
Desktop Single Sign-On Enterprise Single Sign-On

31 Mei 2007

Bob Lannoy
Sectie Onderzoek

Agenda

- Problematiek
- Situering
- Eigenschappen
- Marktoverzicht
- Demo
- Voordelen / nadelen
- Alternatieven
- Besluit



Problematiek (1/3)

Lotus Notes

Enter your password

For user: Bob Lannoy/SMAL

SSH Tectia Client 4.0.5 (Build 354)
Copyright (c) 2000-2003 SSH Communications

This copy of SSH Tectia client is a commercial product licensed to Tectia customer, N/A.

SIEMENS BS2000

SSSSSSSS MM MMM AAAAAAAA LL SSSSSSSS

XTremisWeb
Aanmelden a.u.b.

Gebruikersnaam

Wachtwoord

OK

Welcome to intranet

Login

Username:

Password:

Language: FR ☐ NL ☒

Log-in



Problematiek (2/3)

Heterogene omgevingen / applicaties



Windows



Web



Java



Terminal



Problematiek (3/3)

- Wachtwoord per applicatie of per server
- $\neq$ wachtwoordvereisten
- Verschillende malen aanmelden
- Verlies van wachtwoord
- Zwakke wachtwoorden

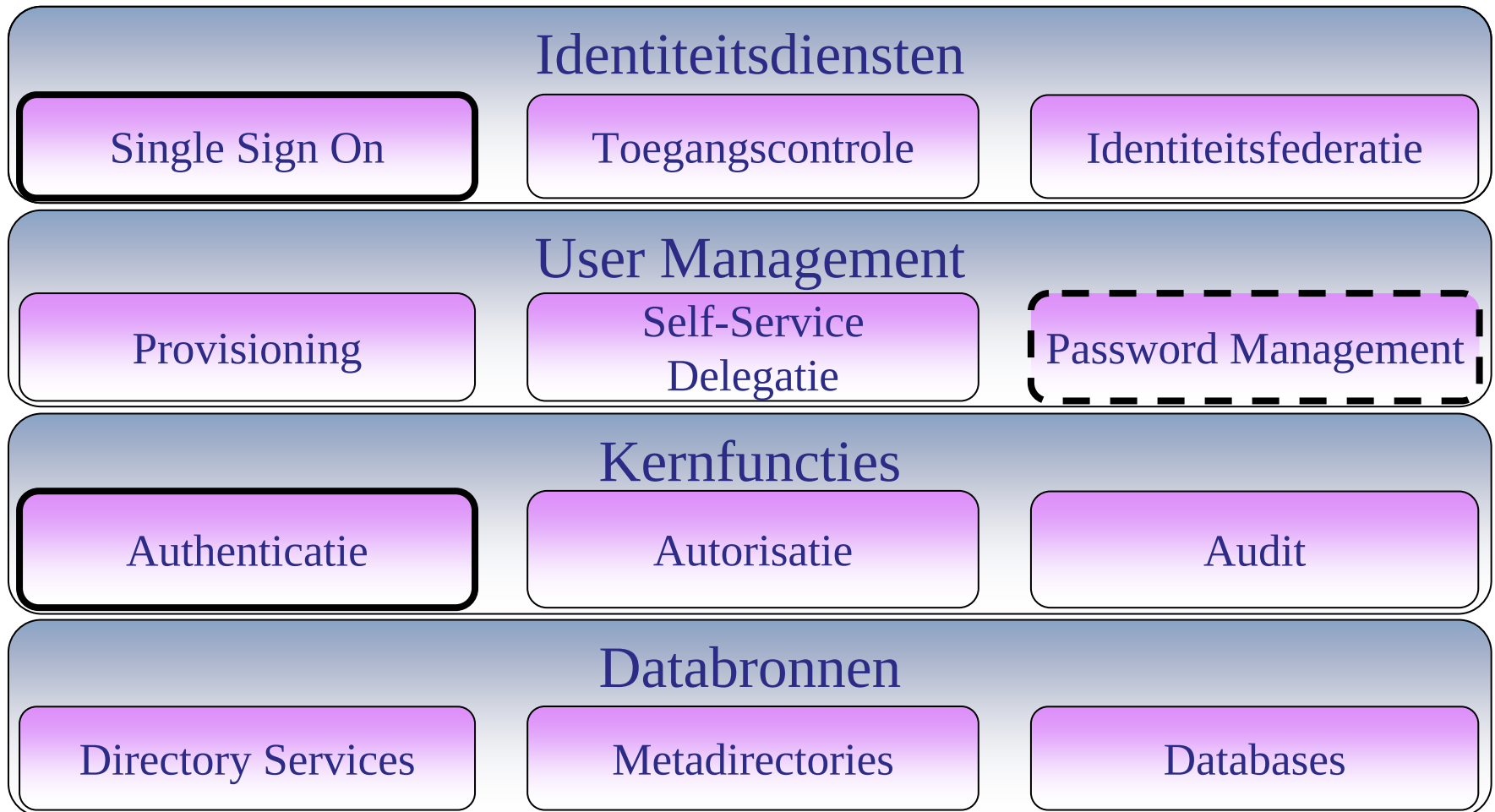


Agenda

- Problematiek
- Situering
- Eigenschappen
- Marktoverzicht
- Demo
- Voordelen / nadelen
- Alternatieven
- Besluit



Situering



Situering

Authenticatie (1/2)

- Kennis van een gegeven

- vb. wachtwoord

bobsmals

Al!5sDz&

- Bezit van iets

- (Hardware)token
 - eID
 - Certificaat

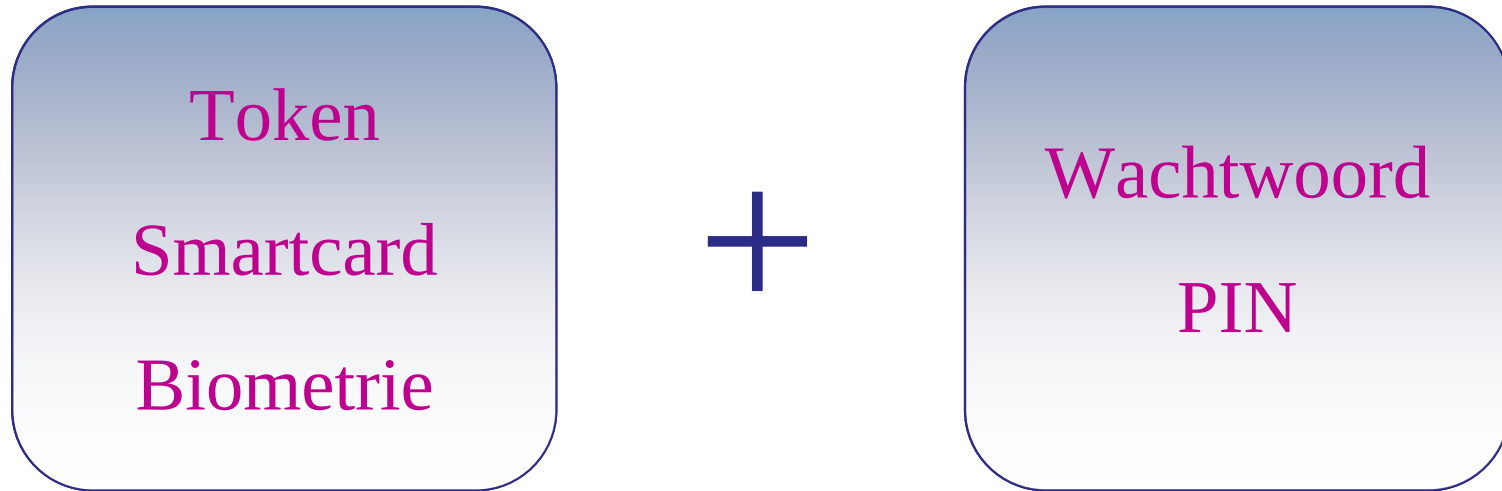


- Fysiek kenmerk

- Biometrie



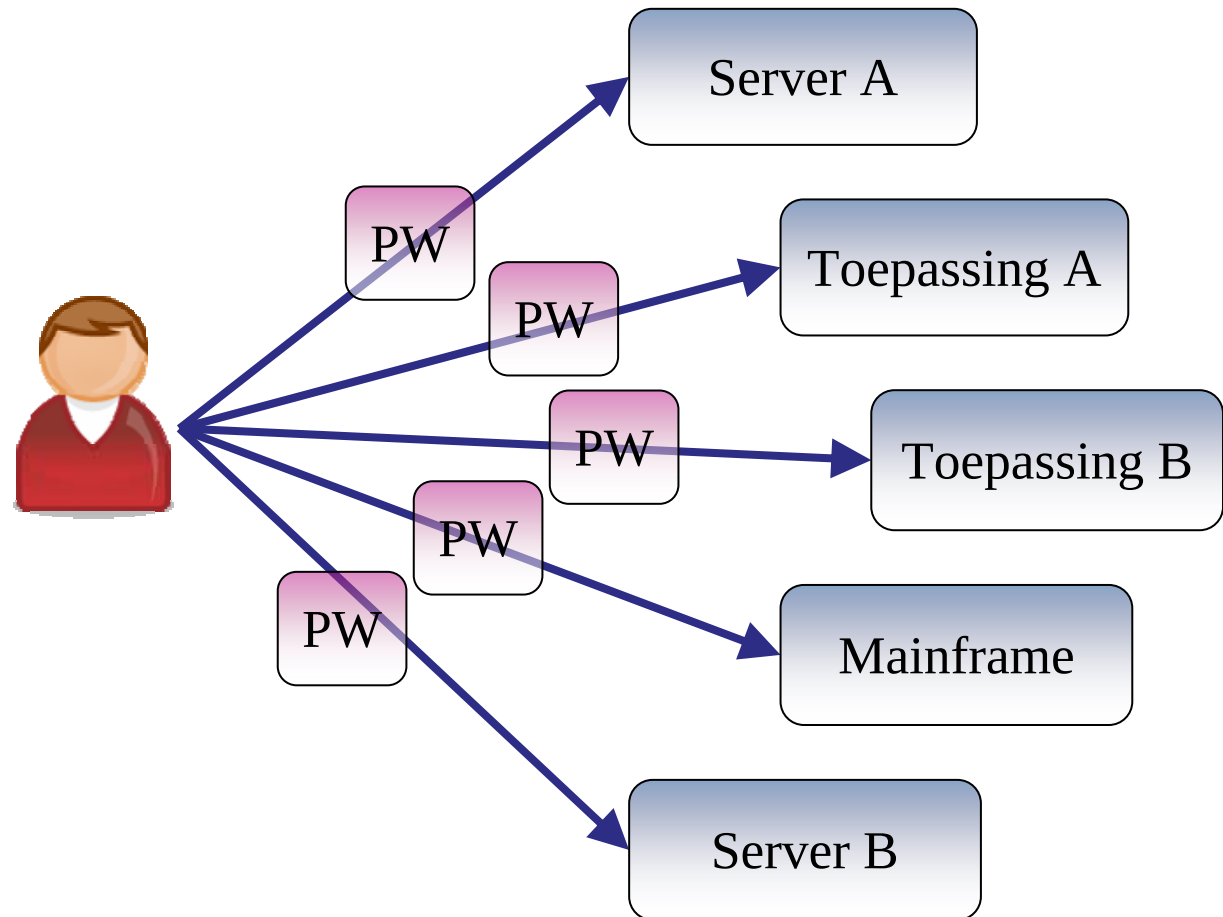
Situering Authenticatie (2/2)



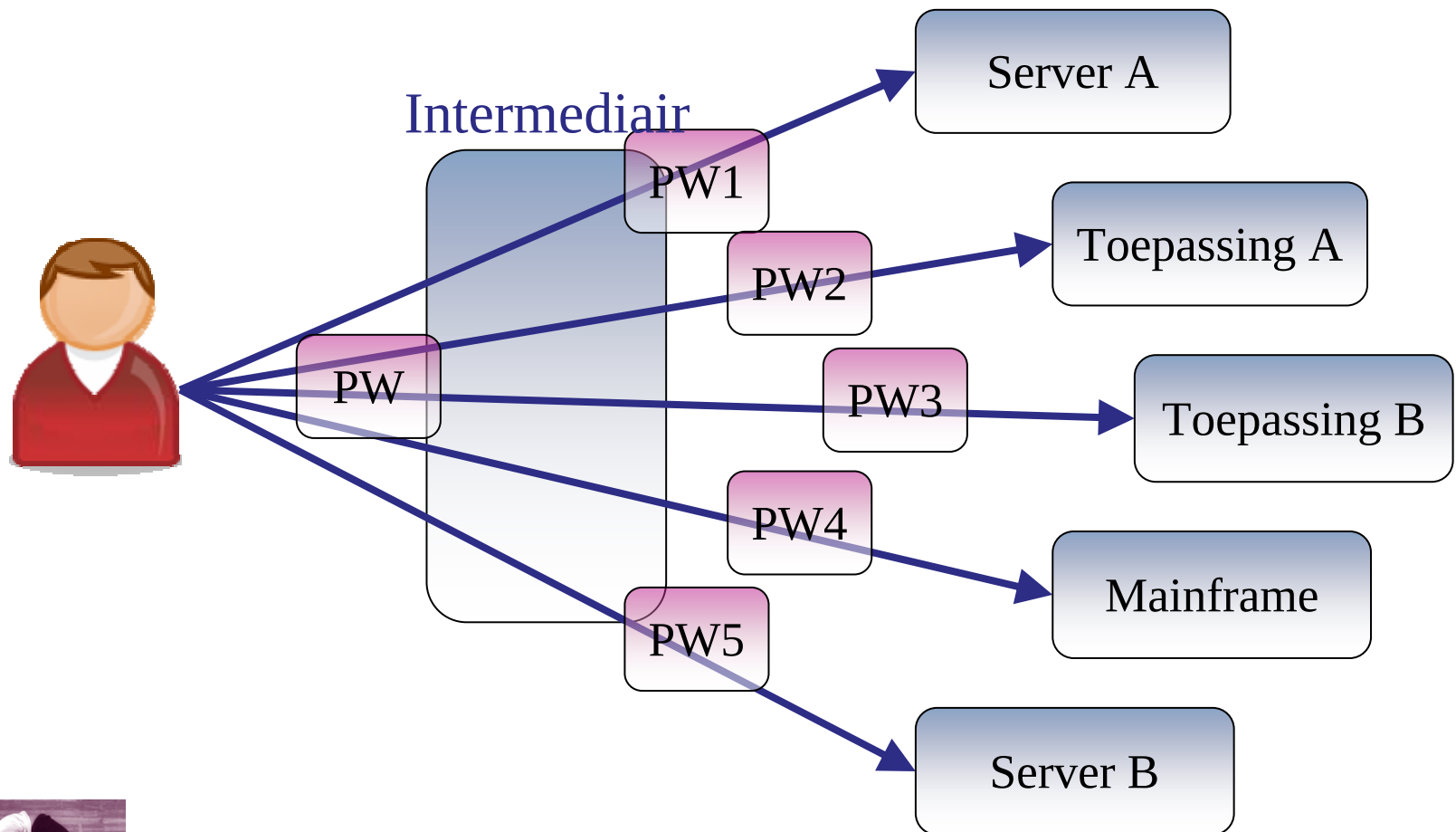
= multi factor authentication



Situering Single Log-On (SLO)



Situering Single Sign-On (SSO)



Situering

SSO vs SLO

Single Log On (SLO)

- één set 'credentials' voor alle systemen
- Meerdere malen aanmelden

Single Sign On (SSO)

- één of meerdere sets credentials
- Eénmaal aanmelden ('sessieoverdracht')



Situering Types SSO

- Web SSO
- Federatie
- Desktop / Enterprise SSO (ESSO)



Situering

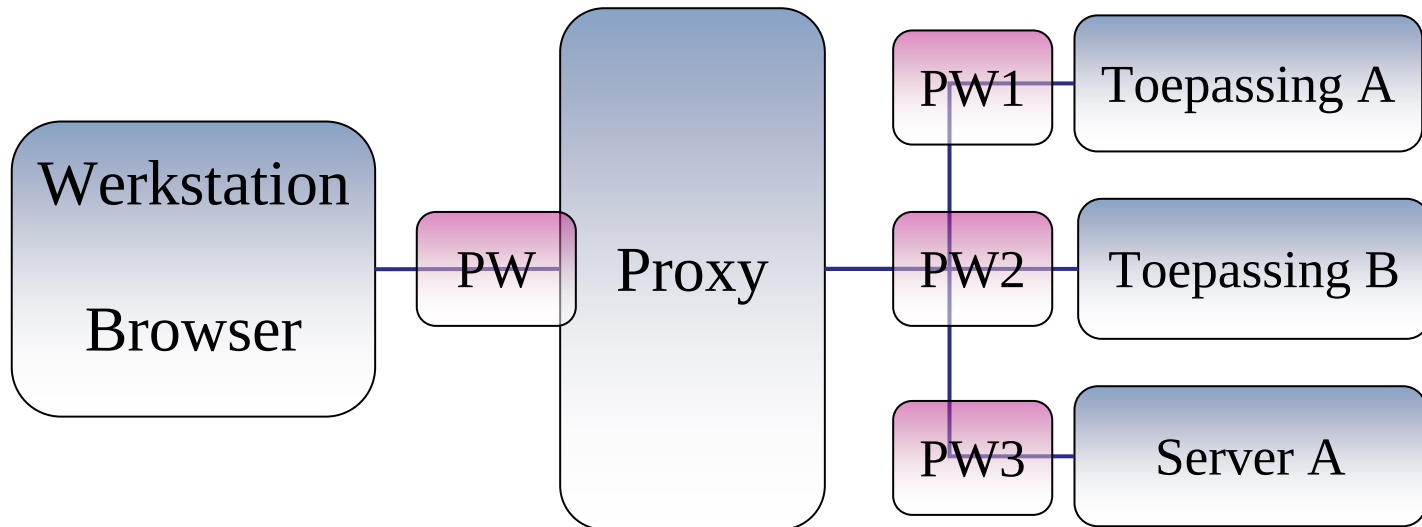
Web SSO (1/3)

- Web gebaseerde toepassingen
- Extranet Access Management
- Twee types:
 - Proxy gebaseerd
 - Agent gebaseerd



Situering Web SSO (2/3)

Proxy gebaseerd

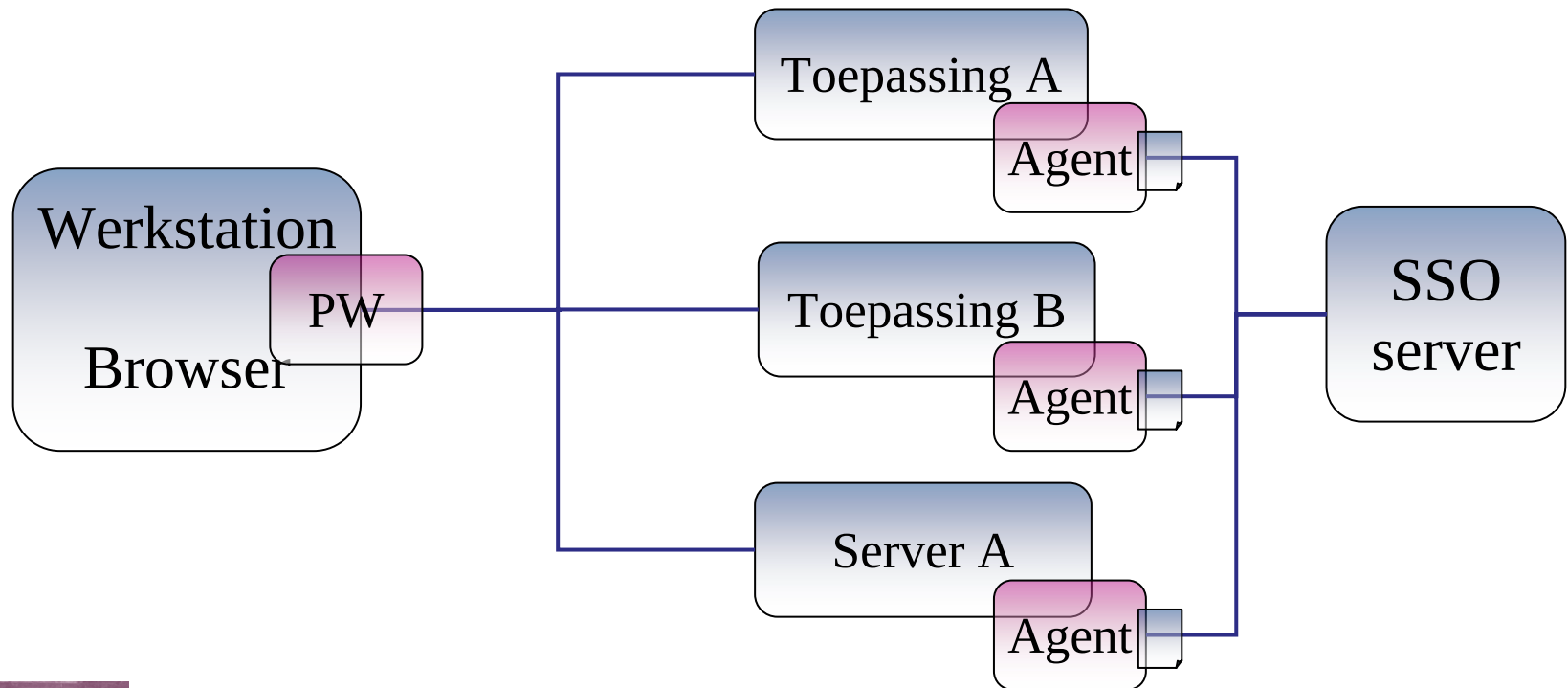


Internet

Extranet

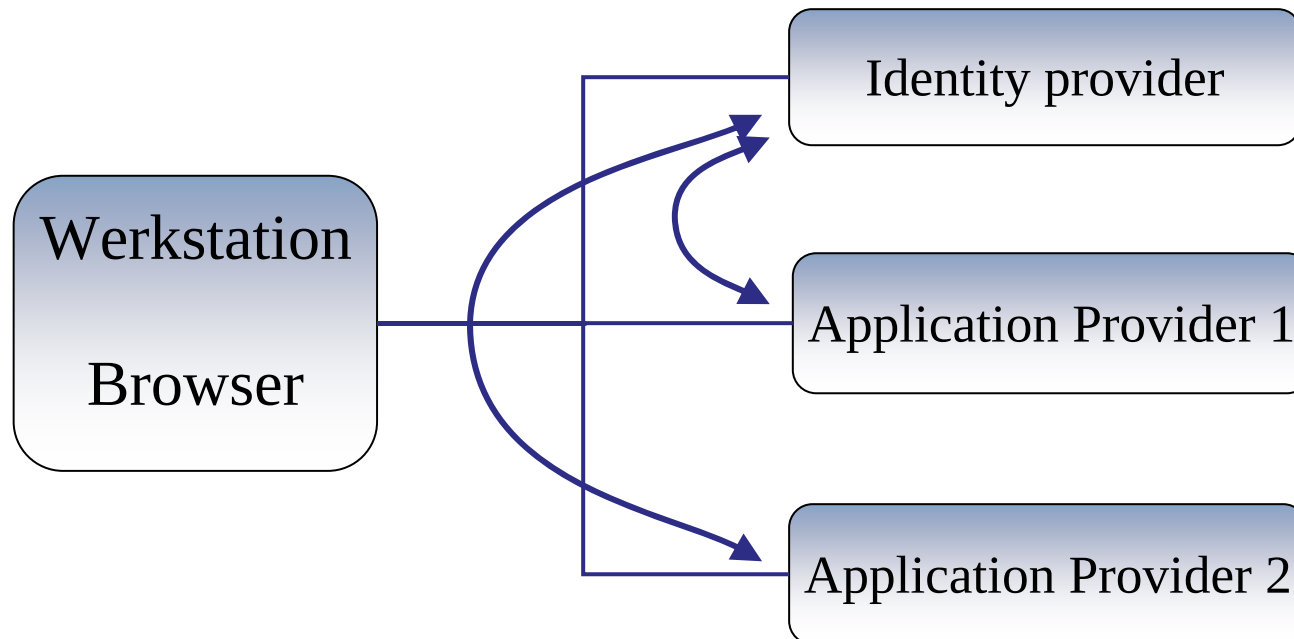
Situering Web SSO (3/3)

Agent gebaseerd

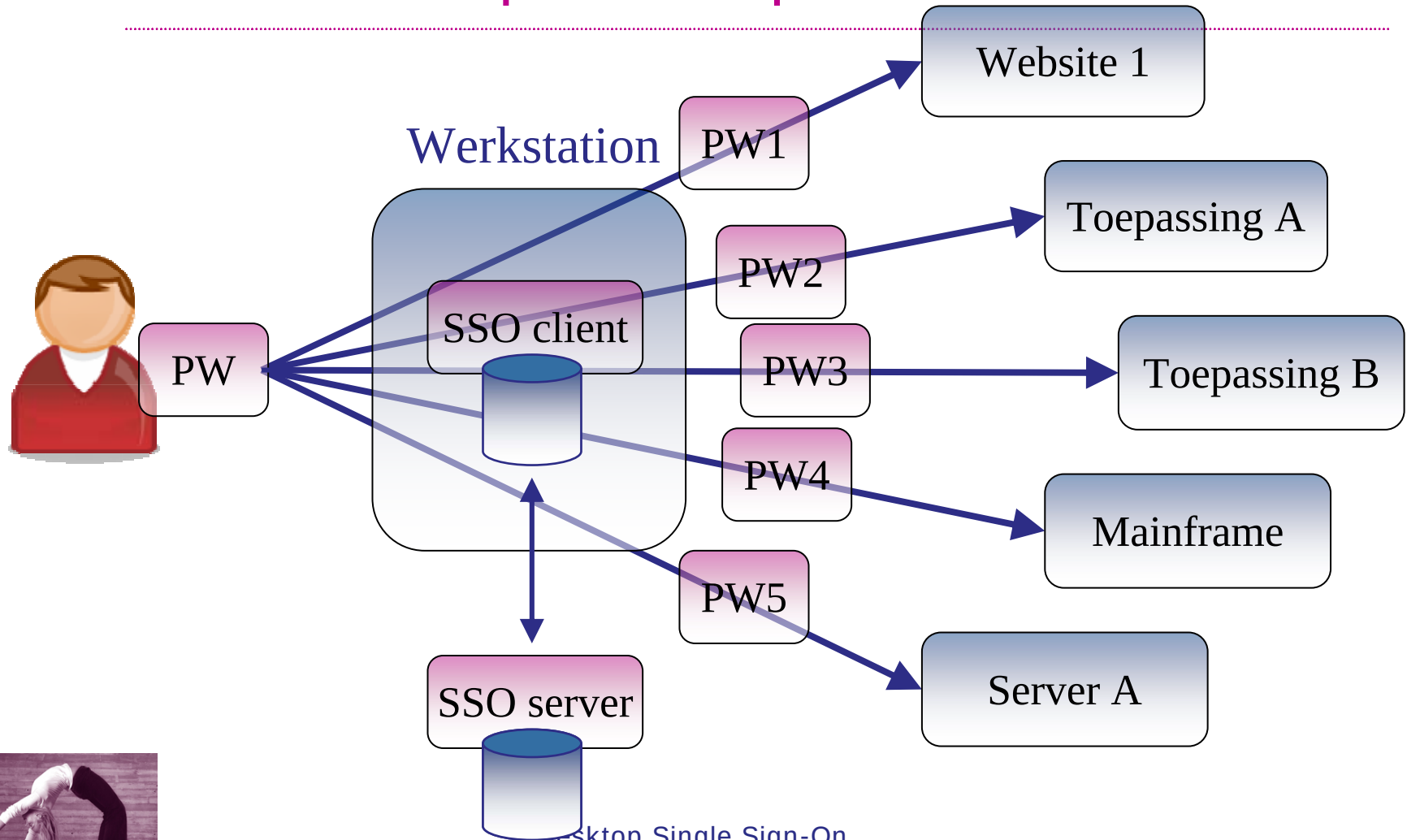


Situering Federatie

SAML, WS-*



Situering Desktop / Enterprise SSO

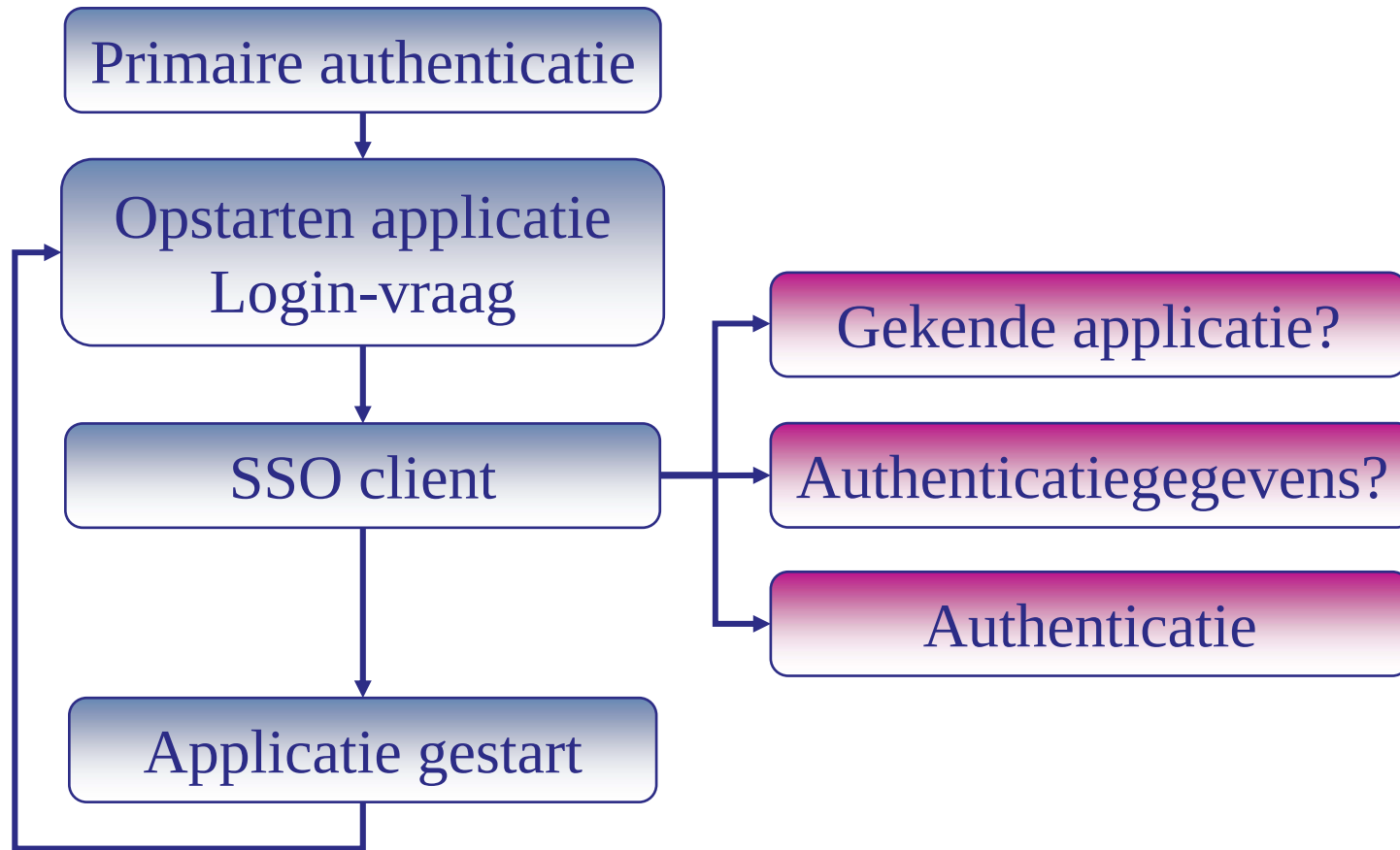


Agenda

- Problematiek
- Situering
- Eigenschappen
- Marktoverzicht
- Demo
- Voordelen / nadelen
- Alternatieven
- Besluit



Eigenschappen (1/2)

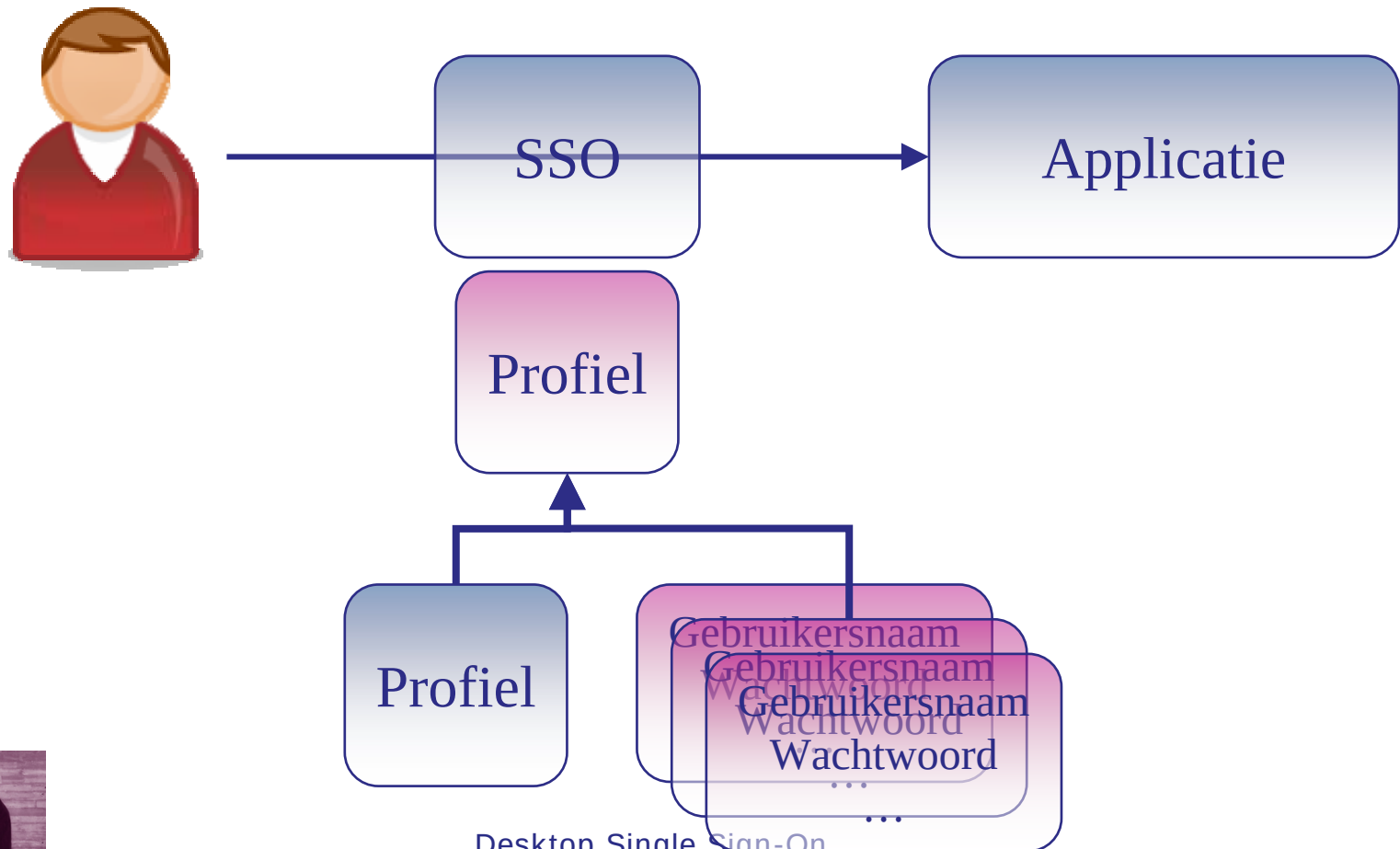


Eigenschappen (2/2)

- Applicatieprofielen
 - Windows
 - Java
 - Terminal
 - Web



Eigenschappen Applicatieprofiel (1/4)



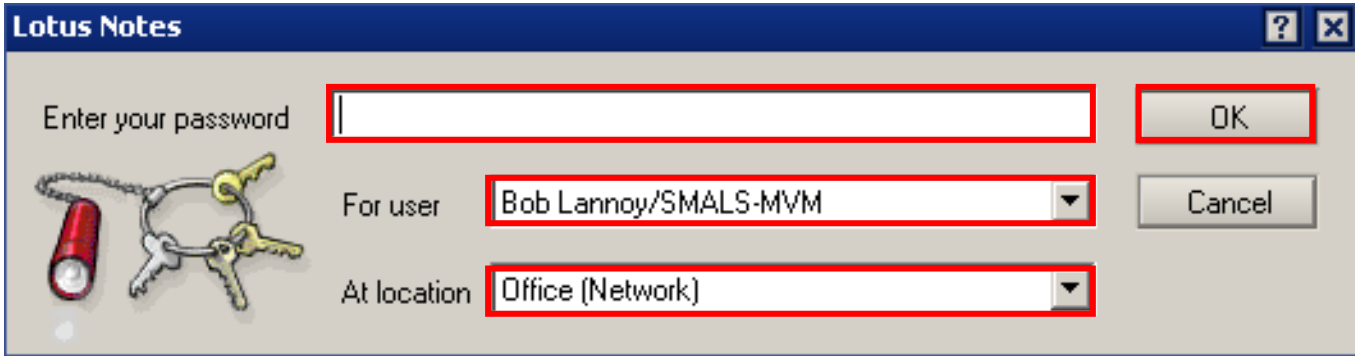
Eigenschappen Applicatieprofiel (2/4)

- Definitie van wachtwoordschermen
 - Login, wachtwoordwijziging, ...
 - Zones met relevante authenticatiegegevens
 - Knoppen of mogelijke acties
- Grafisch of via scripting
- Meerdere logins voor zelfde profiel



Eigenschappen Applicatieprofiel (3/4)

Grafisch



Lotus Notes

Enter your password

For user: Bob Lannoy/SMALS-MVM

At location: Office (Network)

OK Cancel



Eigenschappen Applicatieprofiel (4/4)

Script

Dialog

Title "Lotus Notes"

Class #32770

Ctrl #280

Ctrl #224

EndDialog

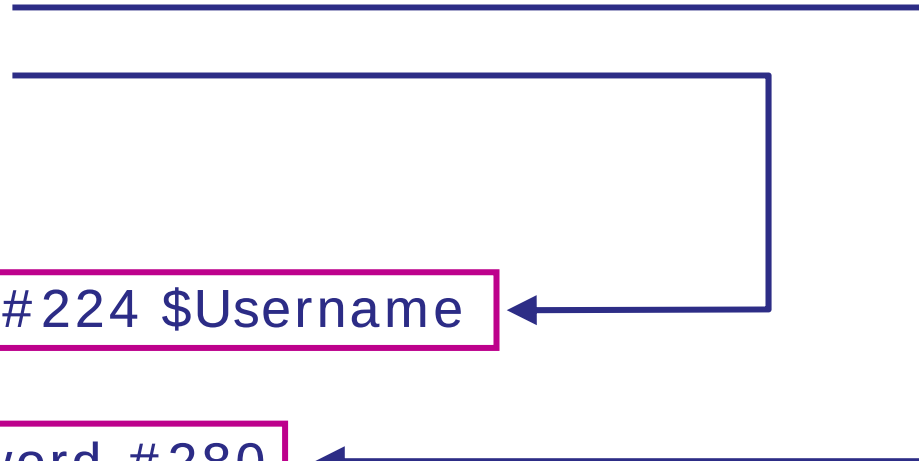
...

ReadText #224 \$Username

...

Type \$Password #280

Click #1



Eigenschappen Systeembeheer (1/2)

- Centrale SSO-server
 - Opslag van credentials in directory server (ActiveDirectory, LDAP)
 - Voorgedefinieerde applicatieprofielen
 - Gebruikersconfiguraties
- Lokale credential-cache
 - Offline functionaliteit
 - Encryptie
 - Bescherming met passphrase (vraag/antwoord)



Eigenschappen Systeembeheer (2/2)

- Administrator
 - Geen toegang tot wachtwoorden van gebruikers
 - Reset van gebruikerswachtwoord
 - Passphrase nodig voor credential store
- Gebruikersconfiguratie
 - Zelf wachtwoorden zien of niet
 - Zelf profielen aanmaken of niet
 - Client onzichtbaar maken
 - ...



Eigenschappen Wachtwoordbeheer

- Vernieuwing van wachtwoord
 - Detectie van scherm voor wachtwoordwijziging
 - Generatie van wachtwoord
- Wachtwoordpolicy
 - Lengte
 - Soorten karakters
 - Hoofdletters / kleine letters



Eigenschappen Veiligheid (1/2)

- Wachtwoordgeneratie door SSO-client
 - Gebruiker kent wachtwoord niet meer
 - Sterkst mogelijke wachtwoord
- Wachtwoordpolicy



Eigenschappen Veiligheid (2/2)

- Toegang tot werkstation = toegang tot alles?
 - Niet voor alle systemen
 - Re-authenticatie voor gevoelige applicaties
 - Primaire sterke authenticatie (Smartcards / USB token)
- Logging / auditing



Eigenschappen Speciale situaties

- Gedeelde PC (Kiosk)
 - Snelle authenticatie & context switch
- Roaming
 - Centrale server
- Offline
 - Credential cache



Agenda

- Problematiek
- Situering
- Eigenschappen
- Marktoverzicht
- Demo
- Voordelen / nadelen
- Alternatieven
- Besluit



Marktoverzicht (1/3)

- Mature markt (jaren 90)
- Gespecialiseerde vendors
 - OEM licenties
- Combinatie met
 - Smartcards / tokens
 - Biometrie
 - Gebruikersbeheer
 - Wachtwoordbeheer



Marktoverzicht (2/3)

- **ActivIdentity SecureLogin** (Protocom → ActivCard)
 - Novell SecureLogin
- **Passlogix v-Go SSO**
 - Citrix Password Manager
 - IBM Tivoli Access Manager for ESSO
 - Oracle ESSO suite
 - RSA Sign On Manager
- **Evidian SSO Xpress & WiseGuard SSOWatch** (Enatel)



Marktoverzicht (3/3)

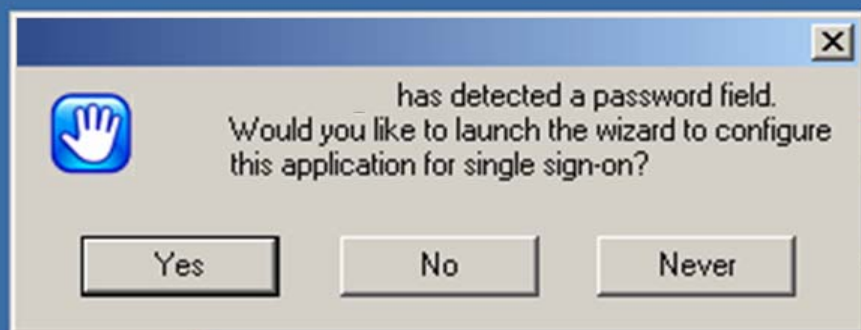
- CA eTrust Single Sign-On
- Imprivata OneSign (appliance)
- PassGo Enterprise SSO
 - SSOPlus (gratis)



DEMO

- Standaardprofiel
- Nieuw applicatieprofiel
 - Login scherm
 - Meerdere credentials
 - Wachtwoordwijziging
 - Policy
- Terminal emulatie
- Systeembeheer





--- Login C/S ---

User ID:

Sector:

Department:

Password:

Environment:

OK Cancel

Add Application Wizard

Select the appropriate fields and enter credentials

Enter required credentials in the fields of the application window you are trying to login to

Drag each of the Hand icons to the corresponding fields in the Login/Change Password window, then click Next

☒

Username:

☐

Password:

☐

Optional:

☐

OK Button:



< Back

Next >

Cancel

Help

User ID:

Sector:

Department:

Password:

Environment:

OK

Cancel

Network
smals-mvm

Applications

- Java
- Terminal Emulator
- Web
- Windows

Logins

Preferences

Password Policies

Advanced Settings

Distribution

Preferences - "All"

General

Allow users to (de)activate SSO via system tray	Yes
Allow users to backup/restore	Yes
Allow users to change passphrase	Yes
Allow users to modify credentials through the GUI	Yes
Allow users to modify names of applications and logins	Yes
Allow users to view and change preferences	Yes
Allow users to view and modify API preferences	Yes
Allow users to view and modify application definitions	Yes
Allow users to view passwords	Yes
Container has priority over User	No
Detect incorrect passwords	Yes
Disable single sign-on	No
Display the system tray icon	Yes
Enable cache file	Yes
Enable logging to Novell Audit	Yes
Enable the New Login Wizard on the system tray icon	Yes
Enforce passphrase enrollment	No
Enter API license key(s)	
Password protect the system tray icon	No

OK
Cancel
Apply



Password Policy - "GDAUTPolicy"

Minimum length	6
Maximum length	6
Minimum punctuation characters	
Maximum punctuation characters	0
Minimum uppercase characters	
Maximum uppercase characters	3
Minimum lowercase characters	
Maximum lowercase characters	3
Minimum numeric characters	2
Maximum numeric characters	2
Disallow repeated characters	Yes
Disallow duplicate characters	Yes
Disallow sequential characters	Yes
Begin with an uppercase character	No
Prohibited characters	



Agenda

- Problematiek
- Situering
- Eigenschappen
- Marktoverzicht
- Demo
- Voordelen / nadelen
- Alternatieven
- Besluit



Voordelen (1/3)

Harde voordelen (ROI berekeningen)

- Tijdswinst voor gebruikers
 $\# \text{ gebruikers} \times \# \text{ applicaties} \times \text{logintijd}$
- Helpdesk kosten voor wachtwoord reset
 $\# \text{ resets/gebruiker} \times \text{gebruikers} \times (\text{kostprijs reset})$
- Licentieprijs
 - Per gebruiker (50 – 100 €)
 - Eventuele serverlicentie



Voordelen (2/3)

# gebruikers	500
# applicaties	5
Tijdswinst / app	5 s
# vergeten wachtwoorden/jaar/gebruiker	2
Kostprijs wachtwoordinterventie	10 €
Totale tijdswinst / jaar	32 d
aan 400 € / dag	12 800 €
Besparing helpdeskkost / jaar	10 000 €
Totaal over drie jaar	70 000 €
Kostprijs tool (aan 70 €, over drie jaar)	56 000 €



Voordelen (3/3)

- Bijkomende kosten voor
 - Sterke authenticatie
 - Implementatie
 - Eventuele serverlicentie
- Zachte voordelen
 - Verhoogde veiligheid
 - Wachtwoordpolicy
 - Generatie van wachtwoorden
 - Gebruikersgemak



Nadelen (1/2)

- PC is uniek toegangspunt ("keys to the kingdom")
- SSO-client software op elke PC noodzakelijk
- PC zonder SSO → gebruiker moet wachtwoorden kennen
- Afhankelijk van aanmeldschermen
- Probleemapplicaties
 - Oude terminal emulatie
 - Niet identificeerbare vensters



Nadelen (2/2)

- One Time Passwords
 - Invullen van pin
 - OTP zelf nog invullen
- Primair wachtwoord vergeten?
 - Self service password reset
- Kostprijs
 - alternatieven?



Agenda

- Problematiek
- Situering
- Eigenschappen
- Marktoverzicht
- Demo
- Voordelen / nadelen
- Alternatieven
- Besluit

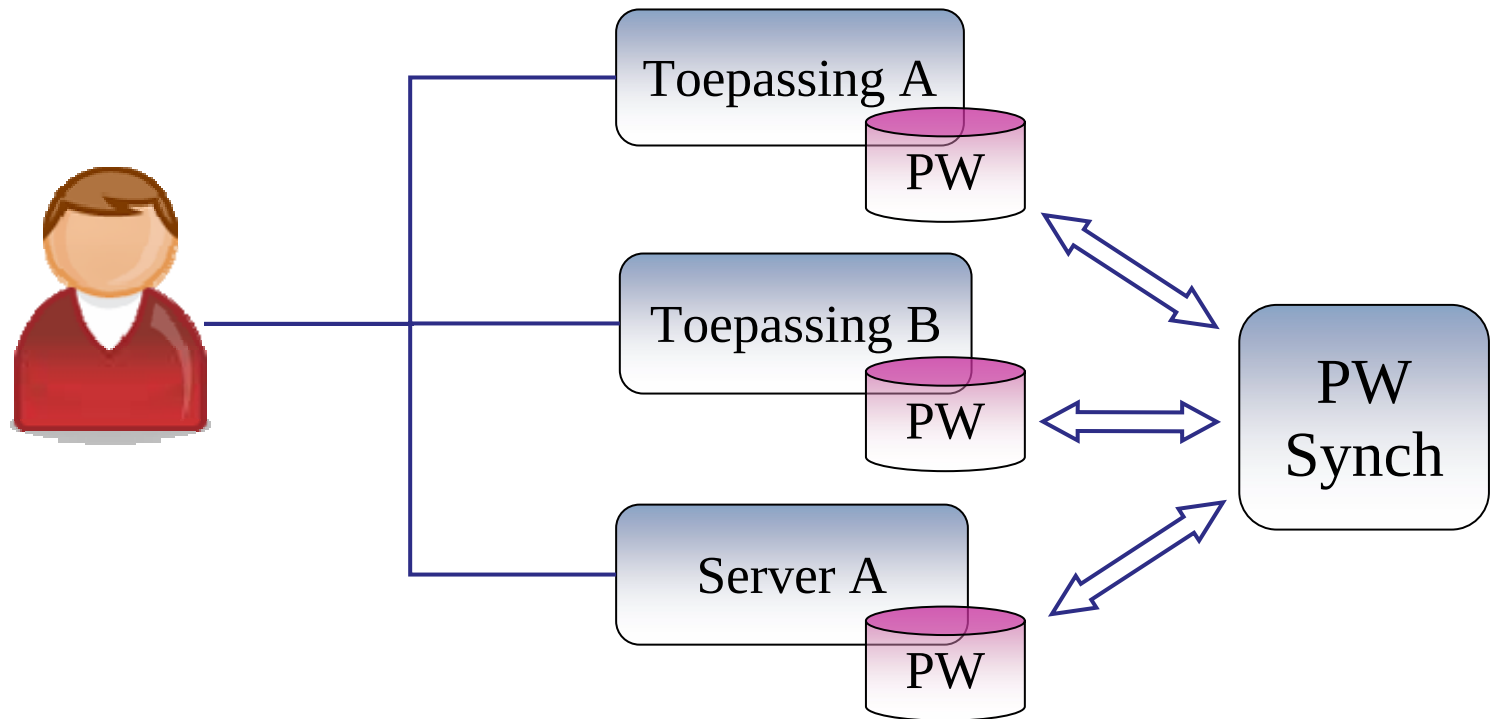


Alternatieven (1/3)

- Desktop SSO ~ lapmiddel
 - Front-end oplossing
 - Systemen zijn niet op elkaar afgestemd
 - Geen gebruik van centrale authenticatie
 - Verschillende wachtwoordpolicies



Alternatieven Password management (1/2)



Alternatieven

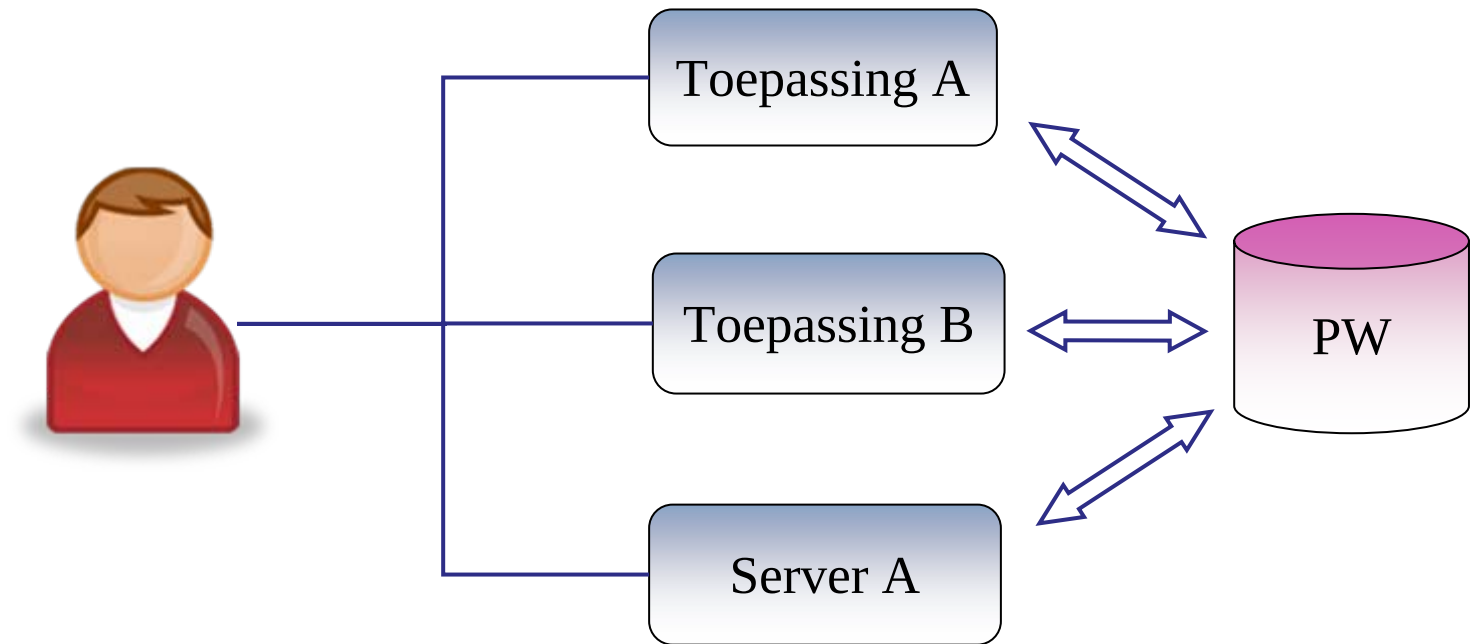
Password Management (2/2)

- Single Log On
- Synchronisatie van verschillende accountsystemen
- Detectie wijziging & propagatie
- Opgelet: complexe problematiek
 - Wachtwoordvereisten $\neq$ elk systeem



Alternatieven

Directory gebaseerde authenticatie (1/2)



Alternatieven

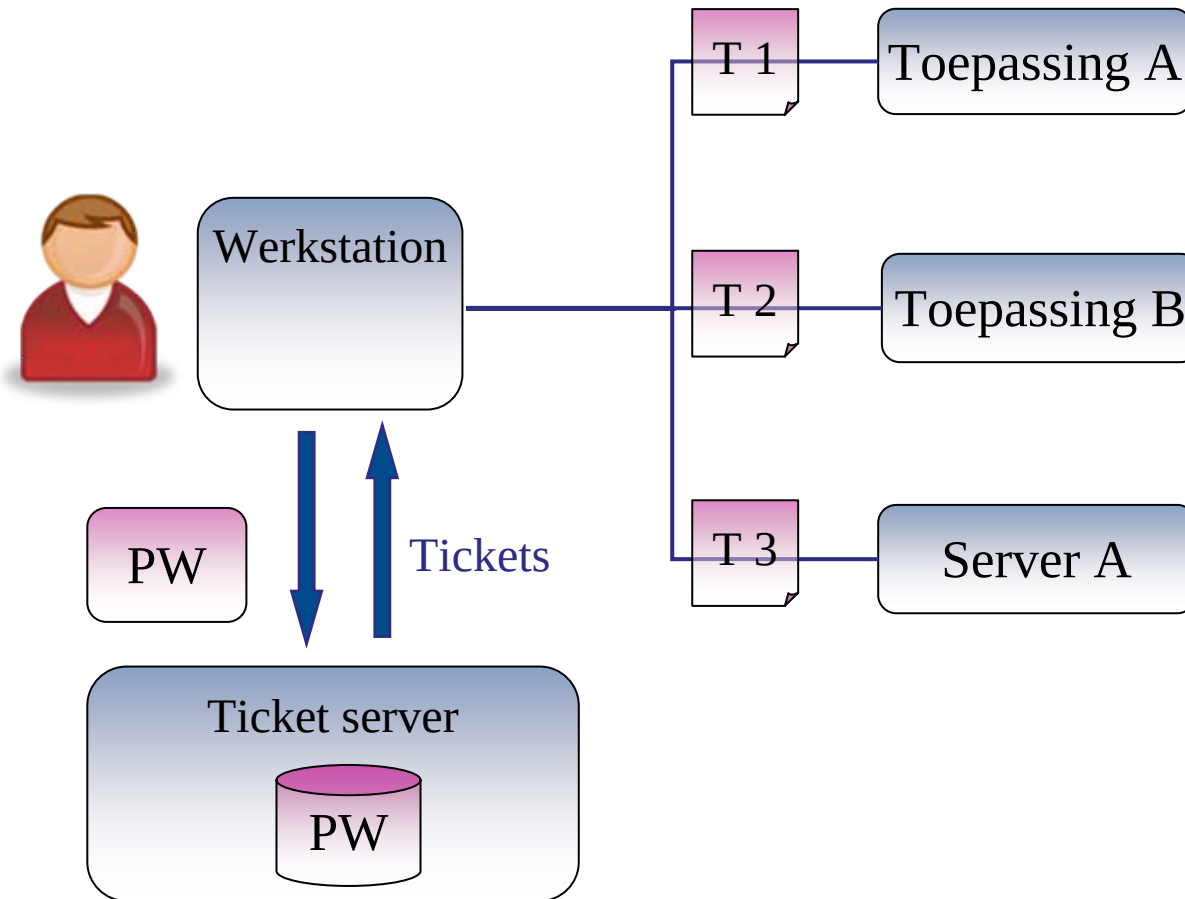
Directory gebaseerde authenticatie (2/2)

- Single Log On
- Centrale directory (LDAP, ActiveDirectory, DB)
- Applicaties moeten gekoppeld worden met directory
- 1 enkele directory voor alle authenticatiegegevens niet altijd realistisch



Alternatieven

Ticket gebaseerde authenticatie (1/2)



Alternatieven

Ticket gebaseerde authenticatie (2/2)

- Single Sign On
- Kerberos/Windows
- Koppeling applicatie – ticketsysteem
- Geschikt voor homogene omgevingen



Alternatieven

- Browser functionaliteit (SSO)
 - Enkel webtoepassingen
 - Lokaal op workstation
 - Beveiliging van credential cache
 - Geen systeembeheer
- Federatie (SSO)
 - Enkel webtoepassingen
 - Cross domein



Besluit (1/2)

- Mature technologie
- "Front-end" oplossing
 - Back-end oplossingen als alternatief
- Is dit iets voor u?
 - Aantal wachtwoorden
 - Soorten systemen
 - Verlies van wachtwoord
 - Toekomst van huidige applicaties
 - Alternatieven



Besluit (2/2)

- Implementatie
 - Uitrollen voor specifieke applicaties
 - Stapsgewijs
 - Uitgebreid testen
- Probleemapplicaties
- Extra's
 - Sterke authenticatie
 - Self Service Password Reset



Vragen?

Bob Lannoy

Mail: Bob.lannoy@smals.be



Referenties

- "Le Single Sign On : Le problème de l'authentification unique", M. Laloy, Maart 2004
- "Gebruikers- en toegangsbeheer", B. Lannoy, Oktober 2005 (http://www.smals.be/site_nl/content/Realisations/smals_realisations_generic_0102.html)

