

# Authentication and Citizenry Access

## Keeping the Keys to the Kingdom Safe

**November 28, 2007**

**Dave Pickens**  
**Sun Microsystems, Inc.**



# Authentication and Citizenry Access

## Keeping the Keys to the Kingdom Safe

**Dave Pickens, Principal Engineer  
Chief Architect - US  
State/Local Gov't, Education and Healthcare (GEH)  
Sun Microsystems, Inc.**

**SHIFT—OUR UNIVERSE. OUR WORLD. YOUR MOVE.**



# Ground Rules

- Cell phones on s-t-u-n
- Interruptions to a minimum
- Active Participation
- Questions

# Purpose

- This is a high-level presentation
- Some fundamentals of IdM overall
- Primarily focuses on Authentication
- Provides information about latest issues and techniques

Government is  
All About Participation

Participation Requires  
Trust

And Trust Requires  
Identity

# Presenter

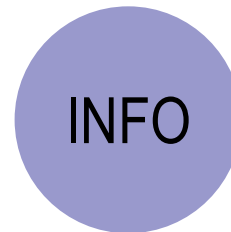
## **Dave Pickens**

Principal Engineer currently serving as the Chief Architect for US Government, Education and Healthcare group at Sun Microsystems. Prior to joining Sun, he worked for Deloitte & Touche. Today he specializes in Identity Management (IdM), Electronic Messaging and Architecture / Methodologies.

# AGENDA

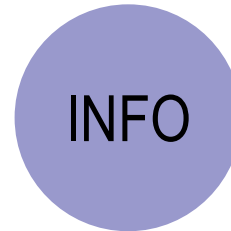
- Parts of the Whole
- It's What not Who
- Some Things
- Hot Issues
- Recap

# Components



**Directory**  
- People

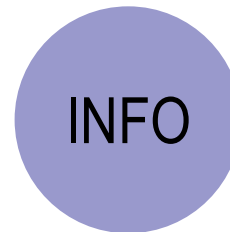
# Components



## Directory

- People
- *Devices*
- *Resources*
- *Services*

# Components

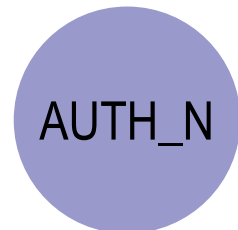


## Directory

- People
- Devices
- Resources
- Services

## Authentication

- Password



# Components



INFO

## Directory

- People
- Devices
- Resources
- Services

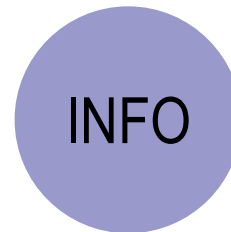


AUTH\_N

## Authentication

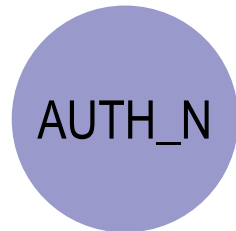
- Password
- *Token*
- *Biometrics*
- *Certificates*
- *Digital Certificates*

# Components



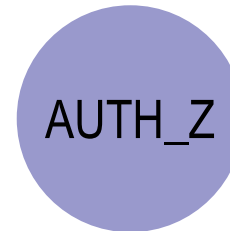
## Directory

- People
- Devices
- Resources
- Services



## Authentication

- Password
- Token
- Biometrics
- Certificates
- Digital Certificates



## Authorization

- Policy Mgmt

# Components



INFO

## Directory

- People
- Devices
- Resources
- Services



AUTH\_N

## Authentication

- Password
- Token
- Biometrics
- Certificates
- Digital Certificates

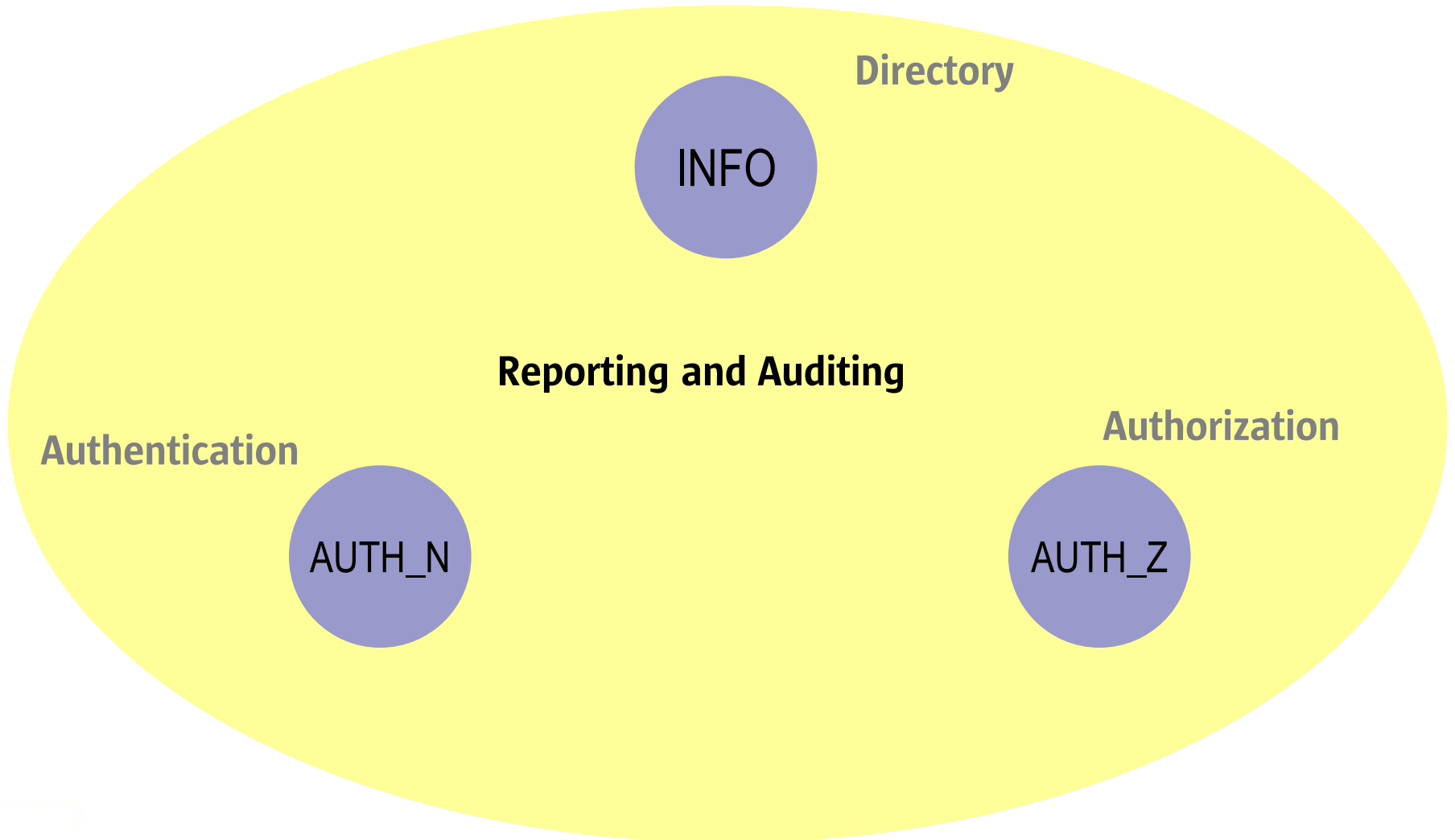


AUTH\_Z

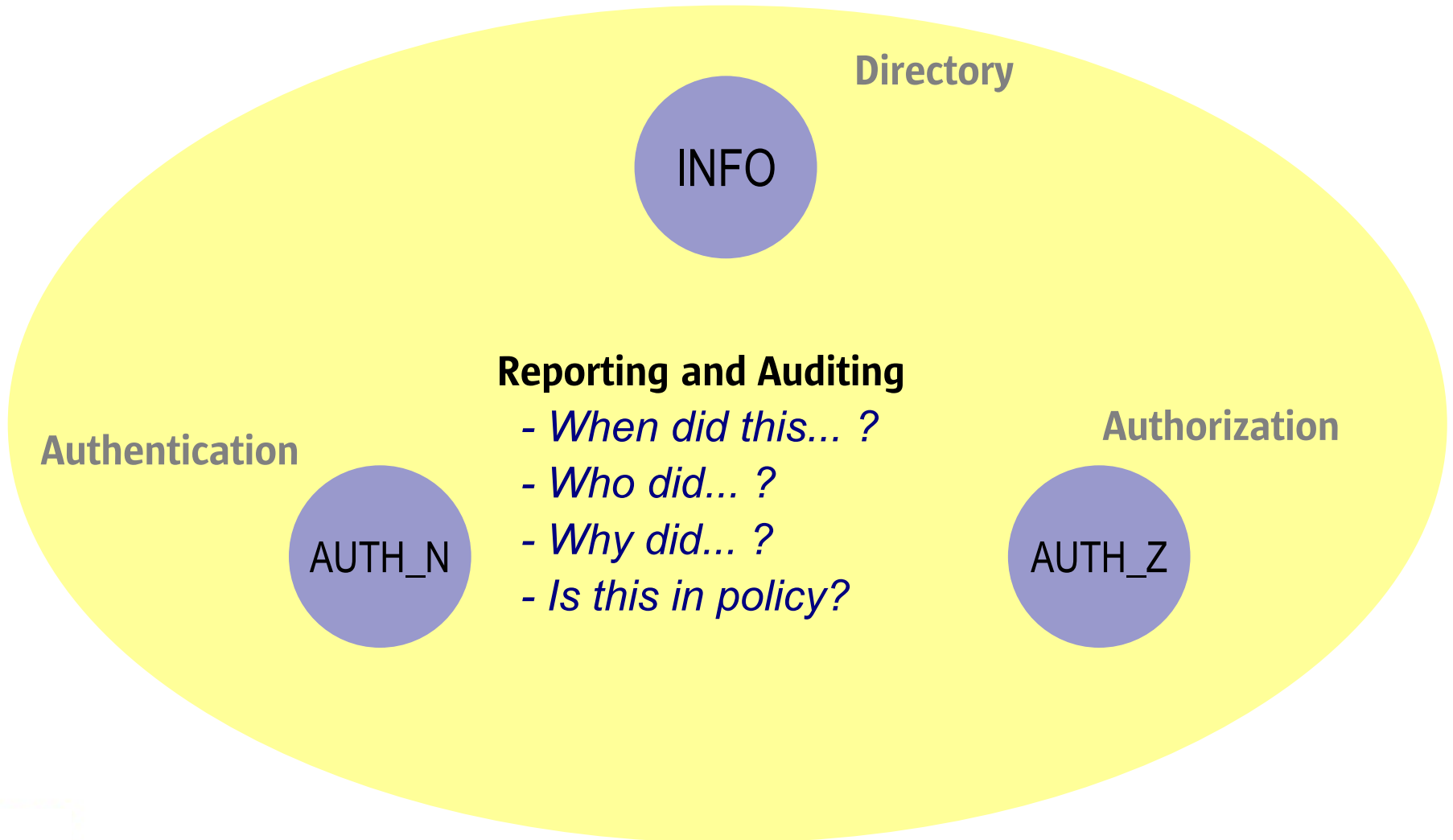
## Authorization

- Policy Mgmt
- *Date/Time*
- *Who you are...*
- *What you do...*
- *Where you are...*

# Components



# Components



Even Though Focus  
Is **Authentication**

You **Cannot** Ignore  
Directory, Authorization  
or Reporting

# What is Authentication?

- It's something you know...
  - > password
  - > process
- It's something you have...
  - > smart card
  - > token card
- It's something you are...
  - > fingerprint
  - > signature

# The thing about Authentication...

- Each method has advantages
- Each method has drawbacks
- You don't want to make it too difficult
- You don't want to make it too easy
- One type does not fit every situation

You Need More than  
**ONE**

Needs to match the asset  
**VALUE**

# Relative Costs of Each Method...

- Passwords
- Smart Card
- Token Card
- Biometrics

# Not all Citizens are Equal...

- Some are more **equal** than others
- City / County / State Employee
- Contractor / Developer
- Business Owner
- Joe “tax payer” Citizen
- Jane “of the neighboring county” Citizen
- The Fourth Estate (aka the press)

It's not **WHO** you are

It's **WHAT** you have  
access to

# Some things around Authentication...

- Self Service
- Account Claiming
- Password Recovery / Reset
- Update Info
- Delegated Administration

# Self Service

- Drives costs down
- Provides most up-to-date info
- Needs to incorporate feedback / notify loop
- It's the de facto internet experience
- Large catch all for many things...
  - > Account Claiming
  - > Password Reset
  - > Update One's Own Data

# Account Claiming

- How do you setup thousands of accounts?
- Dangling account issue
- Identifier issues
- Process driven **not** {blah} driven
- Look to best internet sites as examples
- Will likely not be able to completely avoid “in person” verification

# Password Recover / Reset

- Difference Between Recovery and Reset
- Can Do Modified Account Claiming Process
- Can Use Alternate Password Method
- Can Force 2 Factor Authentication
- Need to Build Feedback Loop Into Process

# Updating Info

- Some Information Needs to be More Current
- Official vs. Unofficial Data
- Main Issues is **WHAT** can be Updated
- Reduces Paperwork Burden
- Speeds Process Up Overall
- Need to Build Feedback Loop Into Process

# Delegated Administration

- Centralized System Creates Own Issues
- Services / Assets Need to be Controlled by Owners
- Delegated Admin Solves the Issue
- Owner Establishes Policy and Process for Access
- Access, Authentication and Directory Centralized

# Hot Issues Affecting Authentication...

- Levels of Assurance (LoA)
- 2 Factor Authentication
- Real ID Initiative

# Levels of Assurance (LoA) – Part 1

- Governmental Interest
- Audit Trail and More
- Not 100% Defined (yet)
- Huge Impact Potential

## Levels of Assurance (LoA) – Part 2

- Level 0 = Never seen the guy, he created his own account through self-service
- Level 1 = Verified through other non-special DB (eg. CC)
- Level 2 = Verified in person using Federally accepted ID
- Level 8 = Verified in person, background check completed and ok

## 2 Factor Authentication– Part 1

- Recently **Hot** Issue Due to Banking Requirements
- Ideally / Originally 2 Factor Meant **2 Different** Types
- Means Something Different Today
- Still Recent Enough Not to be Proven (yet)

## 2 Factor Authentication– Part 2

- It's All “Something You Know”
- Cost for Token / Smart Cards Too High Still
- Still Have Login / Password
- Plus Now Have Random Question of 5

## 2 Factor Authentication– Part 3

- Favorite Color... **ORANGE**
- Favorite Fruit... **ORANGE**
- Cell Phone Provider... **ORANGE**
- ...
- ...

# Real ID Initiative— Part 1

- Department of Homeland Security
- Primarily Focused on Standards
- What Databases **HAVE** to Integrate with Each Other
- What Information (and Format) Has to Be Shared

## Real ID Initiative– Part 2

- DHS working with Arizona
- Lots of push back and discussion
- 20+ States Pass / Consider anti-REAL ID Legislation
- Looked at as a Mixed Bag

# Top 3 or 4 Things

- Plan for Multiple Factor and Types
- Need Authentication Architecture
- Cost / Secureness Should Match Value
- Don't Skip Reporting and Auditing

# Recap

- Given some fundamental IdM information
- Updated you on Authentication related items
- Provided insight into REAL ID, 2 Factor and Levels of Assurance

Government is  
All About Participation

Participation Requires  
Trust

And Trust Requires  
Identity

# Thank You

# Reminders

- Please fill out the evaluations
- Turn evaluations in at Registration Desk
- Presentations will be posted online

## Contact Info:

- email [dave.pickens@sun.com](mailto:dave.pickens@sun.com)
- phone 317-331-4901

# Authentication and Citizenry Access

Keeping the Keys to the Kingdom Safe

Dave Pickens  
dave.pickens@sun.com

**SHIFT**—OUR UNIVERSE. OUR WORLD. YOUR MOVE.

