



The State of California

CIO Academy
Identity Access Management
for
Executives

February 27, 2008

Denise Blair, Chief Information Officer
California Department of Mental Health

Agenda



- Introduction Denise Blair
- Identity Access Management (IAM) Top Questions Denise Blair
- State of CA IAM Initiative Status Lee Macklin
- EDD State of CA IAM Case Study Dale Jablonsky
- IAM Panel Discussion Denise Blair
 - Panelist Members:
 - Russell Jones - Principal/Enterprise Risk Services Deloitte
 - John Bennett – Security Specialist Oracle
 - Steven Greenspan - Director of Eng. & Ops. IdM Northrop Grumman
 - Dale Jablonsky – Chief Information Officer EDD
- Q & A

DRAFT

Goals



- Identify Top IAM Questions every CIO needs to be able to answer to their Executives
- Update on the state of Identity Access Management at The State of CA
- Share State of CA Case Study on EDD's IAM Initiative
- Share Industry Insight on the Identity Access Management
- Provide resources to show you how begin your IAM initiative

Top Questions



1. Does your IAM initiative/project have a "champion" within a line of business (or lines of business)?
2. Does the IAM initiative/project have a clear correlation to a "hot button" operational or compliance issue (e.g. access controls/SOD; better customer service through self service, etc..)?
3. Has an IAM strategy and implementation roadmap been developed and if so, does the strategy/roadmap indicate clear, vetted input from the lines of business, human resources, risk management, and internal audit?

Top Questions



4. Is the driver behind the IAM initiative/project someone in one of the lines of business/corporate functions (e.g. HR) or a software vendor?
5. Is the person that you have put in charge of running the IAM initiative/project skilled in cross-functional initiatives? Do they have a track record of working well with liasons from the lines of business/corporate functions?
6. Is the IAM initiative/project aligned with your enterprise architecture (e.g. SOA) and architectural governance processes?

Top Questions



7. Is the IAM initiative/project aligned with (or supports) strategic/tactical enterprise initiatives (e.g. major ERP deployment/upgrade, enterprise portal, etc..)
8. Has the selected IAM technology been through a vetting process which included input (in the form of business/functional requirements) from the lines of business/corporate functions?
9. Is the selected IAM technology a niche player/point solution? How long have they been in business and does their vision/strategic roadmap line up with your vision/strategic roadmap?



The State of California

CIO Academy
Identity Management
Office of State CIO Perspective

February 20, 2008

Lee Macklin, Acting Director
California Enterprise Architecture Program
Office of State CIO

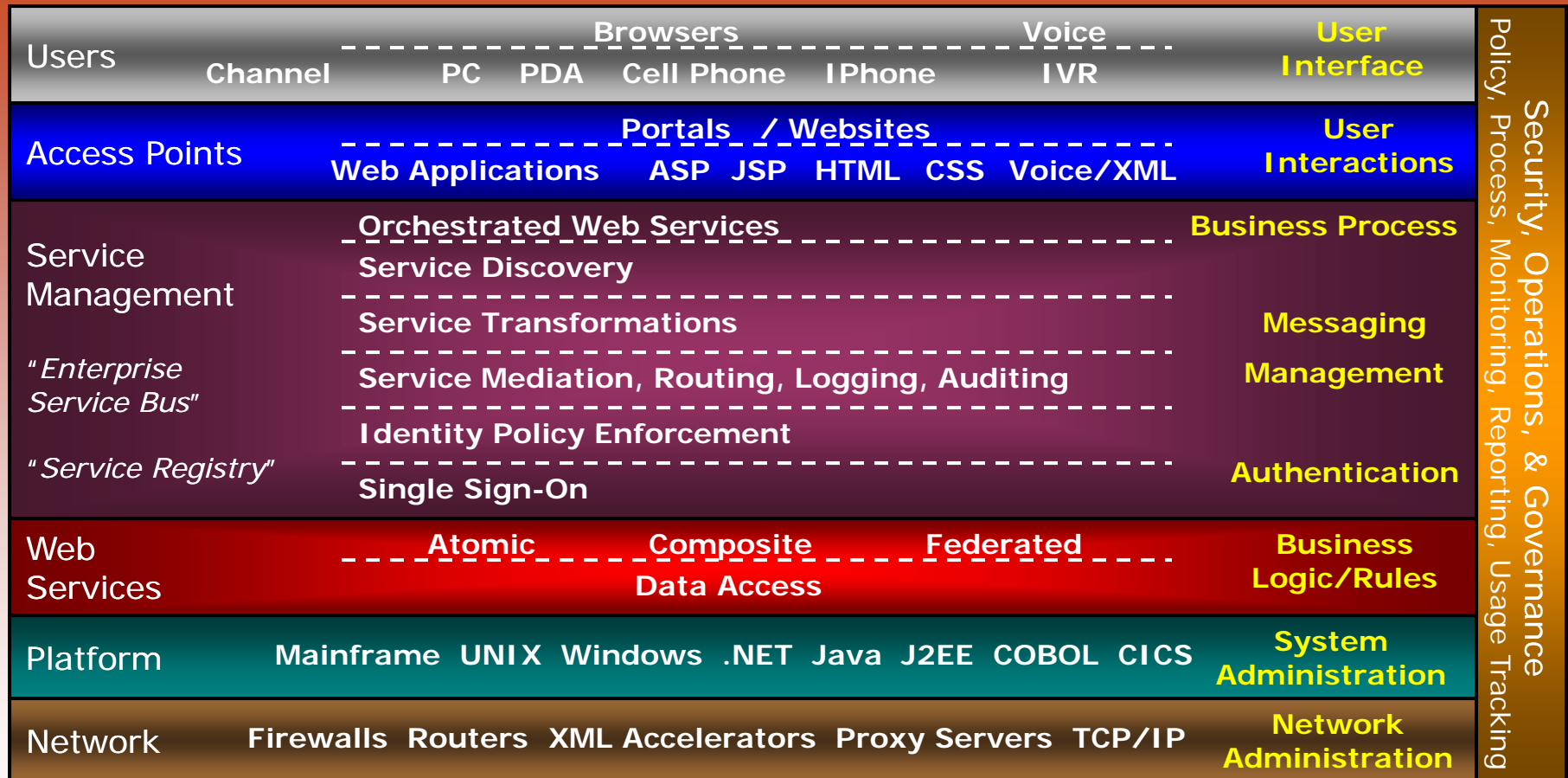
Actively Working On



- Establishing SOA Infrastructure
 - DTS RFI
- Drafting Common Language for SOA & Identity Management
 - Multi-department effort
- Shared Services
 - Processes & Policies
 - Department projects
- Federated Identity Management
 - Progress toward State model
 - Citizens, Medical Providers

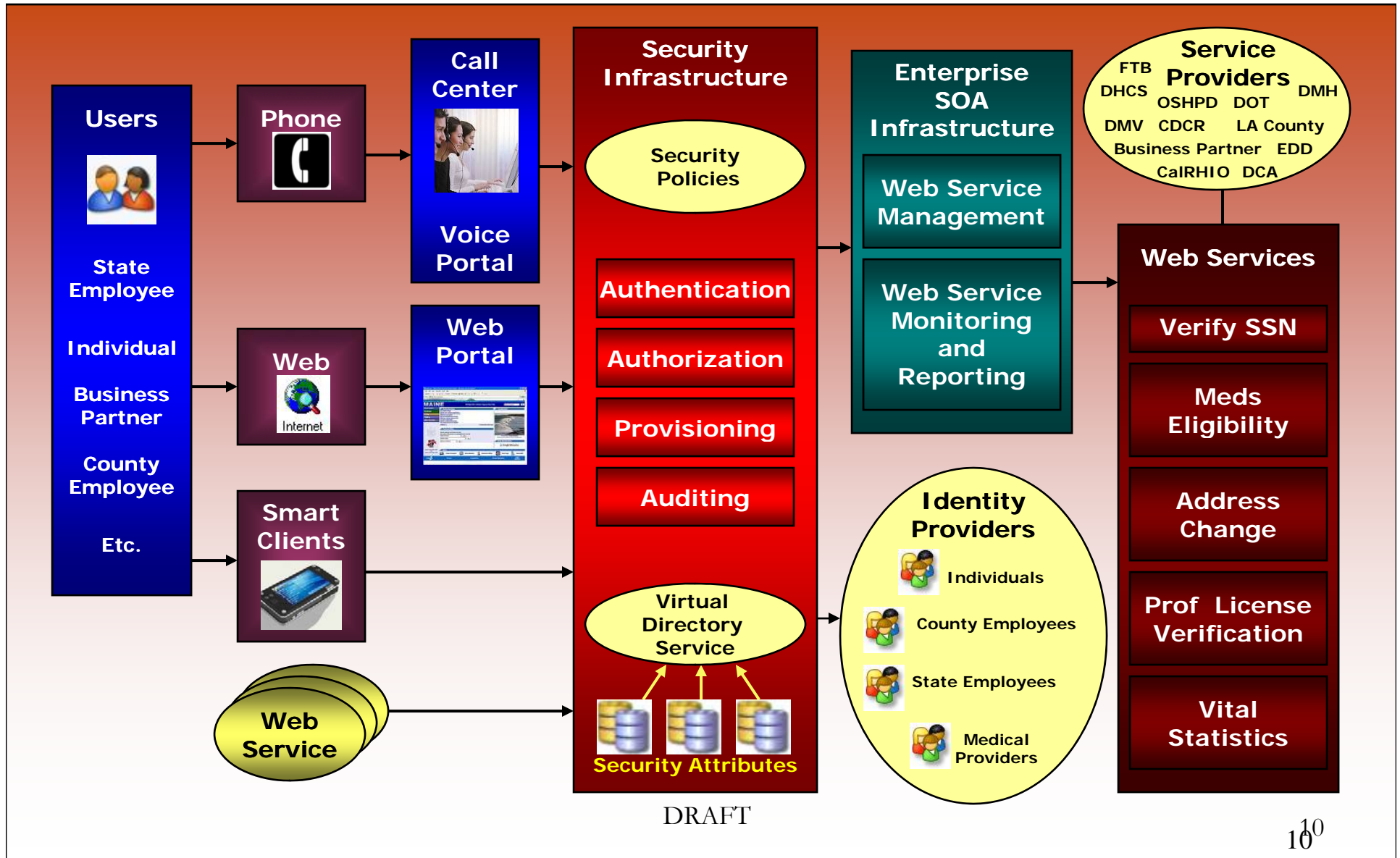
DRAFT

SOA Reference Architecture



DRAFT

Identity Management & SOA



Web Services Security



Key Elements according to Federal Guide to Securing Web Services (NIST 800-95, August 2007)

- Confidentiality of Web service messages using XML Encryption (W3C standard)
- Integrity of Web service messages using XML Signature (W3C) and X.509 certificates (IETF)
- Web service authentication and authorization
 - SAML, XACML (OASIS standards)
- Web Services Security (OASIS standard)
 - End-to-end SOAP messaging security
- Security for Universal Description, Discovery, and Integration (UDDI) (OASIS standard)

Authentication Levels



Assurance levels according to Federal E-Authentication Guide (NIST 800-63)

- Level 1 Basic
 - UserId and Password, Challenge-Response protocol
- Level 2 Single Factor (“Remote Provider”)
 - XML Encryption, Shared secrets, Identity Provider, SAML
- Level 3 Multi-factor (“Proof of Sender”)
 - XML Signature, Identity Provider, SAML
 - Software (digitally signed, encrypted X.509 certificate/PKI)
 - Hardware tokens or One time passwords
- Level 4 Hardware (physical) tokens only
 - Typically smart cards with Bio information

Challenges



- Service Providers have different authentication policies
- Users are defined differently across organizations
- Many standards, protocols, and frameworks to choose from
- Lack of enterprise perspective for project management and funding
- Restrictions on viewing/sharing information across organizations.
- Governance model details need additional work

Questions



Lee.Macklin@dts.ca.gov

916-739-7637

DRAFT



The State of California

CIO Academy

Identity Access Management

EDD Case Study

February 27, 2008

Dale Jablonsky
Chief Information Offices
Employment Development Department

Roadmap to Identity Management



1. Identity Management Requirements Workshop
2. Identity Management Product Selection
3. Identity Management Implementation Strategy

Identity Management Workshop



- Identity Management Background and Introduction
- EDD Baseline Environment
- Use Cases
- Key Requirements
- Conceptual Architecture
- Potential Vendors
- Recommendations & Next Steps

Identity Management Introduction



- Identity Data Services
- Provisioning Services
- Authentication Services
- Access Policy Enforcement Infrastructure
- Federated Identity Services
- Management and Audit Services

EDD Baseline Environment



1. Account Lifecycle Management
2. Applications, Authentication and Authorization

EDD Baseline Environment



1. Account Lifecycle Management

- Citizens/Clients (Individuals)
- State Employees/Contractors
- Employers (G2B)
- Agents
- Government Partners (G2G)
 - Federal Agencies
 - State Agencies
 - Local Government Agencies

EDD Baseline Environment



2. Applications, Authentication and Authorization

- Citizens/Clients (Individuals)
- State Employees/Contractors
- Employers (G2B)
- Government Partners (G2G)
 - Federal Agencies
 - State Agencies
 - Local Government Agencies

Use Cases



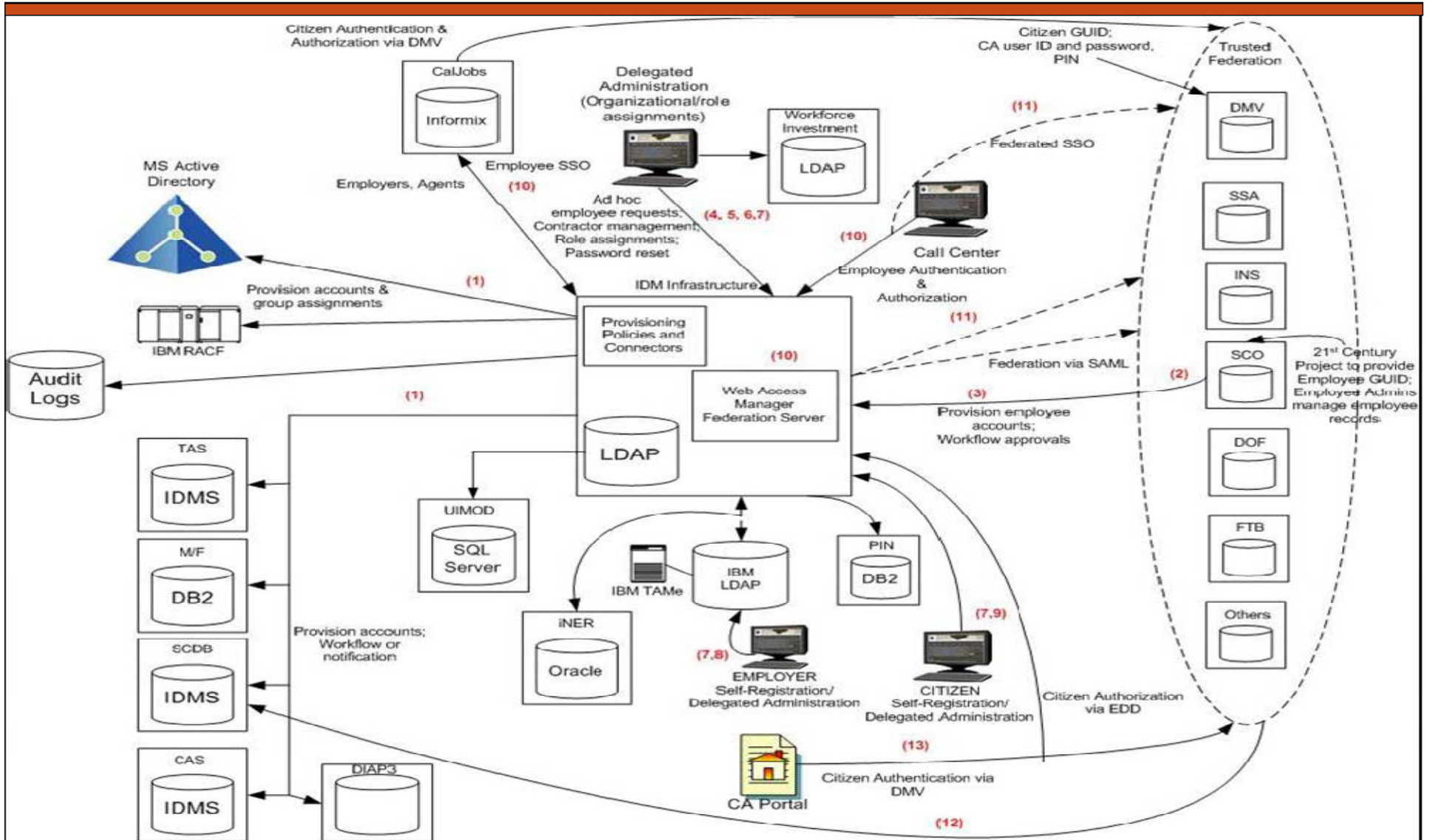
- UI & DI Benefits
- Child Support Services & Benefit Offsets
- EDD Access to DMV (anti-fraud)
- EDD Access to SSA
- EDD Employee Account Provisioning
- Local Gov't Access to Workforce Investment
- Employer Registration
- EDD Application Access (Tax, Claims, Jobs, etc.)

Key Requirements



- Unique Identifiers
- Consistent Management of Identity Data
- Federation with other Government entities
- Authorization by Roles
- Workflow Routing
- Audit Reporting
- Directory Integration
- Delegated Administration
- Self-service Administration

EDD Identity Management Conceptual Architecture



Potential Vendors



- Provisioning
 - Oracle
 - IBM
- Role Engineering
 - Bridgestream
 - Eurekaify

Recommendations & Next Steps



- Make it a Department Initiative
- Select Vendor(s)
- Detail Design and Deployment Strategy
- Evangelize & Educate other State Agencies
- Determine the role of the DMV (Real ID Act)
- Propose & Adopt formal Identity Management Governance
- Develop Identity Management Taxonomy
- Begin a Discovery Phase

Identity Management Product Selection



- Identity Management Selection Criteria
- Architecture Philosophy – Product Suites vs. Point Products
- “Best of Breed” Identity Management Suites

Identity Management Selection Criteria



- Directory Services
- Authentication
- Access Management
- User Provisioning
- Password Management
- Delegated Administration
- Virtual Directory
- Meta-Directory
- Enterprise Single Sign On (SSO)
- Audit

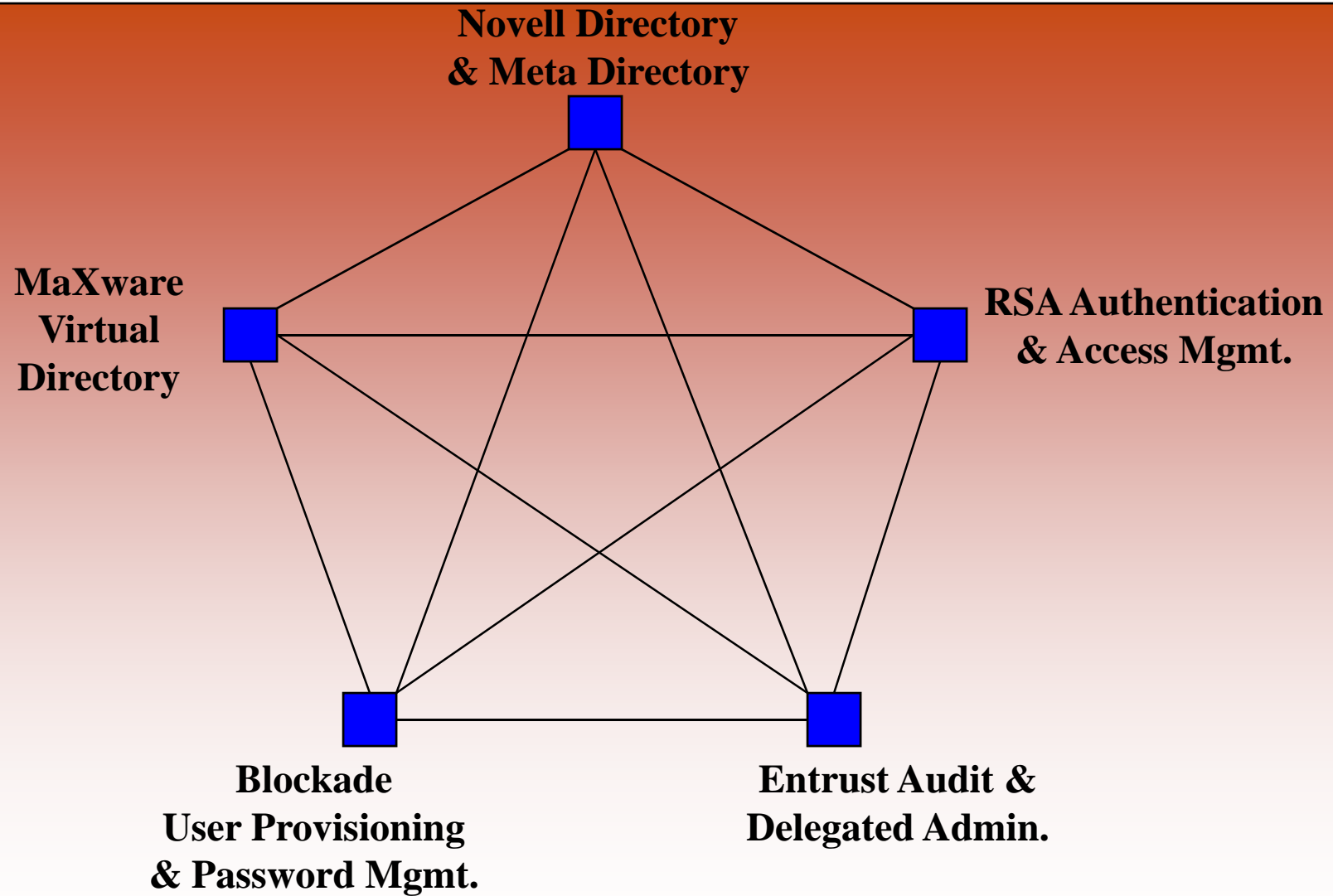
DRAFT

Identity Management Suites vs. Point Products



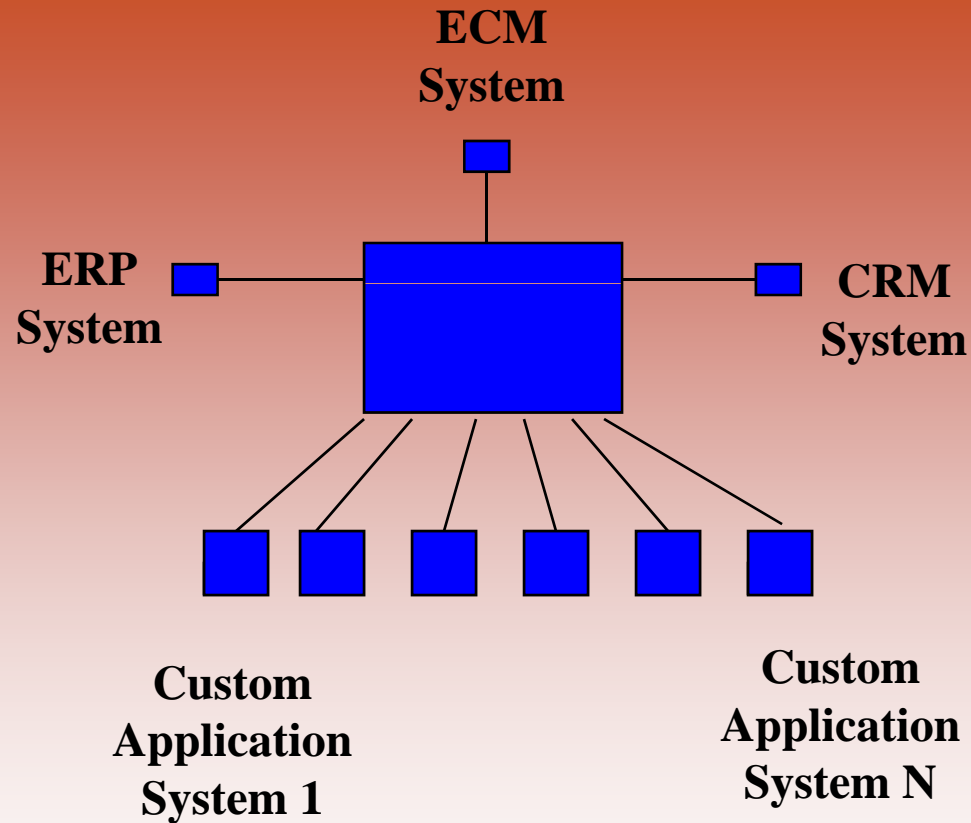
- How much Integration do you want to sign up for?
- Integration is not just a one-time event, it is perpetual!
- Integration points must be managed during engineering, break/fix, upgrades and expansion (in other words, forever)
- The more integration, the less IT Productivity

Point Products Example



DRAFT

Identity Management Environment Integration



DRAFT

“Best of Breed” Identity Management Suites



- Oracle
- IBM
- CA
- Sun
- BMC
- HP
- Microsoft

DRAFT

Identity Management Implementation Strategy



- EDD/DTS Selected Oracle for Individual Identity Management
- EDD will retain IBM for Business Identity Management
- FI\$CAL will determine State EE Identity Management
- Active membership on Statewide SOA Governance where Identity Management is primary focus
- DOL Grant of \$600,000 for Identity Management Pilot
- Identity Management is Incorporated into all EDD RFP's
- Identity Management “bake-off”

DRAFT

Implementation Strategy

DOL Grant



1. Enterprise Identity Management System
2. Web Applications Access Management: Authentication, Authorization, & SSO
3. SOA Web Services Authentication Services
4. CardSpace Identity Solution for Web Sites
5. Enterprise Identity Federation System for Claimants
6. Virtual LDAP Directory System

Strategy

Incorporating into EDD RFP's



- UI Modernization RFP
 - Call Center Network, Platform & Application Upgrade (CalNet II) – Individual access to personal data using IVR
 - Continued Claims Redesign – Individual access to personal data using Internet
- Tax Automated Collection Enhancement System (ACES) RFP – Business access to personal data using Internet
- DI Automation RFP – Medical Provider access to Health data using Internet



The State of California

CIO Academy
Identity Access Management
Panel Discussion

February 27, 2008

Denise Blair
Moderator

Panel Members



- Russell Jones
 - Principal/Enterprise Risk Services Deloitte
- John Bennett
 - Security Specialist Oracle
- Steven Greenspan
 - Director of Eng. & Ops. IdM Northrop
Grumman
- Dale Jablonsky
 - Chief Information Officer EDD

Questions



denise.blair@dmh.ca.gov

DRAFT