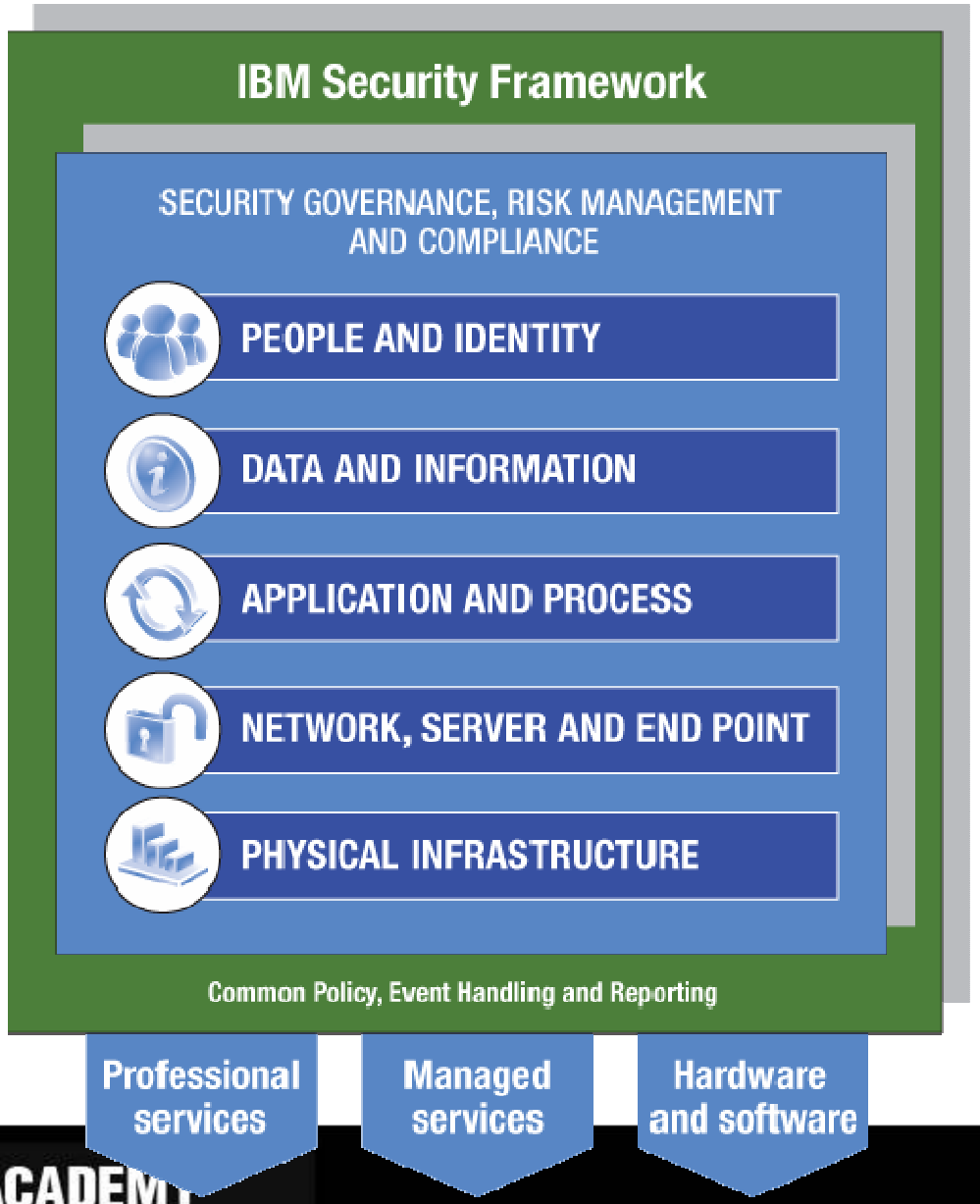
Jak efektywnie i bezpiecznie zarządzać tożsamością użytkowników przy jednoczesnym ułatwieniu korzystania z systemów i aplikacji

TIVOLI SUMMER ACADEMY

25-27 sierpnia, Dwór Chotynia

IBM Security Framework



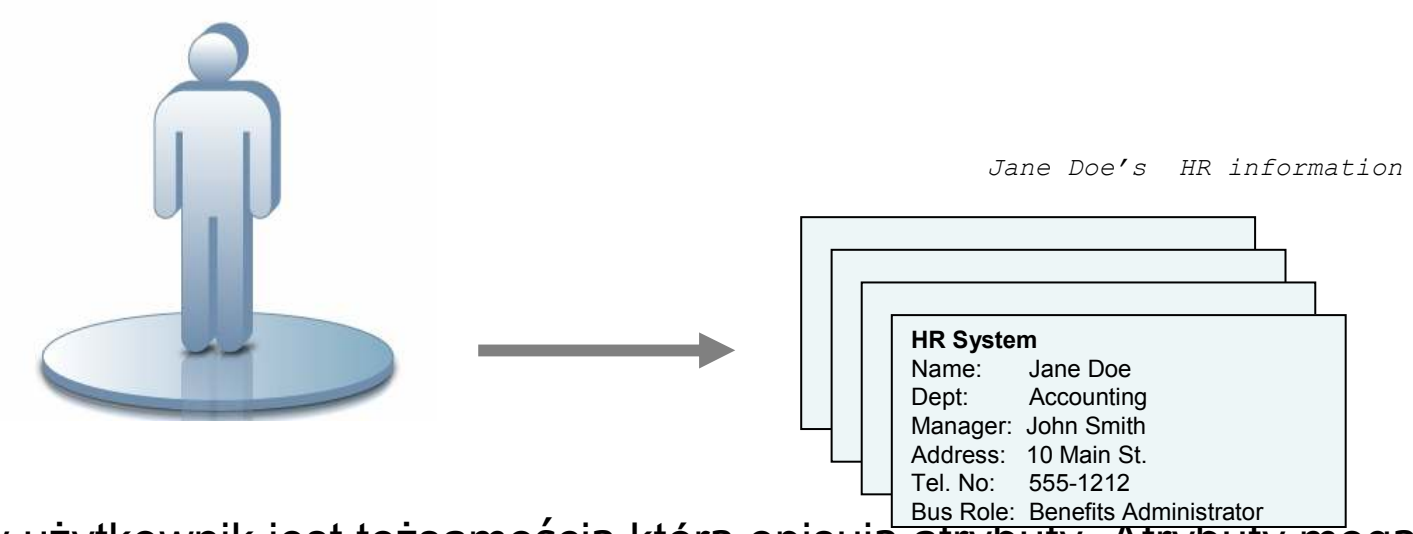
Zarządzanie tożsamością

KTO ma dostęp do **CZEGO** i **DLACZEGO**??

Tożsamości	Polityki	Zasoby

Tożsamości

Użytkownicy którzy potrzebują mieć dostęp do zasobów.



Każdy użytkownik jest tożsamością którą opisują atrybuty. Atrybuty mogą stanowić informacje która może być wykorzystana w podjęciu decyzji do jakich zasobów dany użytkownik powinien mieć dostęp aby móc wykonywać swoje codzienne obowiązki. Przykładem takiego atrybutu może być np. stanowisko.

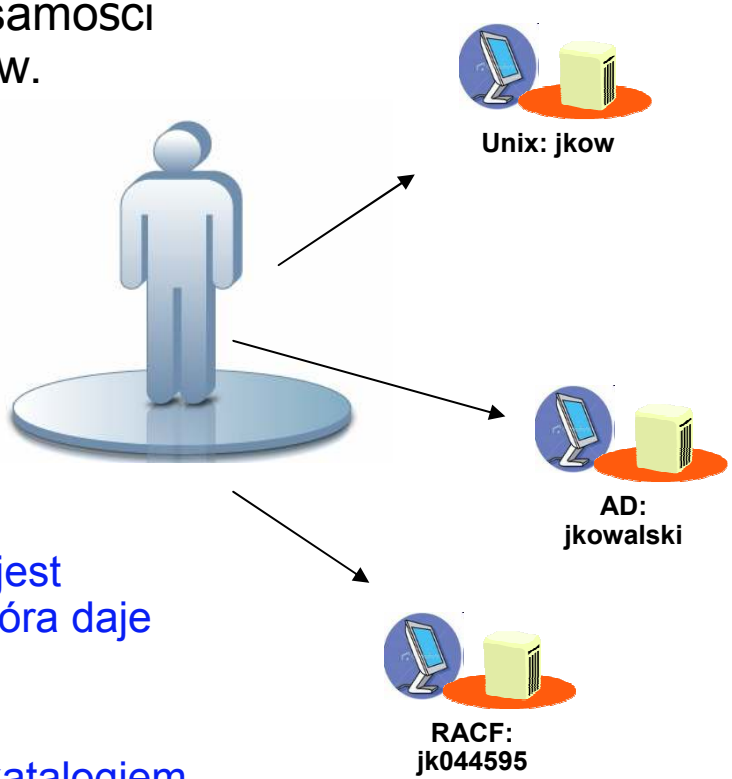
Proces zarządzania tożsamością odpowiedzialny jest za przyznawanie uprawnień użytkownikowi do konkretnego zasobu, ich modyfikację oraz usuwanie uprawnień.

Zasoby

Konta na systemach są wykorzystywane przez tożsamości do wykonywania swoich codziennych obowiązków.

Przykłady:

Systemy Operacyjne	Unix, Windows
Bazy Danych	DB2, Oracle
Aplikacje	SAP, Lotus Notes
Meta Katalogi	Active Directory



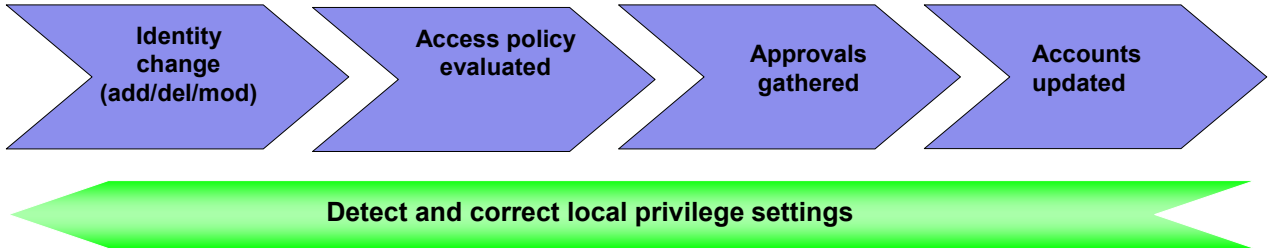
Użytkownik ***jkowalski*** posiada konto w Active Directory i jest członkiem grupy **Domain Users** oraz grupy ***Faktury*** która daje mu uprawnienia do ***Aplikacji Finansowej***.

Użytkownik ***jkow*** posiada konto na systemie AIX wraz z katalogiem domowym ***/home/jkow*** oraz powłoką ***/bin/sh*** a także należy do grupy ***dbadmin***. Grupa ta pozwala użytkownikowi na wykonywanie czynności administracyjnych na bazie danych.

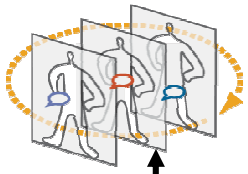
Polityka czyli DLACZEGO uprawnienia zostały nadane?

Polityka definiuje kto może mieć dostęp do zasobów. Politykę określa zestaw uprawnień oraz wykaz osób mogących wnioskować o uprawnienia

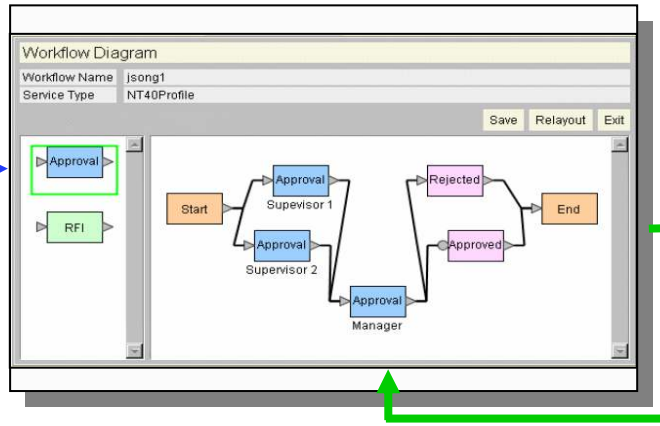
Z polityką związane są procesy które mają na celu zebrać wymagane zgody na przydzielenie uprawnień do osoby wnioskującej oraz ciągłą kontrolę czy osoby te mają właściwe uprawnienia.

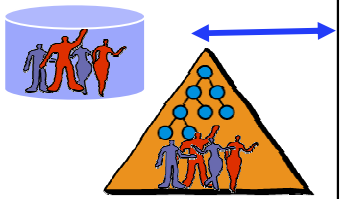


Accounts on 70 different types of systems managed. Plus, In-House Systems & portals



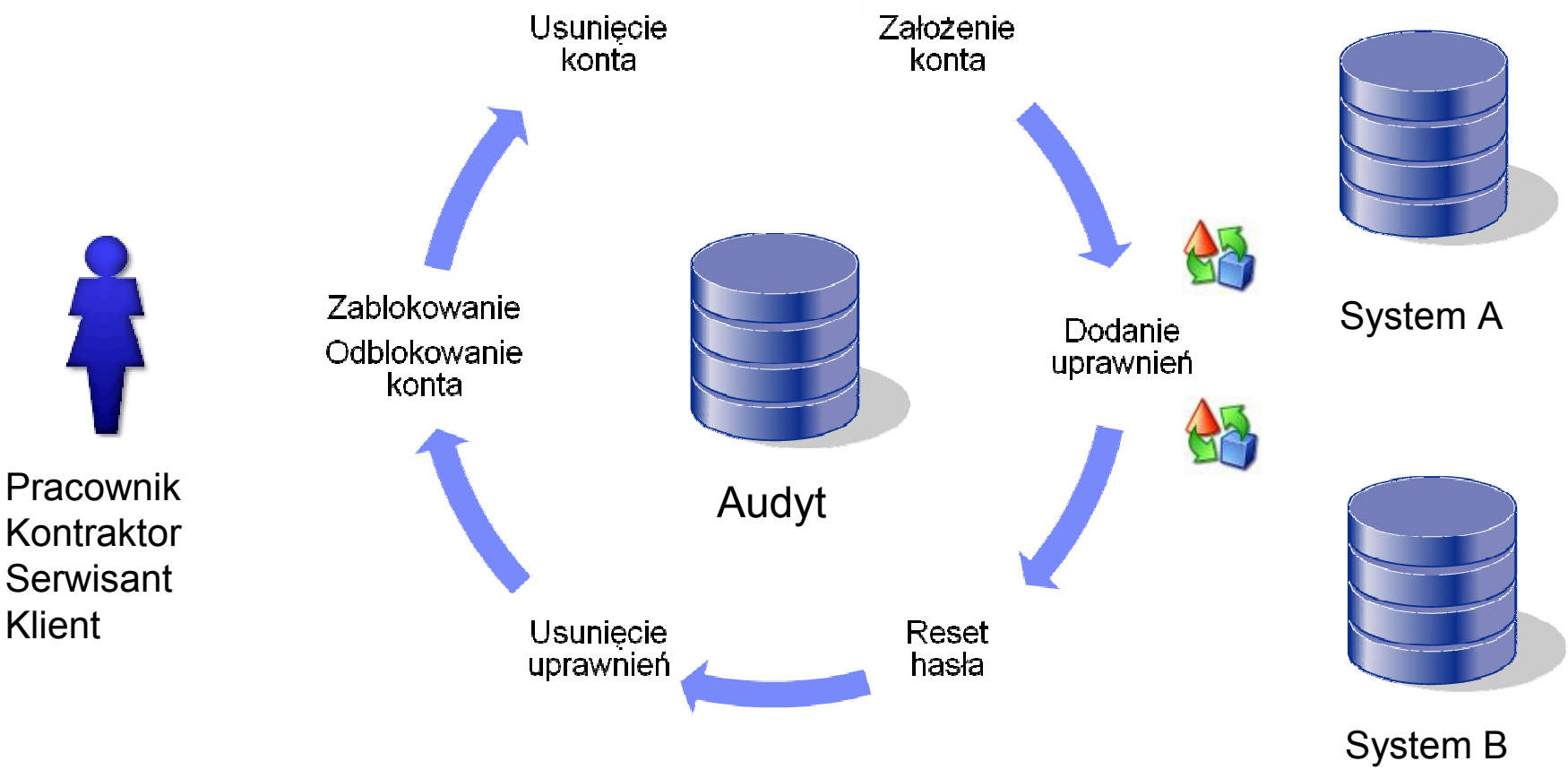
Tivoli Identity Manager





HR Systems/ Identity Stores

Cykl życia konta



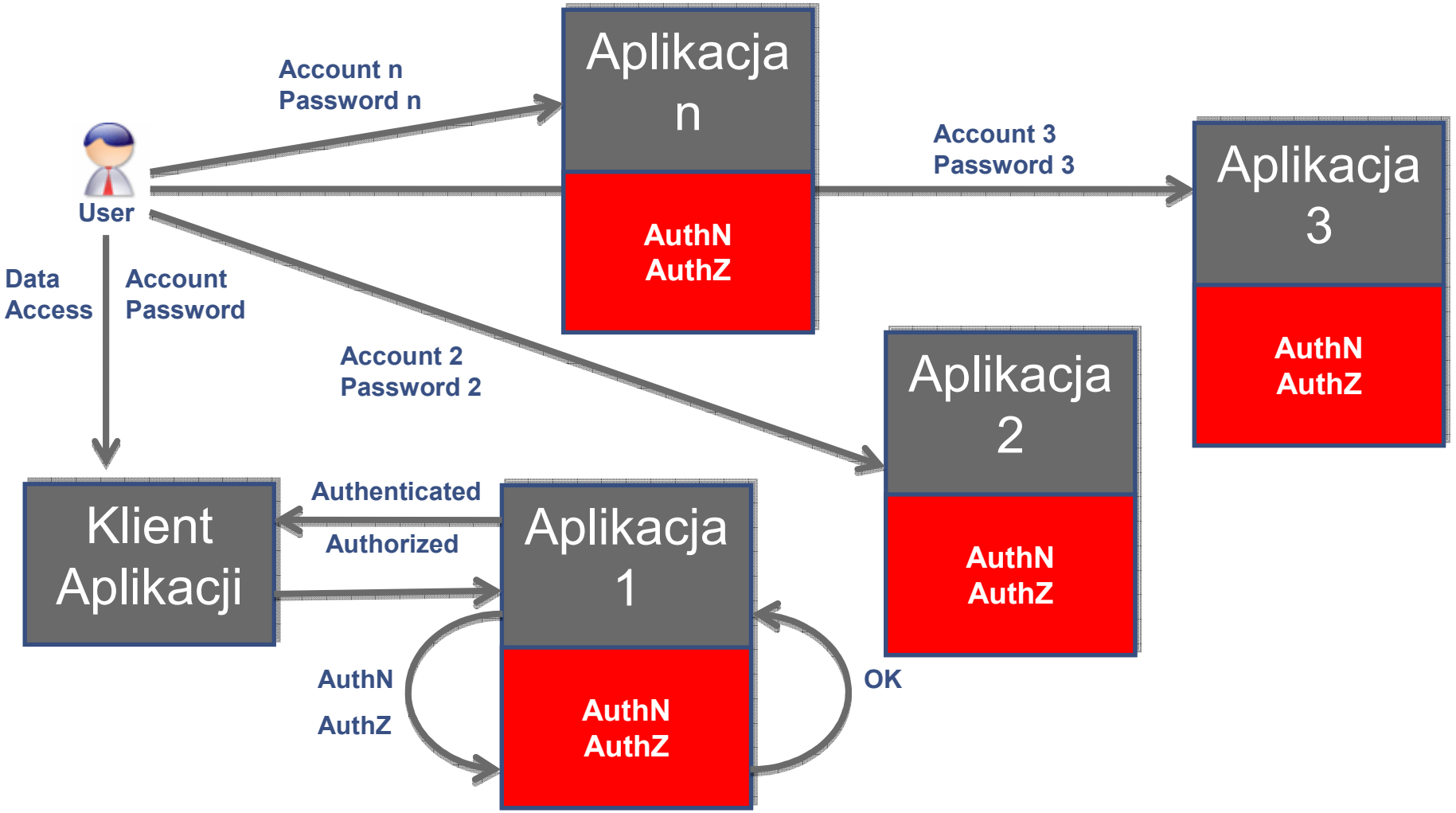
Raportowanie

- 29 gotowych raportów między innymi
- lista użytkowników,
- lista systemów,
- lista uprawnień użytkowników i pełnionych przez użytkownika ról w przedsiębiorstwie,
- lista zdarzeń dotyczących procesów (np. kto wystąpił z wnioskiem o konto, kto zatwierdził itp.),
- historia zmian na kontach,
- lista nieużywanych tzn. „martwych” kont,
- lista nieużywanych kont od określonego czasu,
- niezgodności z określonymi zasadami polityki bezpieczeństwa,

- Możliwość wykorzystania ITIM Report Designer do modyfikacji raportów

- Format PDF lub CSV

SSO: Standardowe logowanie



SSO – Standardowe logowanie

- Wiele kont, wiele haseł
  - Użytkownicy zapisują hasła
  - Użytkownicy zapominają hasła -> HelpDesk
  - Użytkownicy przeznaczają dużo czasu na obsługę kont, haseł
  - Użytkownicy posiadający dużo haseł są niezadowoleni
  - Użytkownicy starają się łamać polityki poprzez trywializację haseł, powtarzanie ich
  - Wymuszenie budowy niezależnych polityk kontroli siły haseł
- Duże koszty zarządzania
- Brak audytu zmian haseł

- *„Każdy użytkownik będzie zapisywał hasła jeśli*
- *jest ich więcej niż 4 i są okresowo zmieniane!!!”*
- *„Większość użytkowników przechowuje zapisane*
- *hasła w pobliżu stacji roboczej”*
- *„Najłatwiejszym sposobem otrzymania*
- *nieautoryzowanego dostępu do danych*
- *jest kradzież zapisywanych przez*
- *użytkowników haseł”*

Rozwiązanie w szczegółach

Rozwiązanie w szczegółach

Silne uwierzytelnienie

- Wsparcie dla:
  - Passive RFID (Mifare, HID iClass)
  - Active RFID (Xyloc)
  - Tokeny (Vasco, Authenex)
  - USB Key (DigiSafe, Charismathics)
  - MobileAccessCode
    - SMS
    - E-mail
  - Sonar
  - Biometryka (UPEK, DigitalPersona)
- Wsparcie dla:
  - Logowania do systemu
  - Logowanie do aplikacji
  - 2FA
  - Wylogowanie przy nieobecności

ACTIVE RFID

USB Key

TOKENY

SMS

E-MAIL

SONAR

BIOMETRIC

Rozwiązanie w szczegółach

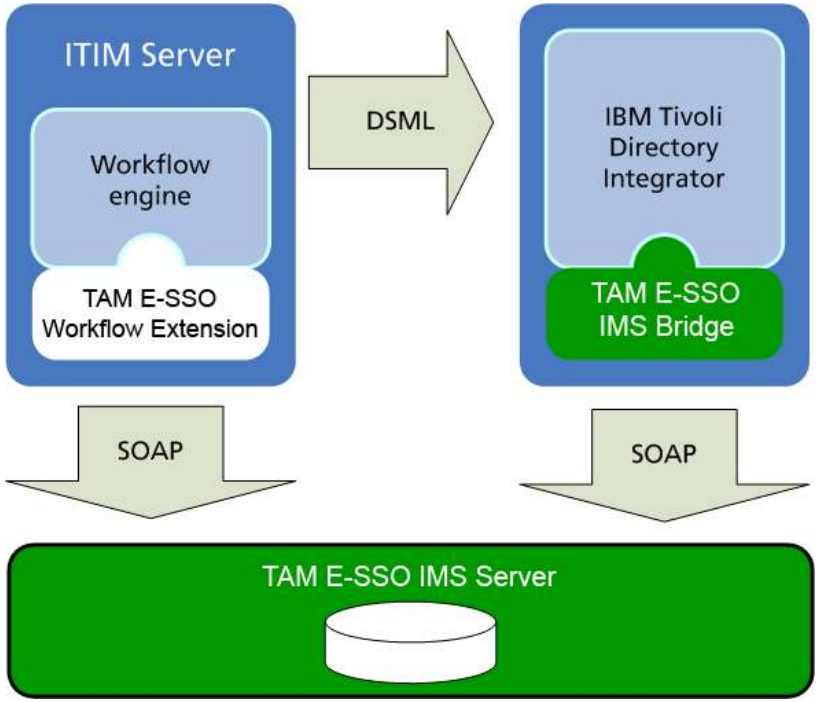
Enterprise SSO

- Wsparcie logowania do większości aplikacji:
  - Windows
  - Web
  - Java
  - Terminal, Mainframe
- Automatyczne budowanie dostępów dla aplikacji webowych, windows, java
- Wsparcie dla usług terminalowych
  - Windows Terminal Services
  - Citrix MetaFrame Presentation Server
- Wsparcie dla cienkiego klienta
  - Terminale Wyse, NeoWare
  - Windows CE, XP embedded
  - RDP dla Windows 2003, Citrix
- EnGINA
  - Łańcuch GINA zamiast podmiany MSGIN

Rozwiązanie w szczegółach

Integracja z Tivoli Identity Management

- Generowane po stronie IM uprawnienia zasilają portfele użytkowników
- Hasła zmieniane przez użytkowników automatycznie zasilają portfel
- System IM zarządza dostępem do TAMESSO
- Blokowanie portfela użytkownika z IM
- Wsparcie dla TIM 4.6, 5.0 i 5.1



Pytania

Dziękuje za uwagę