Biometric SSO Authentication Using Java Enterprise System

Edward Clay
Security Architect
edward.clay@sun.com

&

Ramesh Nagappan CISSP
Java Technology Architect
ramesh.nagappan@sun.com

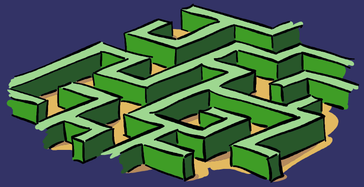
Agenda

Part 1 : Identity and Biometrics

- Why/why not password and user ID
- What is biometrics
- Different topologies of biometrics
- Which biometrics is most widely excepted
- The good the bad and the ugly of biometrics

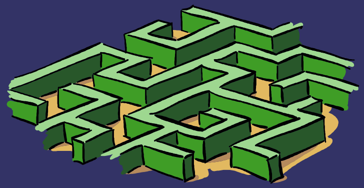
Part 2 : Multi-factor Biometric SSO Authentication

- Logical Architecture
- Tools of the Trade
- Access Manager – Biobex Integration for SSO
- Building an Authentication Chain with Smartcards
- Biometrics Provisioning using Identity Manager
- Multifactor Authentication Demo.



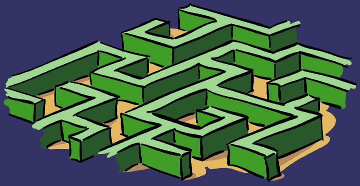
Part 1 - Identity and Biometrics

Ed Clay



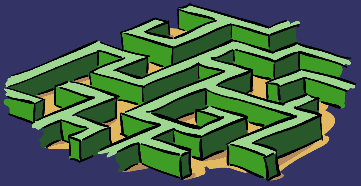
The cyber world

- How do you know who is on the system?
  - User name and password is that enough
    - Is the OS or application secure? (front door is not enough)
    - Did they share it?
    - Did someone steal it?
    - Brute force attack?



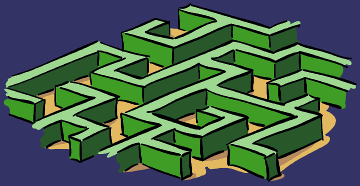
Our focus

- Confidentiality
  - The Who
    - How do we know who is accessing what?
    - User name and password?



The real world

- How do you know?
  - How do you ID a brother, sister, mother or father?
    - What if it changes?
    - What if someone tries to become them?



Identity Management (IDM)

- Identity

A representation of data, including attributes

- Authentication

A level of security guaranteeing the likely validity of that representation

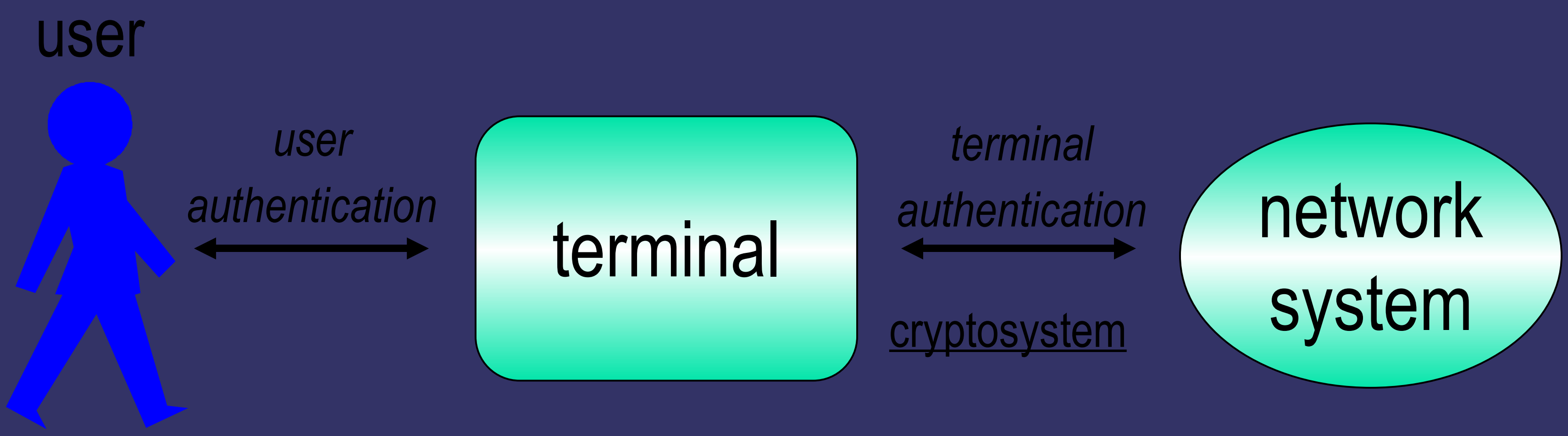
- Authorization

ВИЗА

ВЫЕЗД

The provisioning of services or activities based upon an authenticated identity

Why does Biometrics make since?



user

user authentication

terminal

terminal authentication

cryptosystem

network system

Knowledge-based : Threat of forgetting

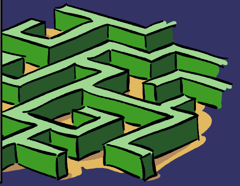
e.g. password

Possession-based : Threat of loss

e.g. Card

Individual characteristics : No threat of forgetting or loss

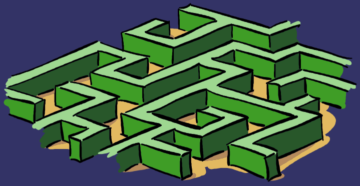
e.g. fingerprint, voice, handwriting



Strong authentication

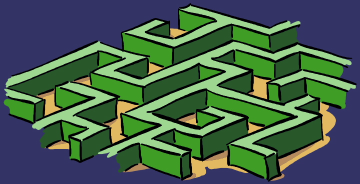
What is it?

- Three factor or Multifactor
  - What I know (Proof of Knowledge)
  - What I have (Proof of Possession)
  - What I am (Proof of Physical/Behavioral)



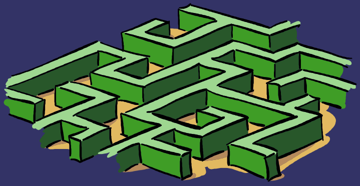
Strong authentication

- Commonly two-factor is used !
  - User name and biometrics
  - SafeWord card and user name and pin number (Sun)



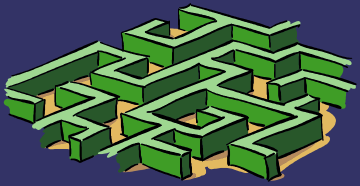
Complexity and cost

- Each layer adds complexity and cost.
  - So why use more then user name and password?
    - Data value (real cost or perceived cost)
    - Resource value (real or perceived)
    - Reduce complexity (SSO or Simple sign on)



Biometrics two main categories

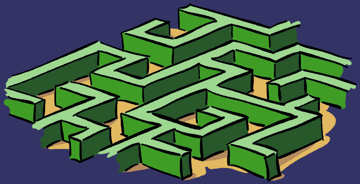
- 1. Phenotypic or Behavioral - Phenotypic traits are ones that we develop or acquire over time through our own individual experiences. Examples of these are voice recognition, signature verification or gait examination.
-
- 2. Genotypic (genetic) or Physical Genotypic identification is the use of individual genetic traits to identify a person. Examples of these are fingerprint analysis, facial recognition and vein patter analysis.



Biometrics two main methods

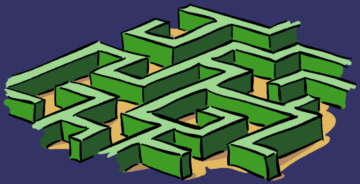
- 1. Passive or covert – Examples of these are Face, Voice or gait
-
- 2. Active or overt – Examples of these are Fingerprint, hand geometry or retinal scanning

Note: Iris scanning technology is becoming covert.



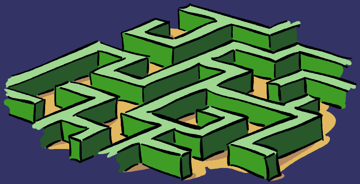
What makes a good biometrics?

- 1. User acceptance
- 2. Ease of use
- 3. Technology costs
- 4. Deploy ability
- 5. Maturity of the technology
- 6. Time for user to get it.



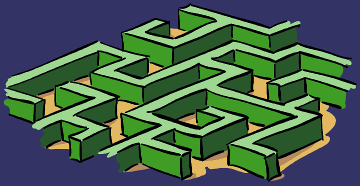
Biometric user acceptance

- 1. Number of calls to the help desk
- 2. Number of attempted authentication (False Accept Rate (FAR) and False Reject Rate (FRR))
- 3. Number of users using fallback authentication
- 4. Right technology for the right location



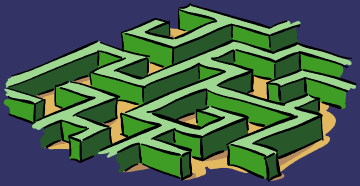
Biometric ease of use

- 1. Ergonomics
- 2. FRR
- 3. Biometric software



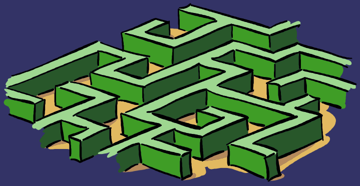
Biometric technology cost

- 1. Device cost
- 2. Deployment costs
- 3. Support



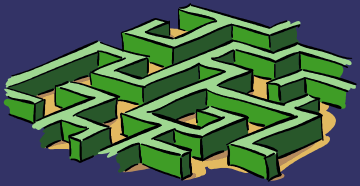
Biometric deploy ability

- 1. Device size
- 2. Environmental conditions
- 3. Infrastructure requirements (is there current support?
- 4. Deployment methodology supported by hardware and software selection?



Biometric maturity of technology

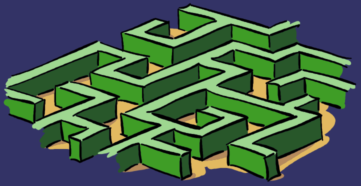
- 1. Market tested
- 2. Improvement in methods (biometric trait, size of device, cost of device or ergonomics)
- 3. Reliable
- 4. Mass produced - not in beta



Most common biometric types

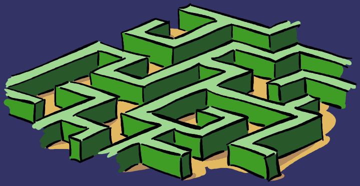
Genotypic biometrics

- 1. Finger print
- 2. Face
- 3. Hand
- 4. Iris



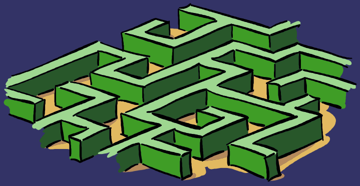
Common Phenotypic biometrics

- 1. Voice
- 2. Signature



The need for standards

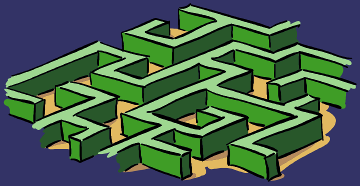
- To accelerate fair competition by clarifying vulnerability and countermeasures.
  - Accuracy test
  - Standards for applying biometrics
- To reduce the cost of system development
  - Application program interface
  - Data format
- For effective development through common framework for biometrics system.
  - Common Criteria
  - Privacy guideline
  - BioAPI, NIST, X9.84, CBEFF, IBIA, ISO 7816-11



The good, the bad and the ugly

All biometrics can be potentially spoofed

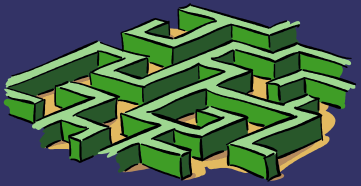
- 1. Every technology has a way to spoof it.
- 2. Technology can make it complicated and costly to spoof.
- 3. Finger print and iris are one of the hardest to spoof. (Tsutomu of Japan)



The good, the bad and the ugly

Not everyone can use all biometrics

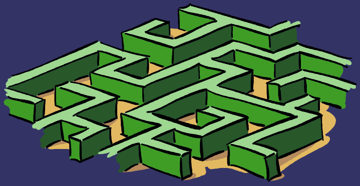
- 1. Missing the part
- 2. Hurt or damaged part
- 3. Not able to cope with the technology



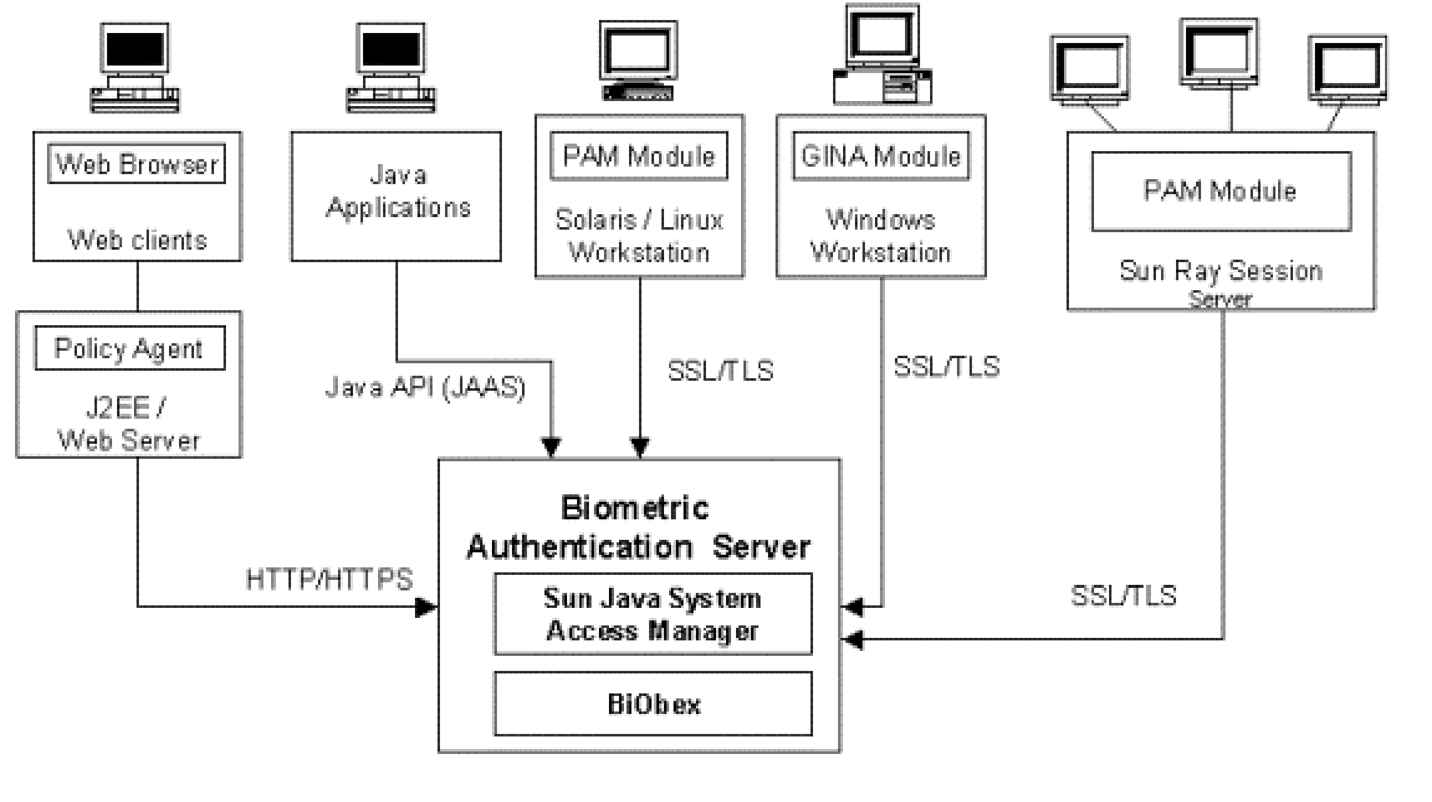
Internalional Biometric Group

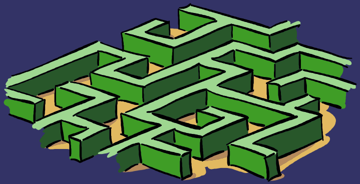
Key Report findings include the following:

1. Global biometric revenues are projected to grow from $2.1B in 2006 to $5.7B in 2010, driven by large-scale government programs and dynamic private-sector initiatives
2. Fingerprint is expected to gain 43.6% of the biometrics market in 2006, followed by face recognition at 19.0%
3. Annual iris recognition revenues are projected to exceed $250m by 2008
4. Asia and North America are expected to be the largest global markets for biometric products and services
5. Multiple-biometric systems will emerge to comprise roughly 5% of the total market for biometrics



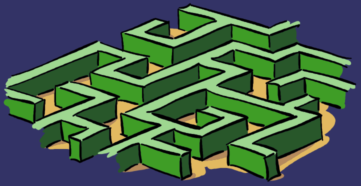
Biometric Integration Options





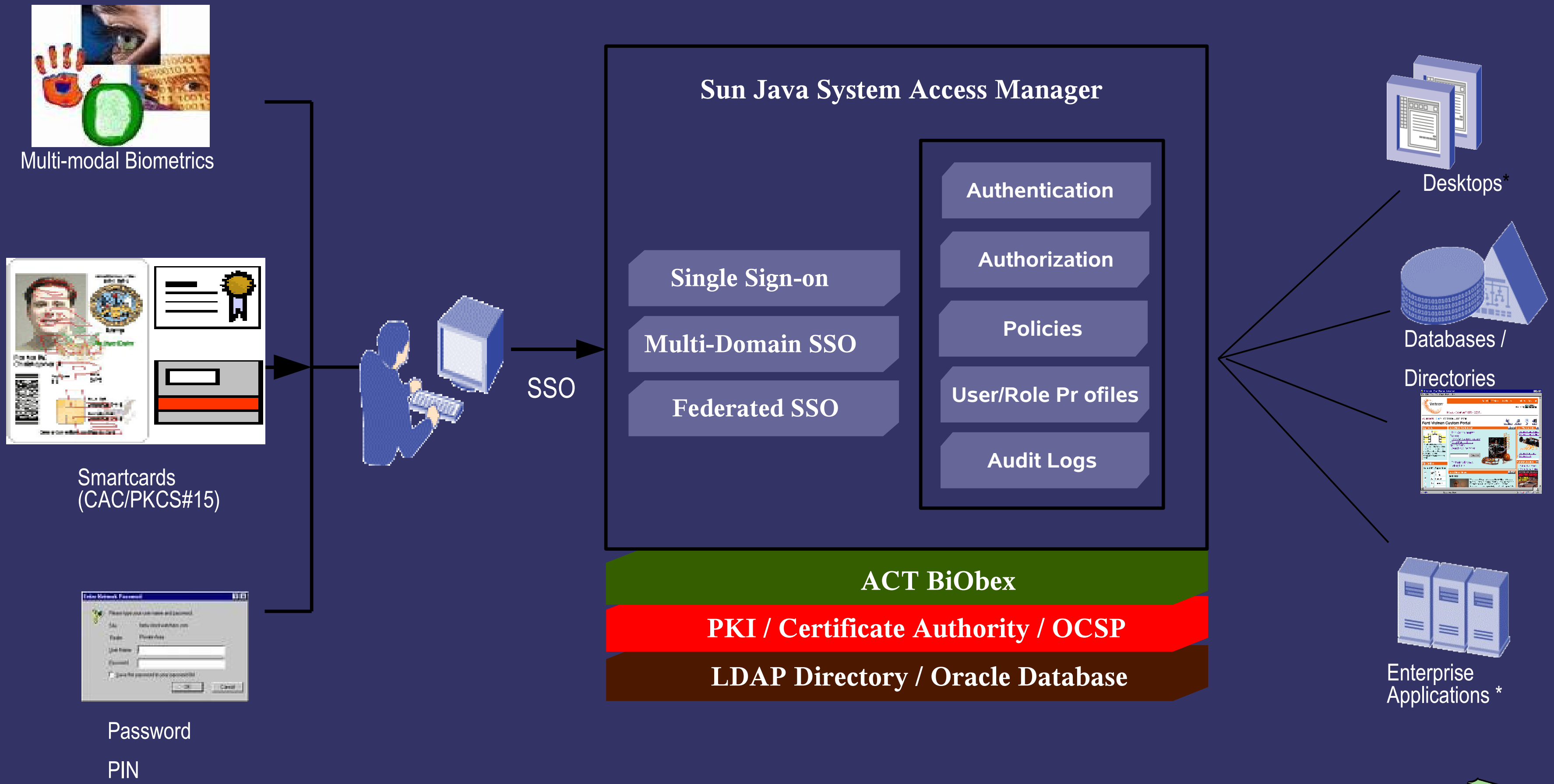
Part 2 – Multifactor Biometric SSO

Ramesh Nagappan



Multi-factor Biometric SSO Architecture

Logical Architecture for enabling SSO and CD-SSO



Multi-modal Biometrics

Smartcards
(CAC/PKCS#15)

Password

PIN

SSO

Sun Java System Access Manager

Single Sign-on

Multi-Domain SSO

Federated SSO

Authentication

Authorization

Policies

User/Role Pr ofiles

Audit Logs

ACT BiObex

PKI / Certificate Authority / OCSP

LDAP Directory / Oracle Database

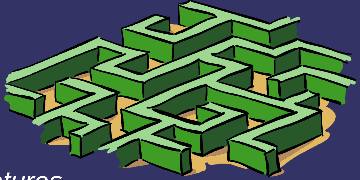
Desktops*

Databases /

Directories

Enterprise
Applications *

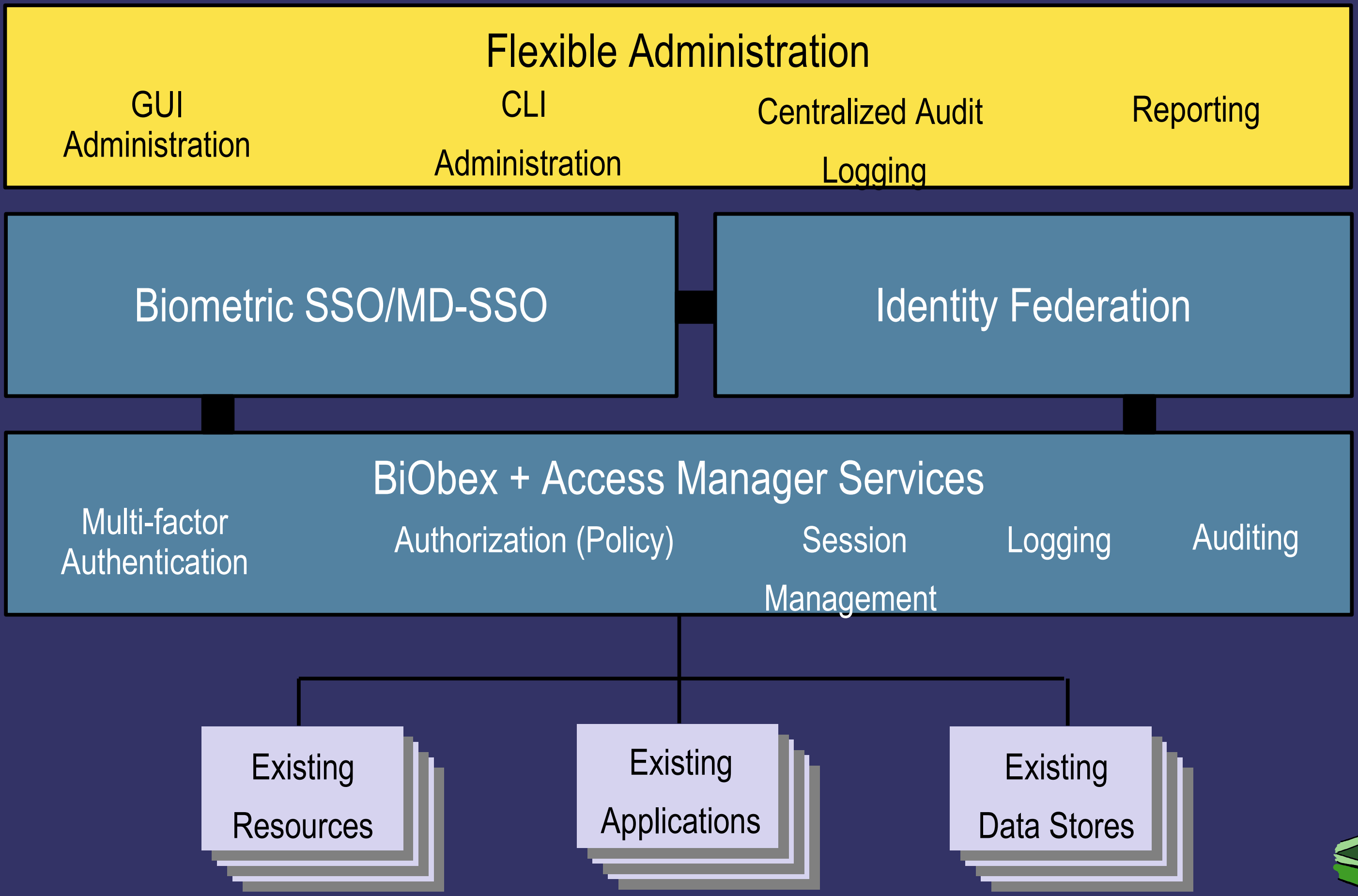
AC TECHNOLOGY, INC.



*SSO/MD-SSO/FSSO to target environment is subject to the availability of supporting authentication scheme and callback features.

Access Manager - BiOBex Integration

Solution capabilities



Flexible Administration

GUI Administration

CLI Administration

Centralized Audit Logging

Reporting

Biometric SSO/MD-SSO

Identity Federation

BiObex + Access Manager Services

Multi-factor Authentication

Authorization (Policy)

Session Management

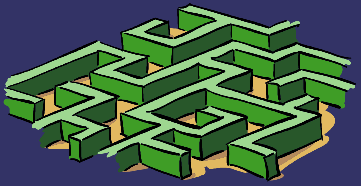
Logging

Auditing

Existing Resources

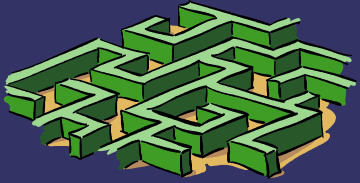
Existing Applications

Existing Data Stores



Tools of the Trade

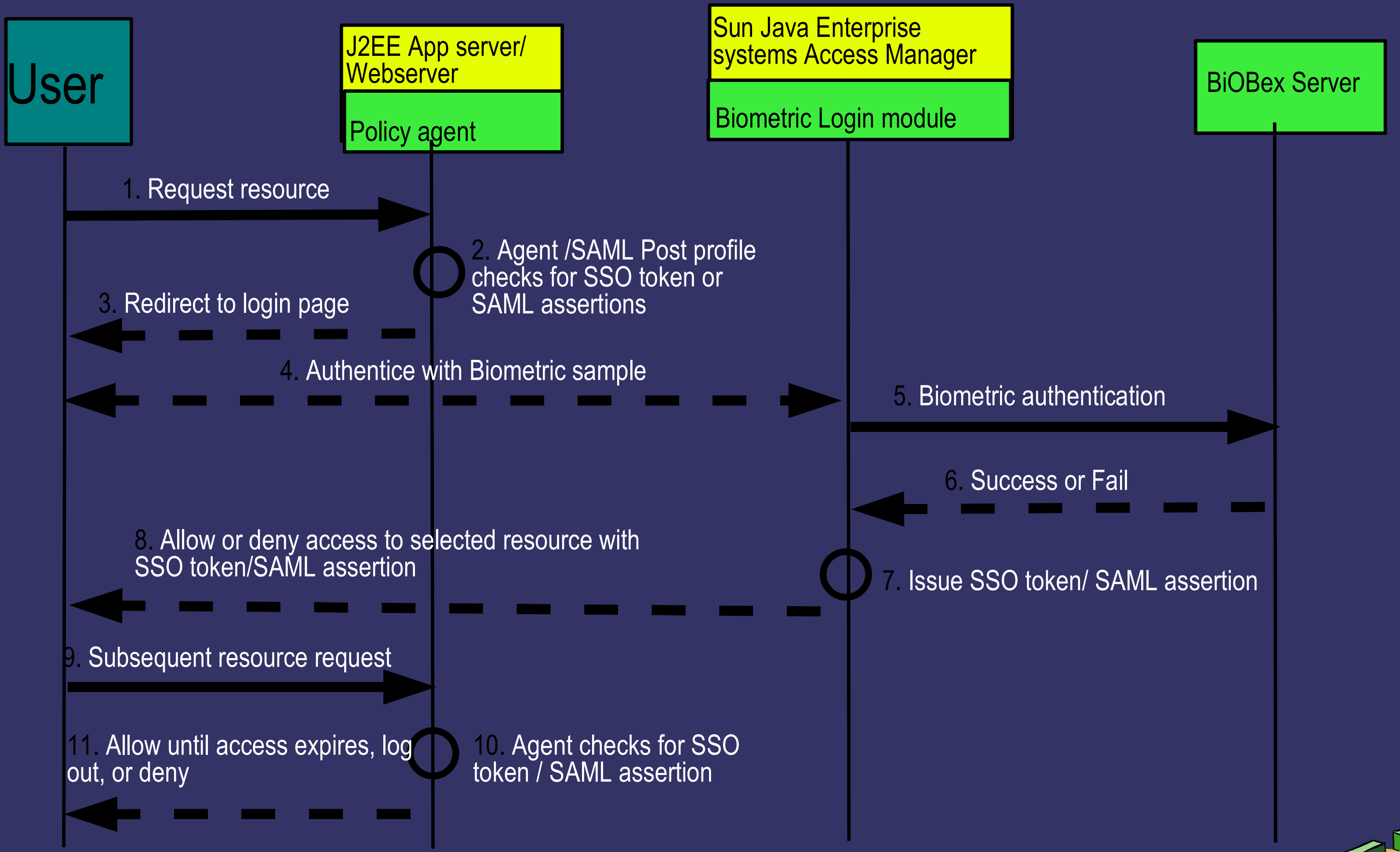
- Sun Java System Access Manager: Configuration
  - BiometricLoginModule for integrating BioBex.
  - Cert module for integrating CAC/PKCS#15 Smartcards
  - LDAP module for LDAP based Password authentication
- Biometrics enabled Desktop Login for Solaris/Linux/SunRay and Windows.
  - PAM Module for Solaris Authentication
  - GINA Module for Windows Authentication
- Sun Java System Identity Manager 6.0
  - SPML Adapter for BioBex
- BiOBex Authentication and Enrollment Server
- ActivIdentity ActivClient for Solaris & Windows (or) OpenSC/Muscle PKCS#11 Plugin for Mozilla



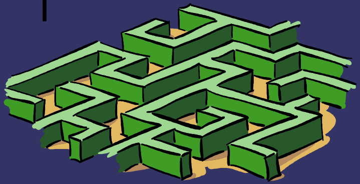
Architecture Highlights

- Multi-factor and Multi-modal Biometrics based Single sign-on (SSO) and Single Log out (SLO) to Web, J2EE, Microsoft and Enterprise Applications.
    - Issue SSO Token or SAML assertions for target sites.
- Biometrics enabled Desktop Login for Solaris/Linux/SunRay and Windows.
- Biometrics based authentication chaining allows Multi-factor authentication with other providers such as Smartcards, LDAP etc.
- SSO. Cross-domain SSO and SAML assertions for supporting applications.
- Identity Provisioning and Synchronization using Identity Manager via SPML.
- End-to-end security infrastructure ensuring confidentiality and integrity at all levels of communication.

Understanding Biometric SSO

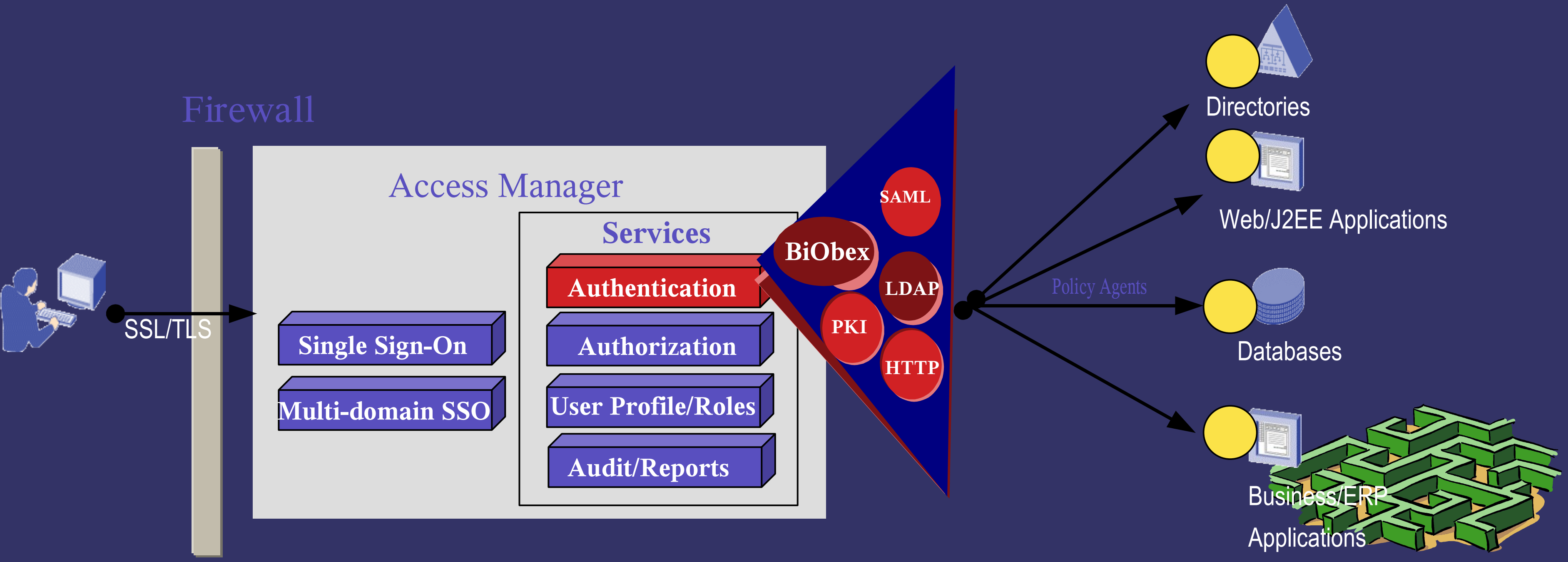


User
J2EE App server/ Webserver
Policy agent
Sun Java Enterprise systems Access Manager
Biometric Login module
BiOBex Server
1. Request resource
2. Agent /SAML Post profile checks for SSO token or SAML assertions
3. Redirect to login page
4. Authentice with Biometric sample
5. Biometric authentication
6. Success or Fail
7. Issue SSO token/ SAML assertion
8. Allow or deny access to selected resource with SSO token/SAML assertion
9. Subsequent resource request
10. Agent checks for SSO token / SAML assertion
11. Allow until access expires, log out, or deny

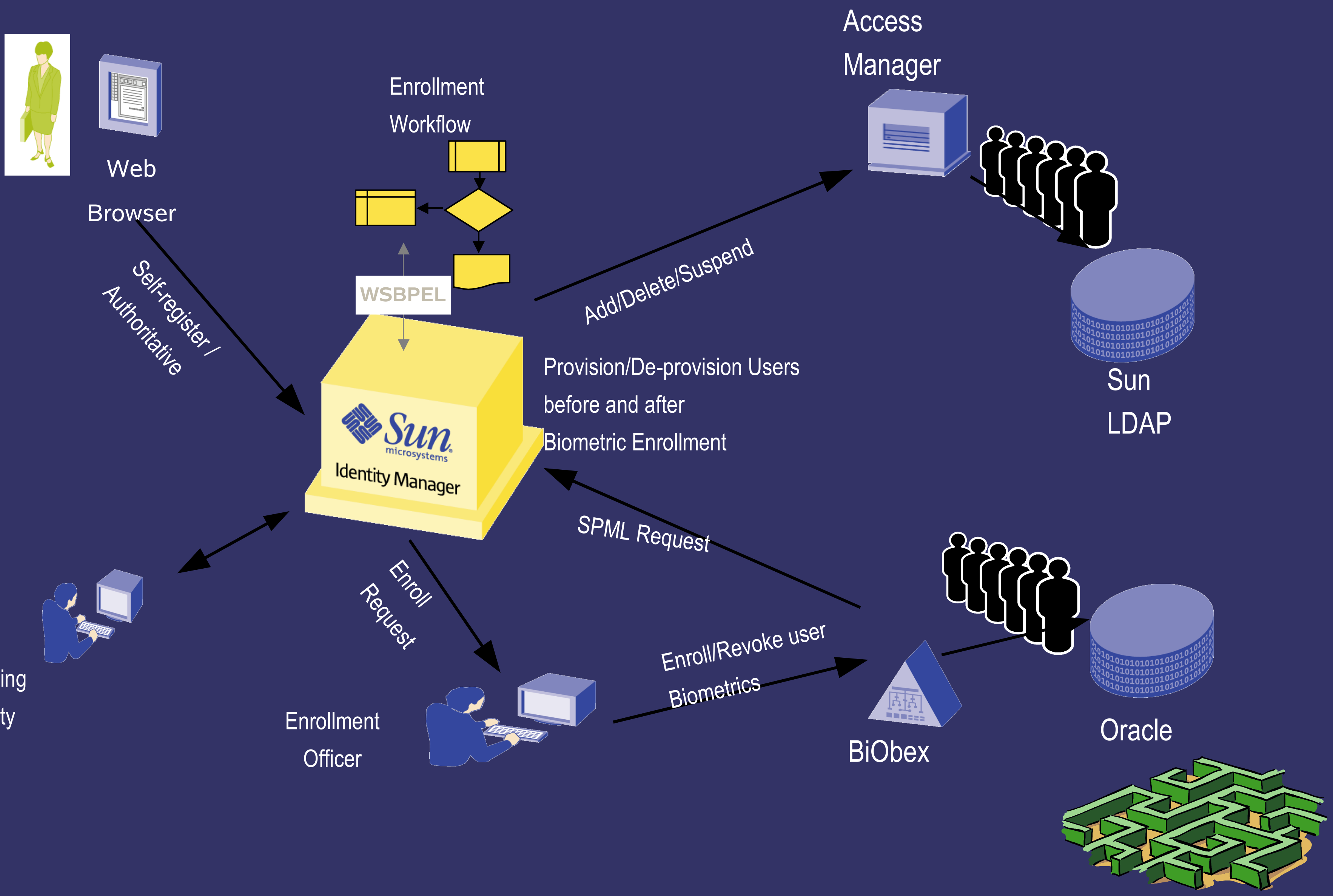


Multi-factor Authentication Chain

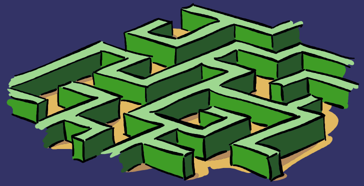
- Access Manager enables multi-factor authentication through authentication chaining features.
- BiObex can be chained with existing authentication mechanisms
  - LDAP, RSA SecurID, Active Directory, JDBC, SAML, others
  - CAC/PKCS#15 Smartcards via Cert Module
- Use custom JAAS based Login modules for unsupported authentication providers.



Provisioning Using Identity Manager



Multi-factor Biometric SSO Portal Demo



Thank you

Ramesh Nagappan
Java Architect
ramesh.nagappan@sun.com

Edward Clay
Security Architect
edward.clay@sun.com