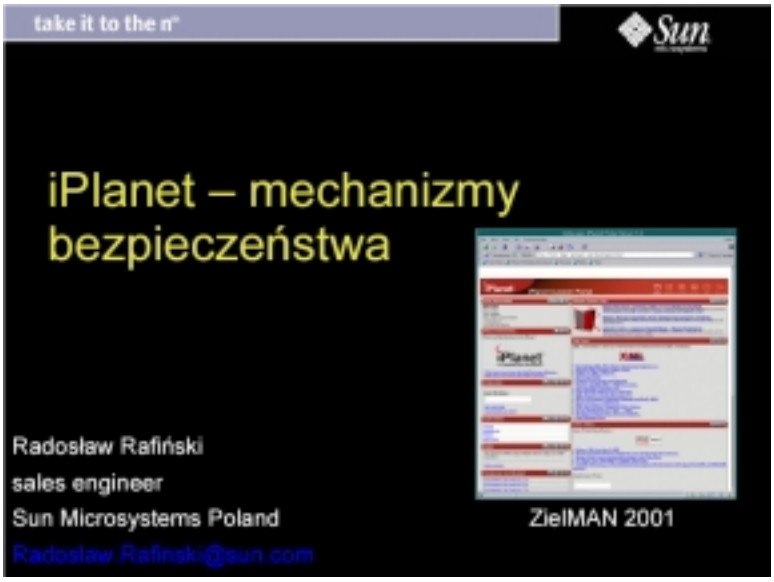
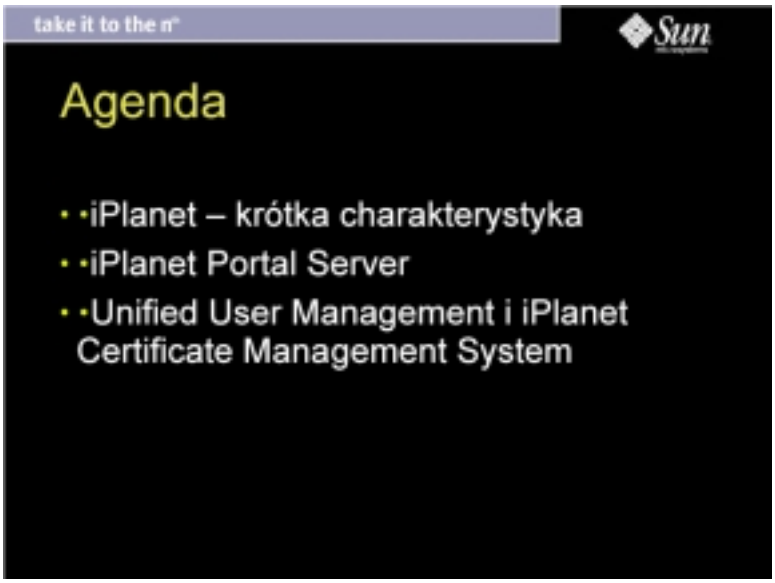
iPlanet – mechanizmy bezpieczeństwa

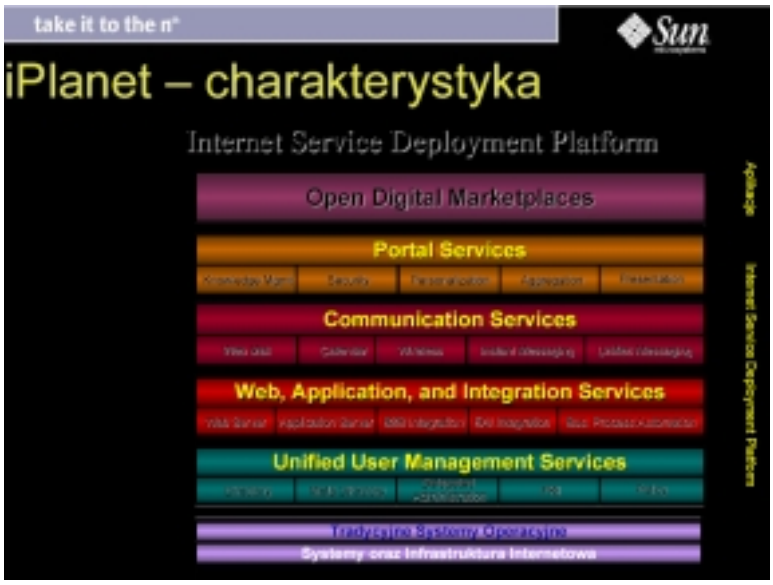
Radosław Rafiński
Sun Microsystems Poland

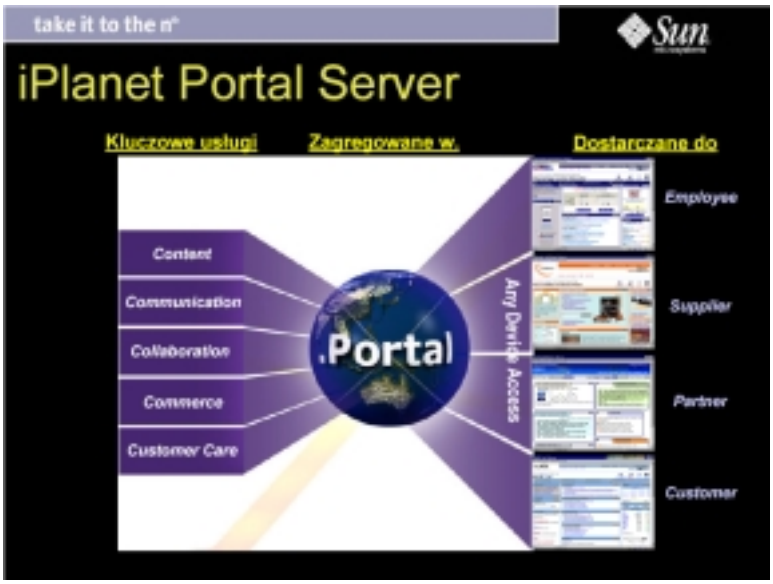
http://www.sun.com/poland/

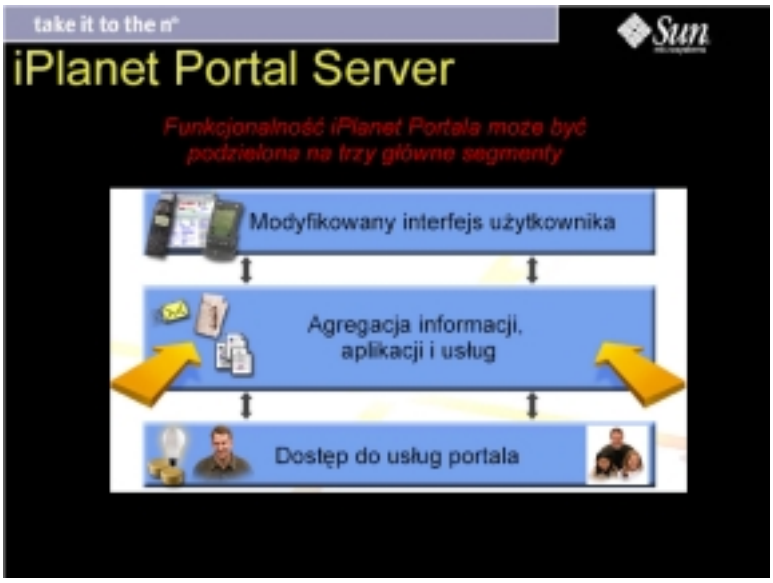


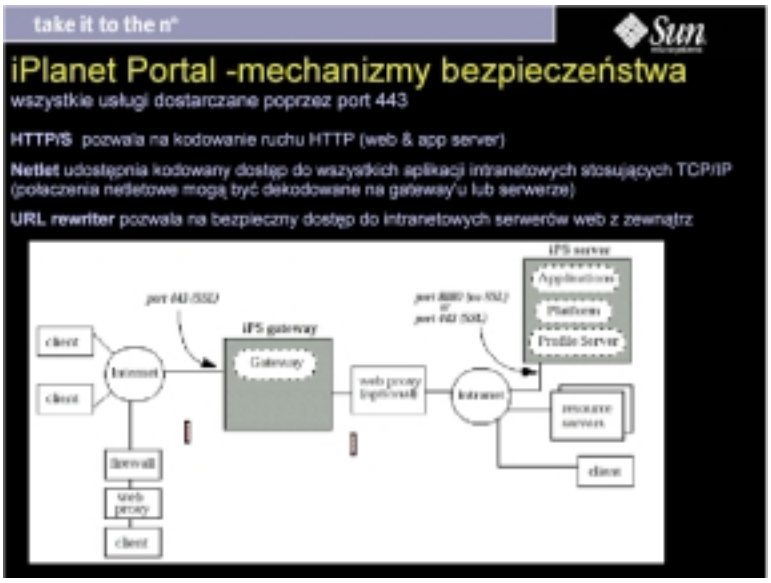

take it to the n
Sun
Agenda
iPlanet – krótka charakterystyka
iPlanet Portal Server
Unified User Management i iPlanet Certificate Management System


take it to the n
Sun
iPlanet – charakterystyka
Alians Internetowy
Platforma sprzętowa
Oprogramowanie, 50M użytkowników portala Netscape
Portal oraz dostęp internetowy, 26M użytkowników portala AOL


take it to the n
Sun
iPlanet – charakterystyka
Internet Service Deployment Platform
Open Digital Marketplaces
Portal Services
Communication Services
Web, Application, and Integration Services
Unified User Management Services
Systemy oraz infrastruktura internetowa


take it to the n
Sun
iPlanet Portal Server
Kluczowe usługi
Zagregowane w
Dostarczane do
Content
Communication
Collaboration
Commerce
Customer Care
Portal
Any Device Access
Employee
Supplier
Partner
Customer


take it to the n
Sun
iPlanet Portal Server
Funkcjonalność iPlanet Portala moze być podzielona na trzy główne segmenty
Modyfikowany interfejs użytkownika
Agregacja informacji, aplikacji i usług
Dostęp do usług portala


take it to the n
Sun
iPlanet Portal -mechanizmy bezpieczeństwa
wszystkie usługi dostarczane poprzez port 443
HTTP/S pozwala na kodowanie ruchu HTTP (web & app server)
Netlet udostępnia kodowany dostęp do wszystkich aplikacji intranetowych stosujących TCP/IP (połaczenia netletowe mogą być dekodowane na gateway'u lub serwerze)
URL rewriter pozwala na bezpieczny dostęp do intranetowych serwerów web z zewnątrz
iPS gateway
client
client
client

take it to the n

Sun

iPlanet Portal -mechanizmy bezpieczeństwa

metody logowania

- Obsługa standardów:
  - LDAP
  - RADIUS
  - NIS
  - UNIX
  - Secure Computing SafeWord digital token
  - RSA Security SecurID digital token
  - Javacard technology / Smartcard
  - X509v3 Digital Certificates (CRL z CMS, wsparcie certyfikatów Entrust & Verisign)
  - S/Key one time password
  - Microsoft Windows/NT domain
  - Membership
  - API do innych, klienckich mechanizmów autentykacji

take it to the n

Sun

iPlanet Portal -mechanizmy bezpieczeństwa

mechanizm Single Sign On

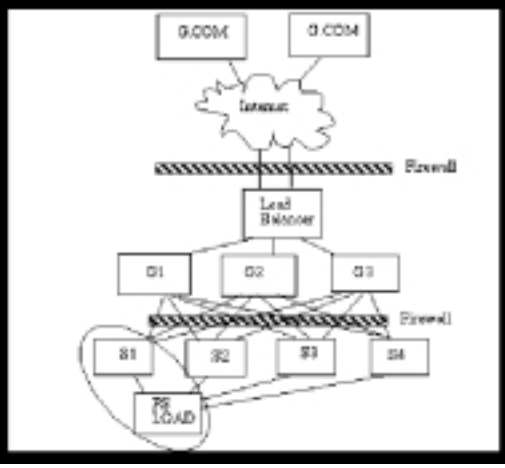
- Klasyczny mechanizm Single SignOn
  - Nie wymaga żadnych modyfikacji po stronie aplikacji i przeglądarki
  - Dostęp do podstawowych aplikacji Web (URL rewriter) i zasobów intranetu (netfile)
- "Customised SSO"
  - Wykorzystuje Portal Serv. Session API do komunikacji z aplikacjami
  - Może wymagać modyfikacji w aplikacjach
  - SID otrzymywane poprzez *cookie*

take it to the n

Sun

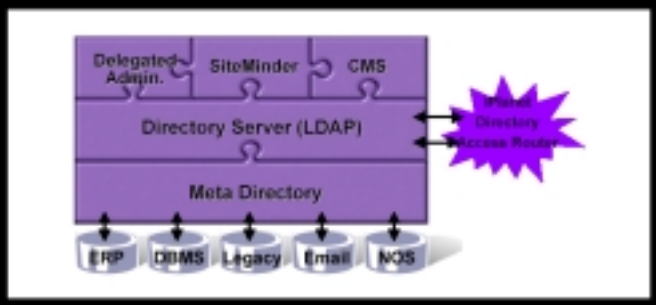
iPlanet Portal -mechanizmy bezpieczeństwa

klastrowanie i "load balancing"



take it to the n

Unified User Management Suite



take it to the n

User Management Suite

- Przechowywanie i zarządzanie profilami i użytkownikami
- Możliwość delegowania zadań administracyjnych
- Autoryzacja użytkowników

take it to the n

UUM – komponenty

- iPlanet Directory Server
- iPlanet Certificate Management System
- iPlanet Meta-Directory
- iPlanet Delegated Administrator
- Netegrity SiteMinder (3rd party)

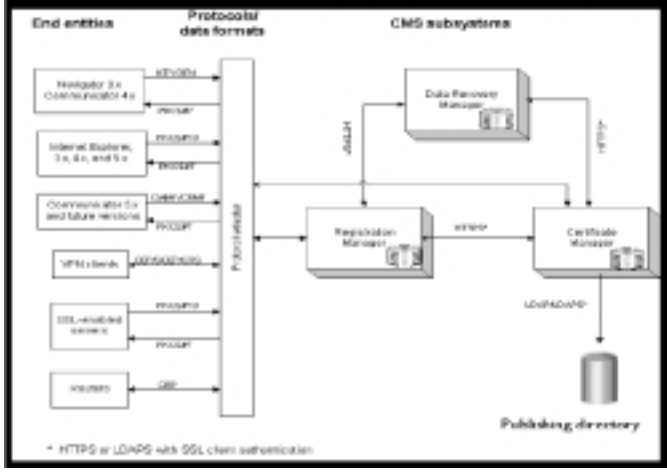
take it to the n°

UUM – zalety rozwiązania

- Bezpieczeństwo rozwiązania (obsługa certyfikatów)
- Wysoka skalowalność
- Uproszczenie i szybkość administracji
  - Centralne zarządzanie przywilejami
  - Automatyczne tworzenie i likwidacja użytkownika we wszystkich podległych systemach poprzez naciśnięcie jednego klawisza (aplikacje webowe, bazy danych, e'mail, ERP ...)
  - Automatyczne rozsyłanie zaktualizowanych profili
  - "Customer Self Service"

take it to the n°

Certificate Management System



take it to the n°

CMS – komponenty

- Elementy końcowe:
  - Przeglądarki: Netscape Navigator, Communicator, Microsoft Internet Explorer
  - Serwery obługujące SSL
  - Routery (np. Cisco)
  - "klienci" VPN (Aventail, KyberPass, RedCreek)
- Certificate Manager
  - Autoryzacja certyfikatów, akceptacja i autentyfikacja zgłoszeń od elementów końcowych (bezpośrednio lub poprzez Registration Manager-a)

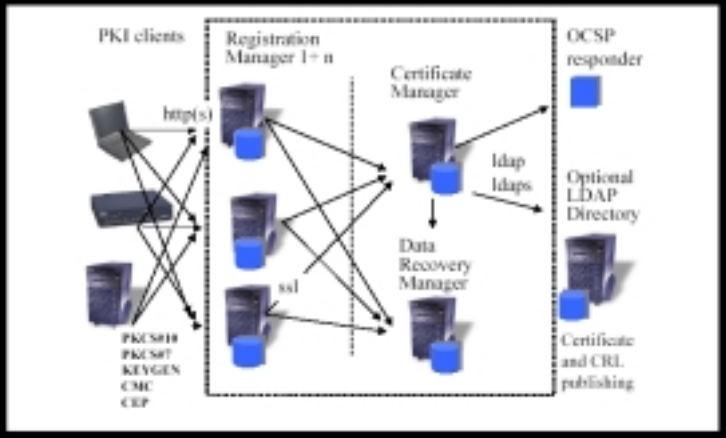
take it to the n

CMS – komponenty cd.

- Registration Manager
  - Zdalna rejestracja, obsługa certyfikatów, odzyskiwanie i generacja kluczy.
  - Kilka RM może współpracować z jednym CM
- Data Recovery Manager
  - Przechowywanie i odzyskiwanie kluczy prywatnych
- Internal Database
  - iDS instalowany razem z CMS
- Publishing Directory
  - Umożliwia ogłaszanie certyfikatów i CRL-i dla serwerów zgodnych z LDAP

take it to the n

CMS – architektura



take it to the n

CMS – elementy kryptografii

- Obsługa certyfikatów z podwójnym kluczem
- Obsługa algorytmów RSA, DSA
- Długości kluczy: 512 – 4096 bitów (RSA), 512 – 1024 bity z 64 bitowym krokiem (DSA)
- Współpraca z tokenami sprzętowymi i akceleratorami kryptograficznymi (nCipher, Chrysalis Luna, Rainbow Technologies)
- Obsługa SCEP i IPSEC – do automatycznej certyfikacji urządzeń sieciowych


take it to the n
Sun
CMS – zgodność ze standardami
CMC: IETF PKIX Certificate Management Standards
SCEP: Certificate Enrollment Protocol
FIPS 140-1: NIST Security Requirements for Cryptographic Modules
PKCS #7,PKCS #10, PKCS #11,OCSP
X.509 v3: formats for digital certificates
LDAP v2, v3,LDAPS: Lightweight Directory Access Protocol
SSL 2.0, 3.0: Secure Socket Layer


take it to the n
Sun
Więcej informacji...
http://www.sun.com
http://www.sun.com.pl
http://www.iplanet.com


Sun
microsystems
Sieć n = spotęgowany Efekt