

---

# **Identity Management: A Financial Services Deployment Story**

**Shawn Ellis**

**Raymond James Financial**

---

# Contents

- **Developing and communicating a vision**
- **What to do in the meantime, the tiered approach**
- **Business case for provisioning**
- **Choosing a product**
- **First attempt: Why did it fail?**
- **Recovery**
- **Second attempt: Why was it successful?**
- **What's next for provisioning at Raymond James?**

# Identity and Access Management

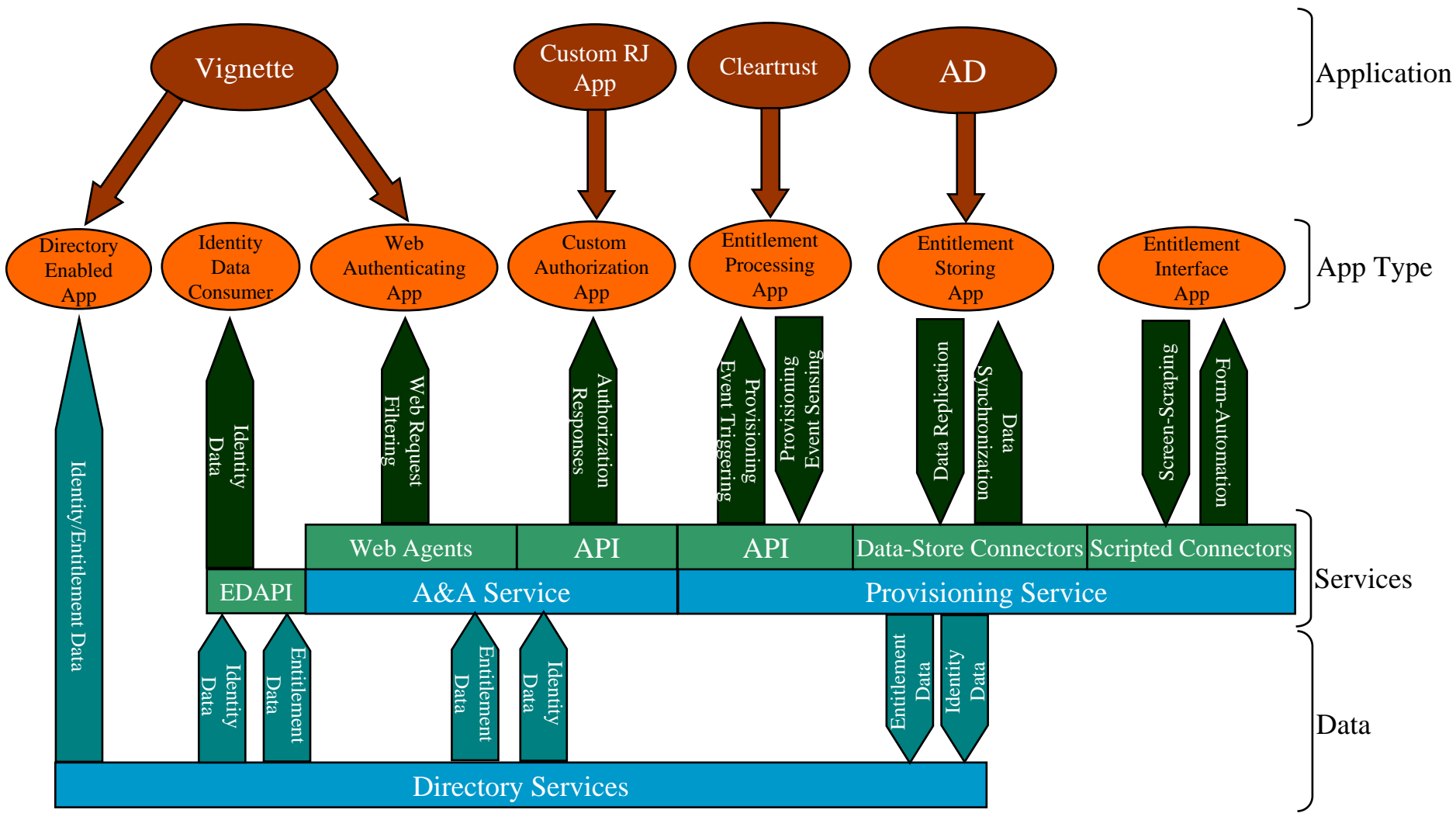
***“the management of information required to identify who a particular user is and to determine what enterprise resources they can access”.***

The services defined within Raymond James to support this process are:

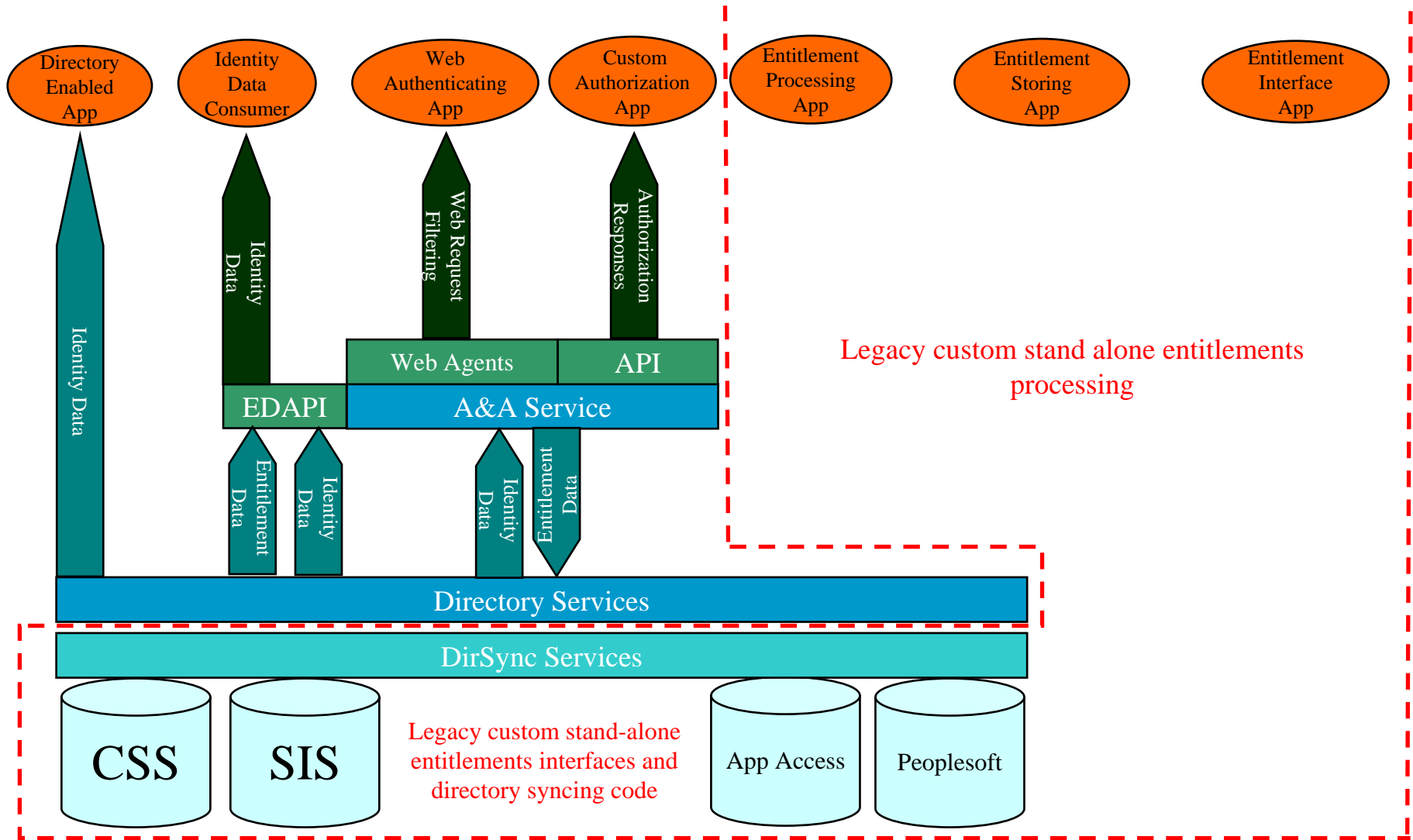
- **Directory Services** – services providing storage and retrieval of identity and entitlement data
- **Authentication Services** – services that confirms a user’s identity
- **Authorization Services** – services that confirm a user’s entitlement to access enterprise resources
- **Provisioning Services** – providing automation of all the steps required to manage (setup, amend and revoke) user or system access and entitlements to electronic services

The Identity and Access Management architecture describes the organization and interaction of the above services.

# I+AM Architecture – Ideal State

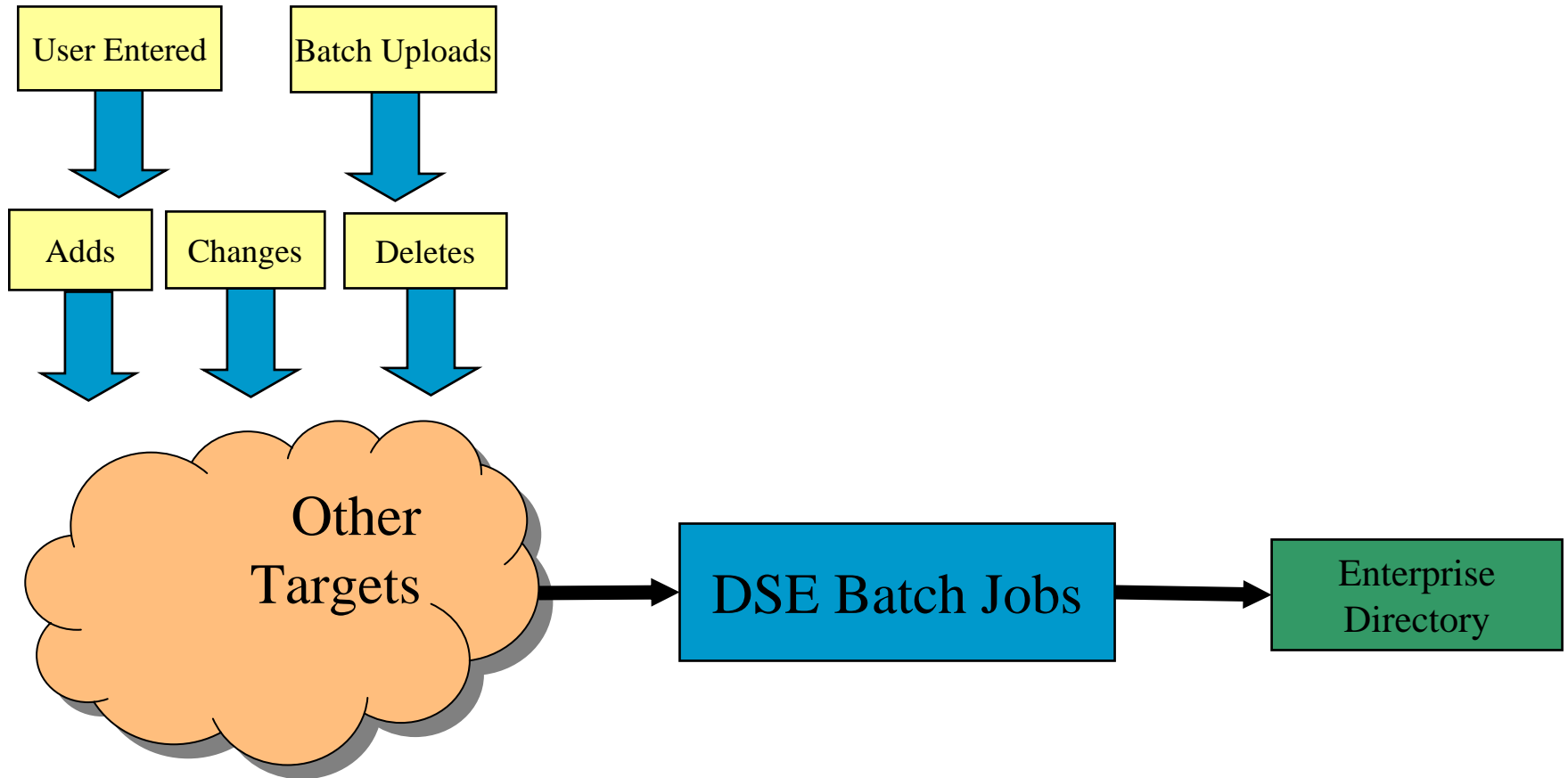


# I+AM Architecture – Current State



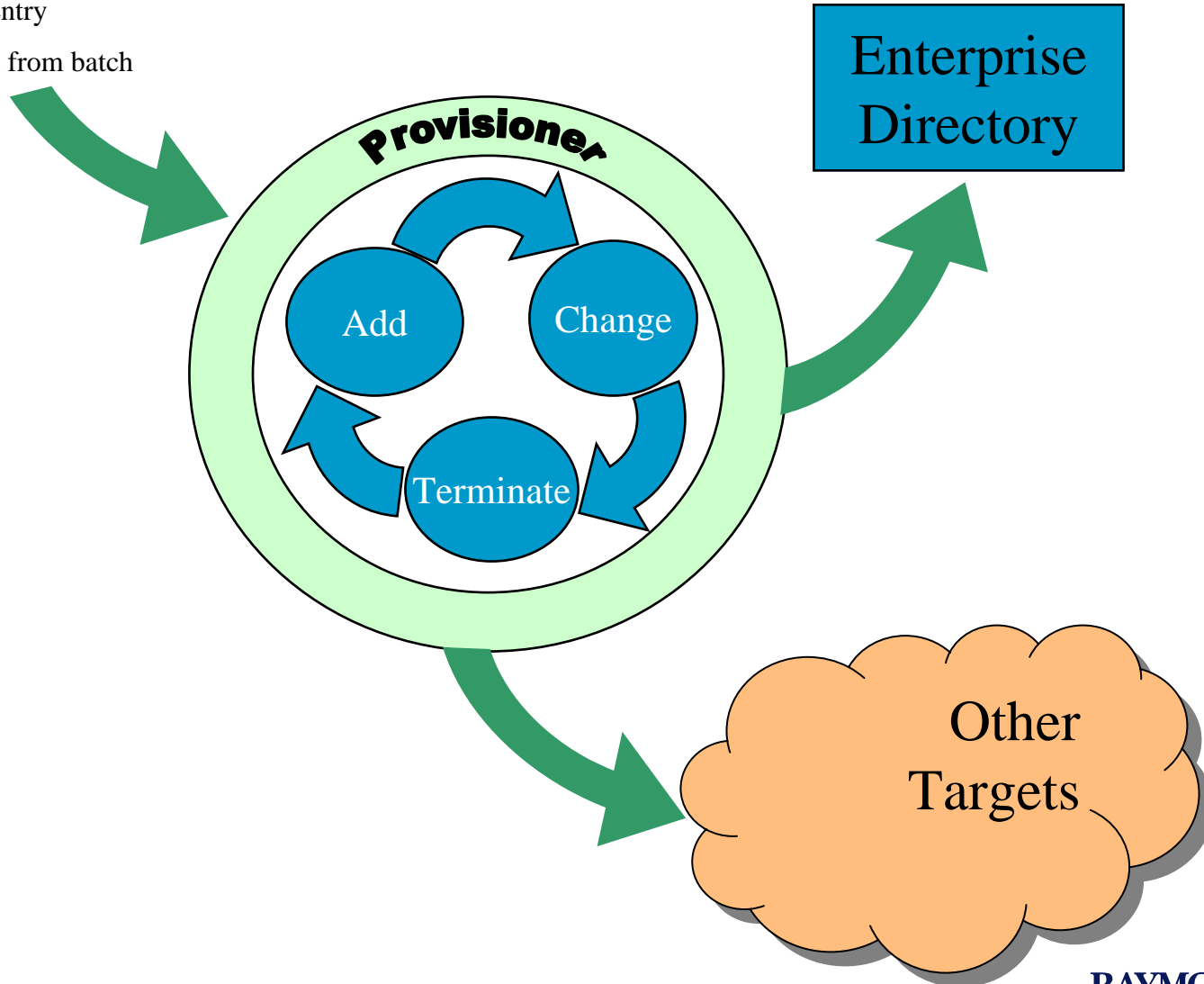
Areas of Opportunity

# Previous State Provisioning Architecture

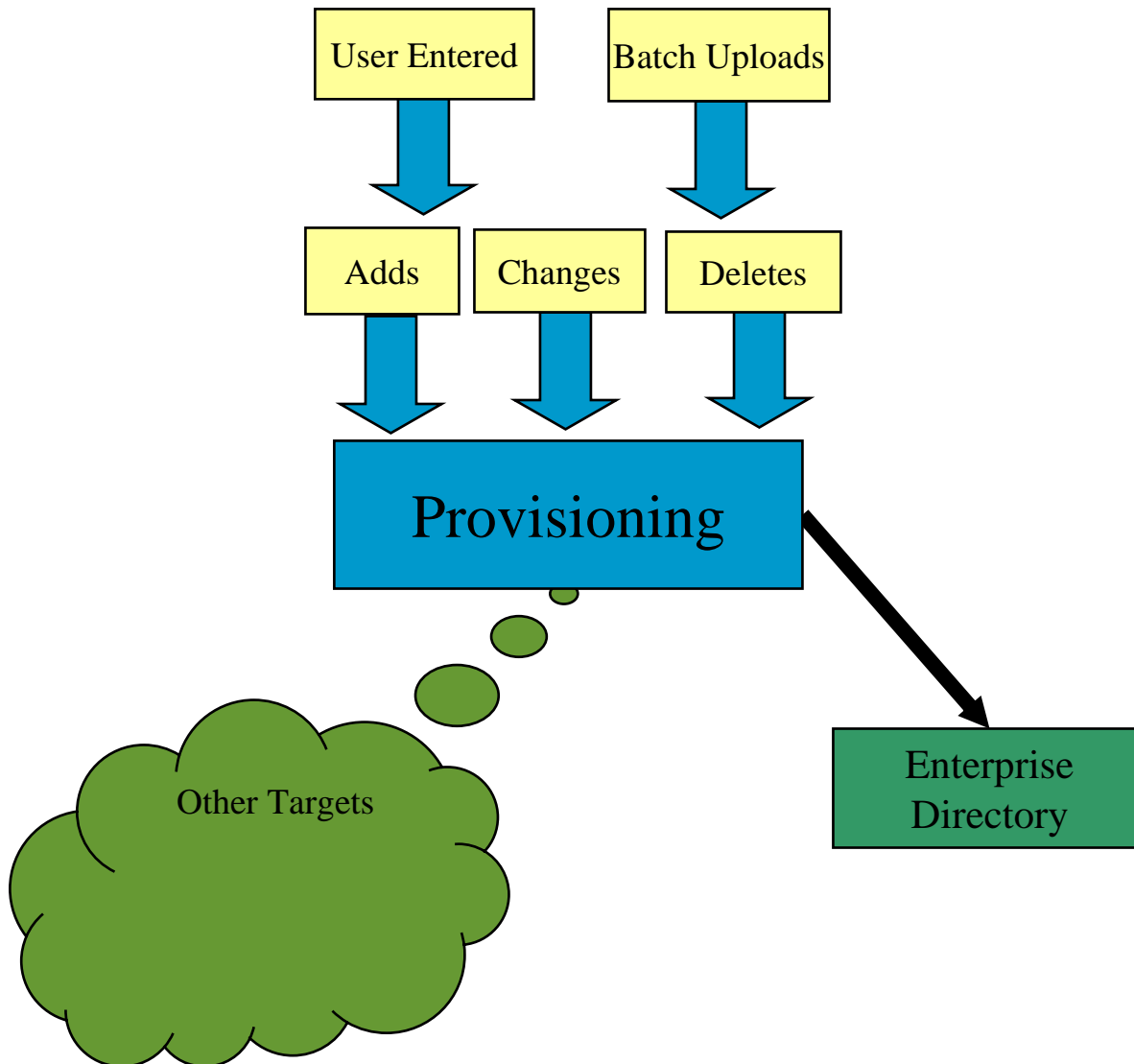


# Current State Provisioning Architecture

- User Entry
- Import from batch



# Current State Provisioning Architecture



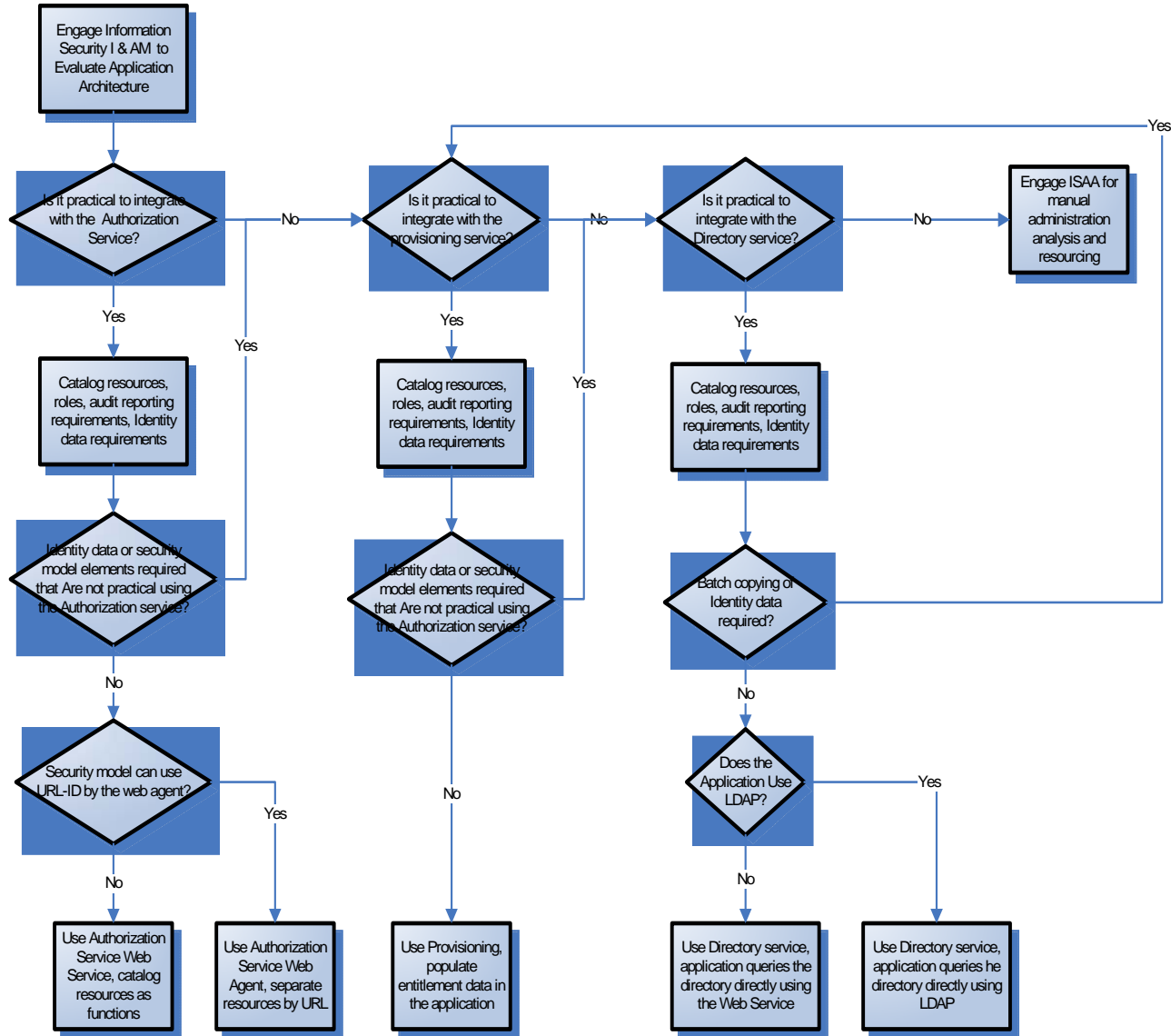
# Tiered Provisioning Approach

Real-Time Provisioning

Batch Processing

Manual Administration

# Identity and Access Management Architecture Decision Tree



# I+AM – The need for a Strategy

The need to pursue a coherent I+AM strategy arises from changes in the systems environment including:

- A large number of diverse applications requiring I+AM functionality
- Increased regulatory and audit controls
- An increasingly dynamic user base

These changes bring with them a number of obstacles:

- **Complex Provisioning** - causing delays and reduced user productivity
- **Data Inconsistency** - in user information across multiple sources
- **Complex Reporting** - of user access privileges
- **Duplicated Development Work** as identity management solutions are built into each application
- **Increased Support and Maintenance Costs** related to the management of entitlements in individual applications
- **Decreased Usability** of application suites with the need for multiple passwords
- **Increased Risk of Mismanagement** – increased exposure to improper manipulation of entitlements

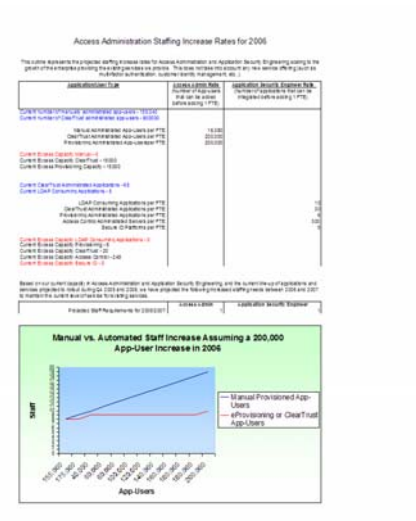
# I+AM – The need for a Strategy

The obstacles outlined above can be addressed through the pursuit of an Identity Management strategy and its delivery of the following:

- **Improved Availability** – Centralized I+AM services support improved availability given a reduction in the points of failure
- **Reduced Development Costs and improved time to market** – the use of a central framework and common services reduces the need for Identity Management to be built into each application.
- **Improved user experience** – by pursuing a consistent approach to entitlements and authentication the user benefits via reduced sign-on and improved turnaround of access requests
- **Standardized Approach to application security** – through the use of common services we are able to standardize the security implemented in each application ensuring a base level of security
- **Improved Security** – ability to de-provision automatically, assurance of the principle of least privilege, consistent standards implemented and easier review of access privileges
- **Improved Control** – this strategy advocates centralized storage and processing of entitlements and authorization. The delivery of this provides greater control of our user and entitlement data. Savings estimated at \$350/user/year.(Giga Report, Giga Information Group, Oct 2002)
- **Increased Productivity** – provided by a more efficient provisioning process allowing resources to undertake their jobs sooner
- **Reduced Provisioning Costs** – replacement of manual with automated processes allowing reduced costs or reallocation of resources to value added tasks
- **Improved Scalability** – a greater ability to process additional users e.g. following an acquisition

# Business Case (Why do Provisioning)

- Risk
- Compliance
- Cost Avoidance (Scalability)



- Cost Savings (Engineering and Business Productivity)

---

# Provisioning Services

## ■ What is it?

User provisioning is the process of managing user identities enterprise-wide. It extends from the definition of the different types of users in the organization through the creation, update and deletion of accounts to the assignment of the appropriate levels of access to enterprise resources for each group. The provisioning service is an automated, data-driven process that quickly and efficiently manages user entitlements through the implementation of a common process.

## ■ What does it cover?

The provisioning service will process all changes to user entitlements. The Provisioning service has the capability to provide the central point for creating, updating and deleting identity data that is interpreted to give the ability for individual user-groups to access enterprise resources.

The Provisioning Service also provides the opportunity for 'self-service' provisioning. Individuals are able to request access to resources or changes to identity data and have that request automatically processed subject to the governing business logic and a pre-defined approval process.

## ■ How is it used?

The provisioning service can be used in several different ways to automate the process of entitling users to resources. It supports an extensive set of data adapters to replicate entitlement or identity data to a target resource if the target resource must evaluate its own access criteria based on this data; The service exposes an API that will allow developers of applications to interact with provisioning events; The service also implements a workflow engine that can incorporate manual tasks into the provisioning process.

The service also exposes an extensive set of auditing capabilities to log the who, what and when of any change. These capabilities will be used to produce audit reports on when and why access is granted to resources.

# Provisioning Services

## ■ Why Use It?

### – **Cost Reduction**

- The implementation of a Provisioning service provides automation of access administration processes reducing processing costs

### – **Cost Avoidance**

- Audit reporting of entitlements does not require duplication across each individual application.
- Reduced hiring based on the economies of scale of a centralized service

### – **Improved Security**

- Automated provisioning and de-provisioning ensures timely intervention in the allocation or removal of entitlements
- Implementation of a consistent process for administering access rights and a consistent level of provisioning across resources

### – **Increased Productivity**

- The Provisioning service will ensure timely creation of entitlements ensuring that long periods of time without access to required applications are not experienced

### – **Improved Flexibility**

- The implementation of such an architecture supports flexibility in movement between roles, the introduction of new applications, the take on of a new user base, etc.

### – **Real Time Entitlements Data**

- The Provisioning Service provides more reliable, real-time replication of entitlements data

### – **Improved Reporting**

- The provisioning services provides a capability to efficiently report on entitlements and provisioning rules

### – **Managed Service**

- The provisioning service is a managed service providing its users with assurances of accuracy, availability and support of provisioning processing

---

# First Product Choice

- **Chose a “Enterprise Class” product.**
  - Complex Architecture
  - Multiple dependencies
  - Complex configuration effort
  - Feature rich
  - “Out of the box” connectors

# Why Did the First Attempt Fail?

## ■ Integration Effort

- “Out of the box” connector difficulties
- Too much customization to the connectors
- Didn’t accommodate existing identity stores well
- Bulk “reverse-synch” puts environments at risk

## ■ Environment Build Effort

- Complex architecture difficult to build environments

## ■ Scalability

- Not really “enterprise class” in throughput of identities

## ■ Support Difficulties

- Difficult to support remotely
- Competent resources were rare

## ■ Missing Milestones/Deadlines

# What Did the First Attempt Cost?

## Consultancy:

**\$150,000.00** Technical and requirements gathering consultancy

## License:

**\$100,000.00** License for the first product

## Hardware:

**\$30,000.00** Server hardware

## RJ Resources:

**\$120,640.00** Internal RJ resource hours

## Total Cost:

**\$400,640.00**

- Opportunity costs

# Recovery

## Convincing the enterprise to try again

- History of success with the process doing “tier 2” provisioning
- Minimal investment to try with the second product
- Flexible amortized license investment from the second vendor
- Different approach to the problem
- Leveraging existing investment in requirements

## ■ Cost recovery

- \$20,000.00 License maintenance stopped payment
- \$500,000.00 Compensated license with other products from the same vendor
- \$30,000.00 Negotiated from the consultancy for their portion of responsibility
- Total Cost recovery of \$540,000.00

## ■ Cost amortization

- Broke up new product purchase into three payments matching the phasing of our project with functionality of the product.

# Second attempt: Why was it successful?

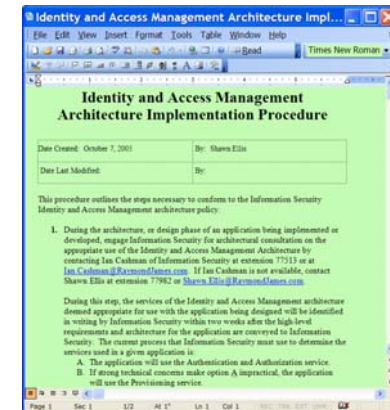
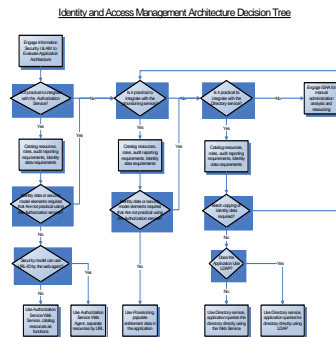
- **Chose a “Enterprise Class” product (pertaining to identity throughput)**
  - Scales to thousands of changes a minute
  - Easily load-balanced
- **Adaptable connectors instead of “out of the box”**
  - More boiler-plate work, less customization
- **Simple architecture**
  - Easy to build environments
  - Easy to keep running
- **Support**
- **Minimal impact to existing identity stores**
  - Starts provisioning identities after it gets turned on, no “initial synch” to put existing identity stores at risk

# Integration Getting IT to Use This Stuff!

## 1. Quality of Service



## 2. Transparency of Process



---

# What's Next for Raymond James IAM

- Utilizing the Enterprise Directory for statistical role generation and managing roles as identities
- Eliminating upstream batch processes by utilizing the provisioning interfaces.
- Delegating policy administration