickets
- Interaktion zwischen Ressourcen und Autorisierungsserver
- Verwendung von Zertifikaten
- Dominanz (Abhängigkeit) von einem Betriebssystem
- Anwendungen müssen einheitliche Protokolle unterstützen (z.B. Kerberos)
- Bsp.: OSF DCE, Windows 2000

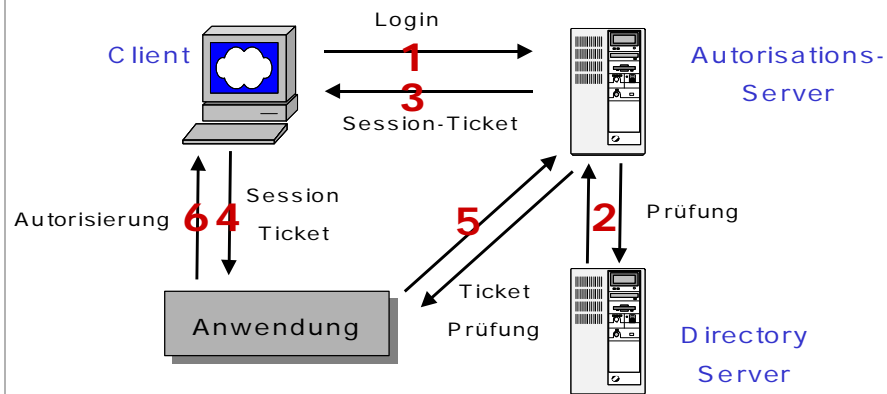
trivadis

Single Sign-On

Copyright Trivadis AG

18

## Kerberos-basierte Systeme - Ablauf



Single Sign-On

Copyright Trivadis AG

19

## PAM-basierte Systeme

- Einheitliche Programm-Schnittstelle für Authentisierung bei Client und Server
- Betriebssystemunabhängig
- Variable und austauschbare Authentisierungsmechanismen (**P**luggable **A**uthentication **M**odules)
- Modularer Aufbau von Account, Session und Passwort Management
- Standardisierung als XSSO (X/OPEN Single Sign-On Service) angestrebt
- Bsp.: Sun Solaris, HP Unix, Linux

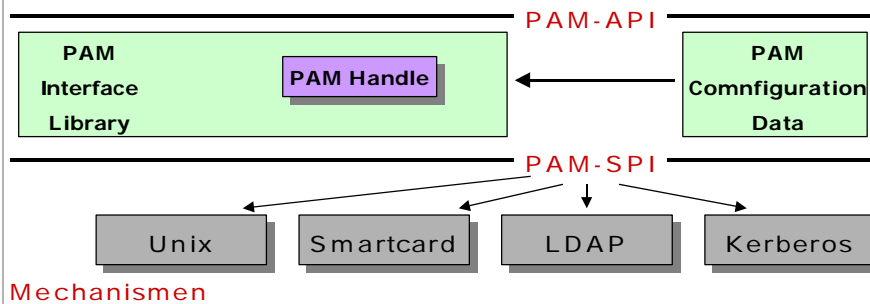
Single Sign-On

Copyright Trivadis AG

20

## PAM-basierte Systeme - Ablauf

### Applikationen



### Mechanismen

Single Sign-On

Copyright Trivadis AG

21

## Aufgesetzte Systeme

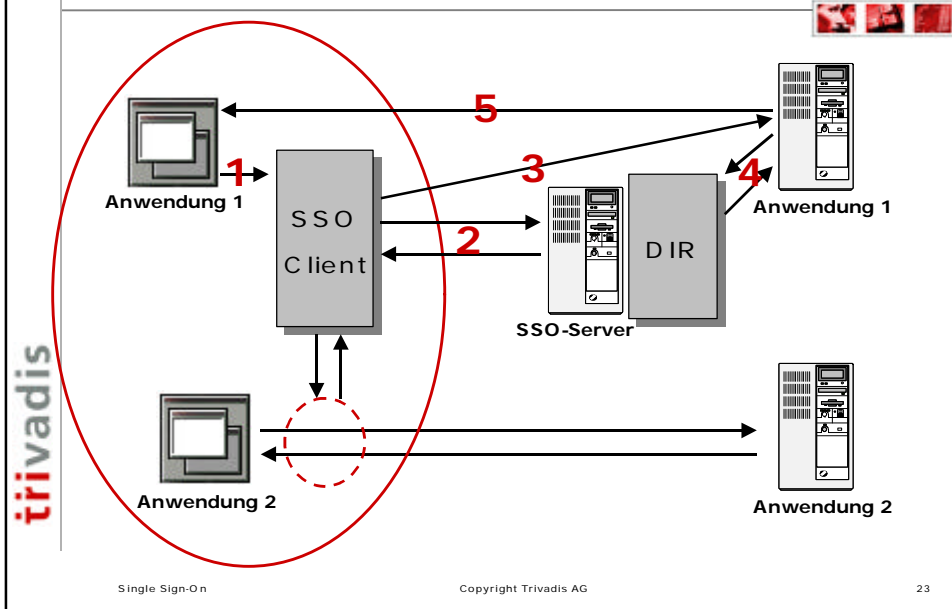
- Nicht in die Betriebssystemarchitektur integriert, sondern als Anwendung aufgesetzt
- Nachträgliche Anpassung von Client- und Serveranwendungen notwendig
- Proprietäre Schnittstellen und Protokolle
- Zentraler Passwort-Store
- Snap-In von Authentisierungsinformationen (Window-Watching)
- Auf eigene Produktpalette gestützt (PKI, Verzeichnis)
- Meist nur für MS-Plattformen verfügbar
- Bsp.: Novell SSO, IBM Tivoli GlobalSignOn, Entrust SSO

Single Sign-On

Copyright Trivadis AG

22

## Aufgesetzte Systeme - Ablauf



## Beispiel - Novel SSO

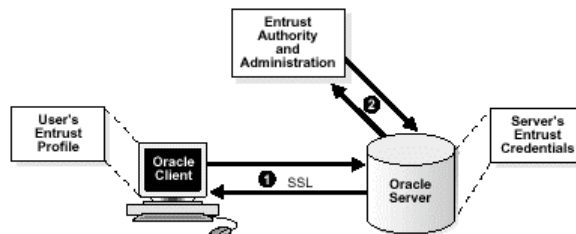
**Authentizierungs-abfrage**

**Logon-Manager**

Application Name	Description
Allgemein Drive	Software
ICQ	My Chat
Outlook	Mailaccount - Trivadis
Trip	Abrechnung

Single Sign-On Copyright Trivadis AG 24

## Beispiel - Entrust



1. Entrust User baut eine SSL-Verbindung zum Oracle Server auf und sendet seine Entrust Credentials
2. Der Oracle Server fragt die Entrust Authority nach dem Status des gesendeten Zertifikates ab

## Ausweg SSO - ???

- Einsatz in heterogenen Systemen mit hohem Aufwand verbunden
- Nicht alle Plattformen unterstützt
- Anpassung der Implementation von nicht „SSO-konformen“ Anwendungen (Source notwendig)
- Noch keine Standards vorhanden
- Zertifikatseinsatz bedingt vollständige Integration einer PKI
- Ungesicherte Arbeitsstation ist ein grosses Risiko

## Fazit und Ausblick



- Bedarf an SSO-Lösungen wird weiter zunehmen
- Integration von SSO in grosse (gewachsene) Umgebungen ist mit hohem Aufwand verbunden = hohe Kosten
- Einheitliche Applikations-Schnittstelle fehlt oder wird nicht durchweg unterstützt (GSS-API)
- Inkompatible Systeme verhindern Standardisierung
- SSO muss professionell gelöst werden (Komplex)
- Keine Out-of-the-Box Lösung

trivadis

## Weitere Informationen...



- Kontakt:
- Download des Vortrages:  
DFN\_2001.pdf unter:

Trivadis AG  
eSecurity  
Rolf Negri  
Kanalstrasse 5  
CH - 8152 Glattdbrugg  
Switzerland

Tel.: +41 1 808 70 20  
Fax: +41 1 808 70 21

eMail:  
rolf.negri@trivadis.com

<http://www.trivadis.com/services/publikationen/publiste.asp>

trivadis