



## LSEC Identity, Access and Information Management Conference 2008

# A new and unique approach to IAM Projects

[Jordi.cuesta@evidian.com](mailto:Jordi.cuesta@evidian.com)

## Agenda

- Introduction
- Traditional approach, example
- New approach for IAM projects

## The domains of Identity & Access Management



ACCESS MANAGEMENT

- **Access Management** secures access to the computers and their data, and controls the way the users connect to the applications. It includes strong authentication, password management, auditing and data encryption.



IDENTITY MANAGEMENT

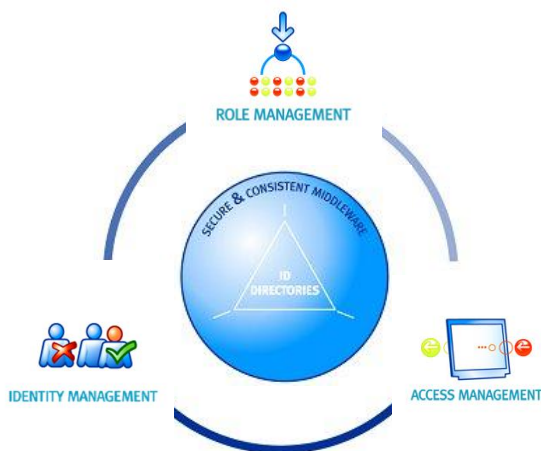
- **Identity Management** focuses on the creation and maintenance of the users digital identities amongst authoritative sources and IT systems.



ROLE MANAGEMENT

- **Role Management** defines and applies security policies to Identity and Access Management, based on high-level business processes. It also provide high-level auditing.

## A solution for IAM Market



## What's an IAM Project about ?



HR define the person profile and to which organization belongs

## What's an IAM Project about ?



HR define the person profile and to which organization belongs

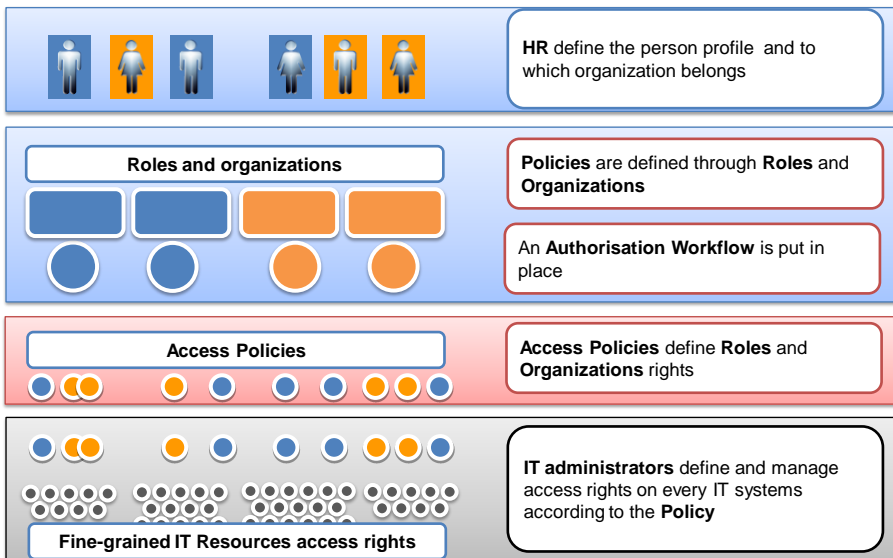
**Roles and organizations**



**Policies** are defined through **Roles and Organizations**

An **Authorisation Workflow** is put in place

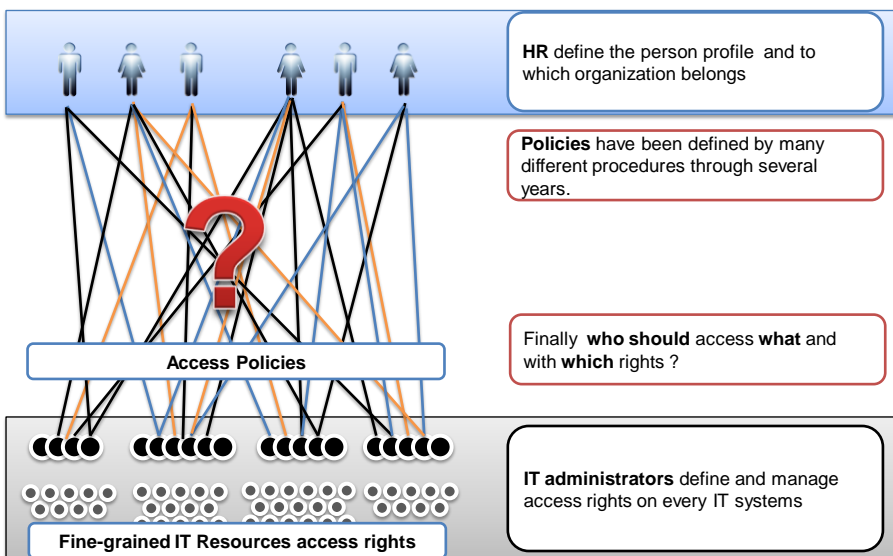
## What's an IAM Project about ?



Page 7 - LSEC Conference, November 2008

**EVIDIAN**  
A Groupe Bull Company

## What's the reality ?



Page 8 - LSEC Conference, November 2008

**EVIDIAN**  
A Groupe Bull Company

## Agenda

- Introduction
- Traditional approach, example
- New approach for IAM projects

Page 9 - LSEC Conference, November 2008

**EVIDIAN**  
A Groupe Bull Company

## The standard IAM project approach

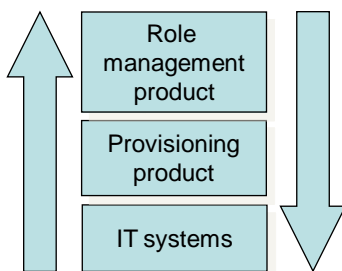
- **The standard IAM approach**
  - Build a central identity repository
  - Maintain identities automatically from business events (H.R.)
  - Centralize knowledge of : "Who can access What?"
  - Offer one single approval workflow for all application accesses
  - Provision automatically when possible
  - Secure user accesses
- **The Major project difficulty : Centralize knowledge**
  - A full information system already exists:
  - X versions of N existing processes,
  - Rights approval history is spread over many media. It's almost impossible to find who granted someone some rights
  - N different policies on account naming makes it hard to identify accounts' owners.

Page 10 - LSEC Conference, November 2008

**EVIDIAN**  
A Groupe Bull Company

## The standard IAM project approach

### ■ The standard Bottom-Up/Top-Down approach



### ■ Implementation scenario

1. Implement account collection for all applications
2. Assign accounts to users
3. Implement workflow processes and define roles

## The standard IAM project approach

### ■ Implementation Difficulties

1. Implement account collection for all applications
  - **800 applications. ~150 really different applications**
    - 25 covered by standard provisioning product
    - 125 agents to develop
  - **1 agent is usually 30 days of development**
  - **Using a flat file instead is 10 days for extraction, cleaning and formatting**
    - 125 applications
      - = 50 agents + 75 flat files
      - = 2,250 person.days = **~11 person.years**



More than **1 M€** for access collection of services with no immediate value

## The standard IAM project approach

### ■ Implementation Difficulties

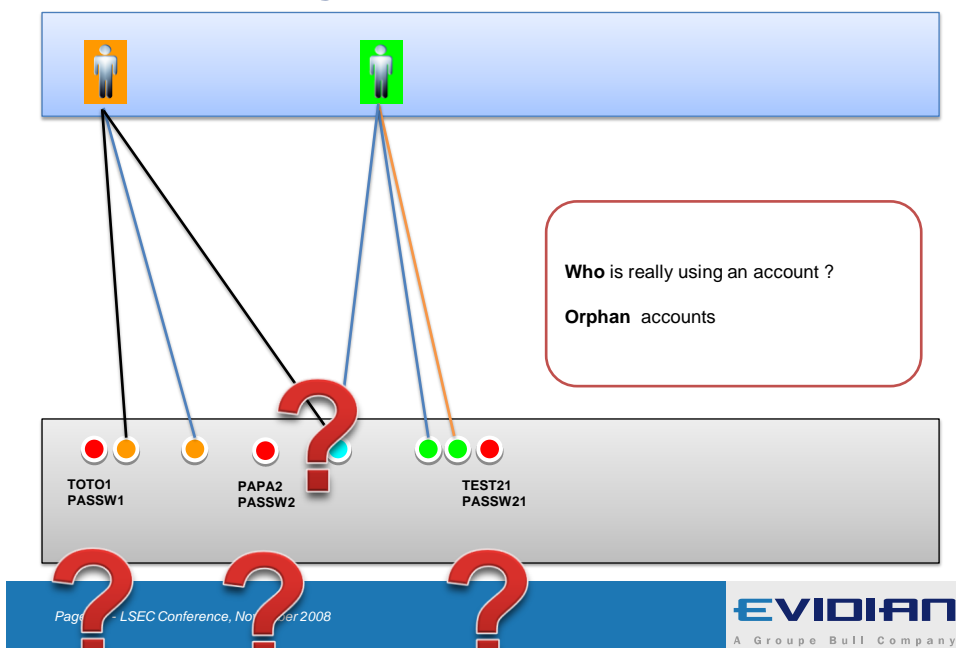
#### 2. Assign accounts to users

- 60,000 users means approximately 600,000 accounts
- Only 30% of the accounts can be matched automatically
  - 420,000 accounts to assign manually
- Assigning one account to one user takes 5 minutes
  - Including orphan/obsolete account detection, homonyms,...

➔ 420,000 **accounts** \* 5 minutes = **1,458 person.days** = ~7 person.years

- ❖ At this point, **18 person.years** will have been spent and we know who is supposed to use each account, but we still don't know:
  - Which accounts are actually used? (account cleaning)
  - Who is *really* using each account? (account stealing/sharing)

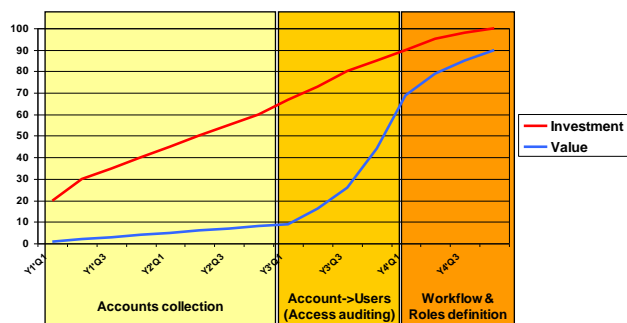
## What have I got ?



## The standard IAM project approach

### Investment plan

Not including licenses and hardware



## Agenda

- Introduction
- Traditional approach, example
- New approach for IAM projects

## New approach for IAM

### Empower People !!!



#### Distribute the work over all your users

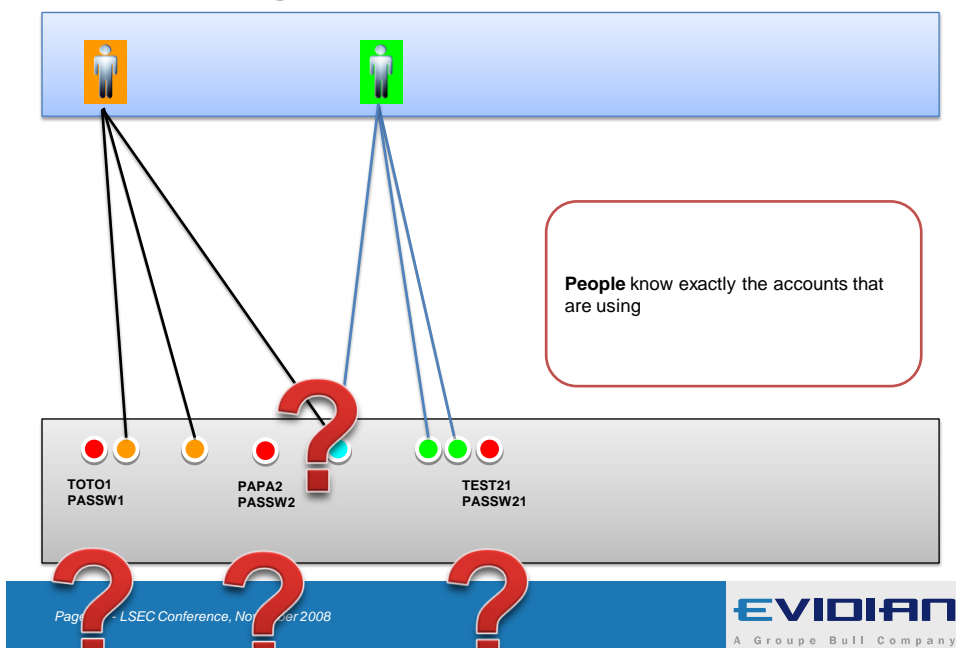
- Users know their account identifiers and passwords
- Their accounts are valid even if the creation rules have changed many times

#### Detect and filter all irregularities at the same time as you collect data

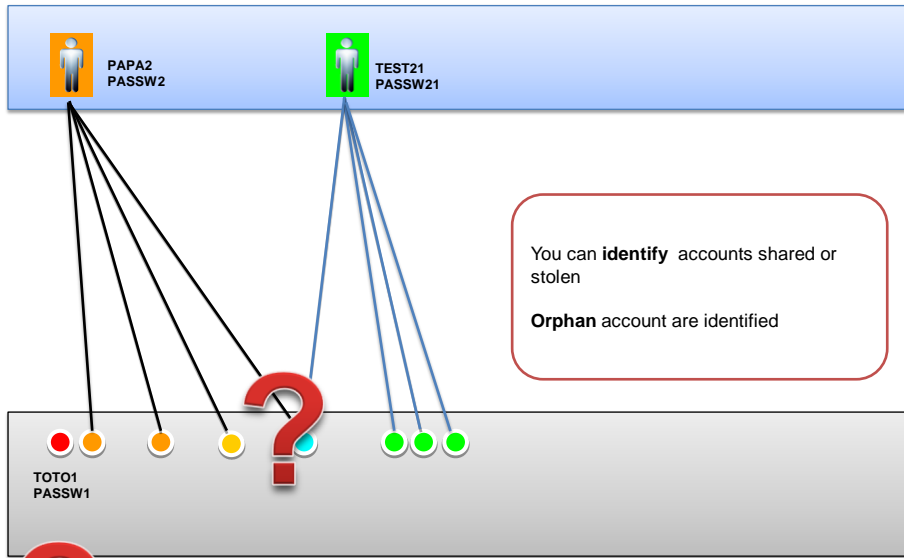
- Users might be using accounts that they're not supposed to (delegated, shared, stolen...)
- Orphan and obsolete accounts are never used

➔ ~99% of the active accounts should be used within a few months

## What do I get, now?



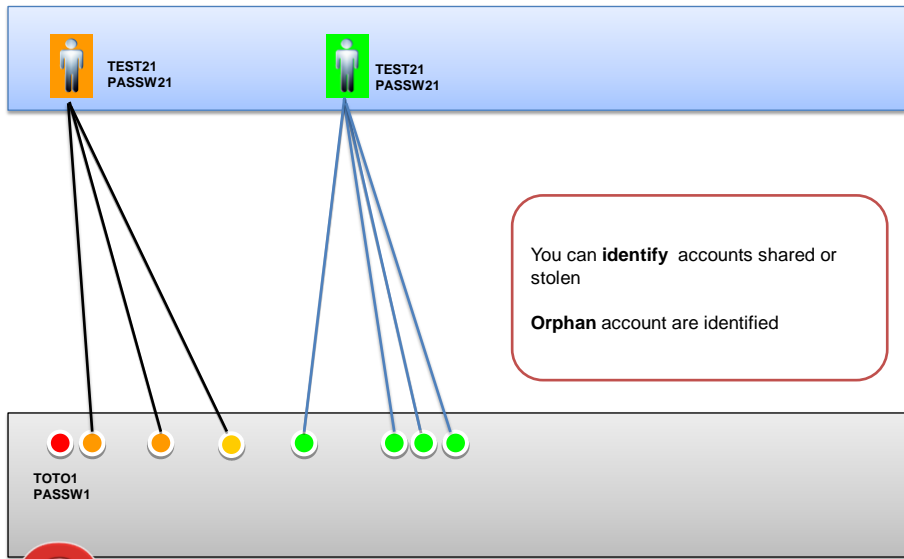
# What do I get, now ?



You can **identify** accounts shared or stolen

**Orphan** account are identified

# What do I get, now ?



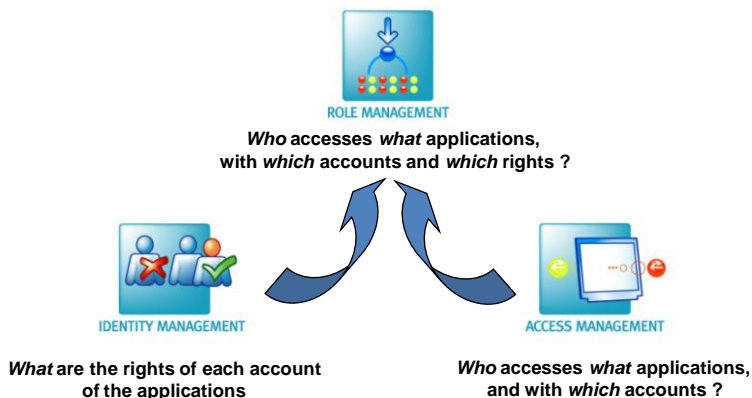
You can **identify** accounts shared or stolen

**Orphan** account are identified

## New approach for IAM



A new bottom-up / top-down approach



Page 21 - LSEC Conference, November 2008

**EVIDIAN**  
A Groupe Bull Company

## New approach for IAM



User-access-driven implementation scenario

- 1. Users self-register their accesses**
- 2. Business processes are implemented**
  - Workflows are designed based on existing processes
  - Provisioning is initially implemented without agents
- 3. Provisioning agents are deployed where needed**

➔ **Steps 2 and 3 could be implemented in parallel**

Page 22 - LSEC Conference, November 2008

**EVIDIAN**  
A Groupe Bull Company

## New approach for IAM



### User accesses self-registration



ACCESS MANAGEMENT

❑ **Access management tool can be used for this purpose:**

- Enterprise single sign-on engine, or
- Self-registration engine

Identifiers are collected transparently when the users access the applications.

Passwords will be checked, as a proof of ownership.

❑ **Major advantages:**

- Less than 1 day per application for configuration ~ **150 person.days**
- Only valid accounts will be collected in 3 to 6 months
- Collect includes the assignment of the account to users
- SSO can be enabled at the same time → **immediate value**

➔ **17 person.years saved for immediate value:**

Reporting of *who* access *what* application with *which* account

SSO increases security while reducing costs

## New approach for IAM



### Business processes implementation



ROLE MANAGEMENT

❑ Approval workflow tool can now be implemented

- The initial state of who can access what is now known
- Processes can be implemented based on existing ones

❑ Provisioning without agent can be deployed

- Traceability of new account creation
- Fluidity of the approval processes

❑ Role management tool can be used to create an access policy

- At this point, we know *who* accesses *what*.
- We can start creating a simplified enterprise role management model  
to sharpen approval workflow policies.

# New approach for IAM



## Pragmatic Provisioning agents deployment



- **Deploy provisioning where it's easy or standard**  
 Do not develop an agent for applications:
  - For which accounts almost never change
  - Used by only a few users
 Use flat files and provisioning without agent instead.
  
- **From access policies to a complete role management**  
 The role management tool can now integrate the rights recovered by the provisioning tool.



*Provisioning deployments often face both business and technical roadblocks*

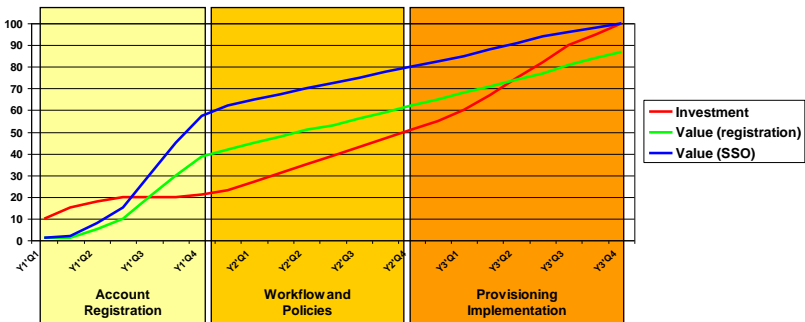
Copyright burton Group

# Evidian's new approach for IAM



## Investment plan

Not including licenses and hardware



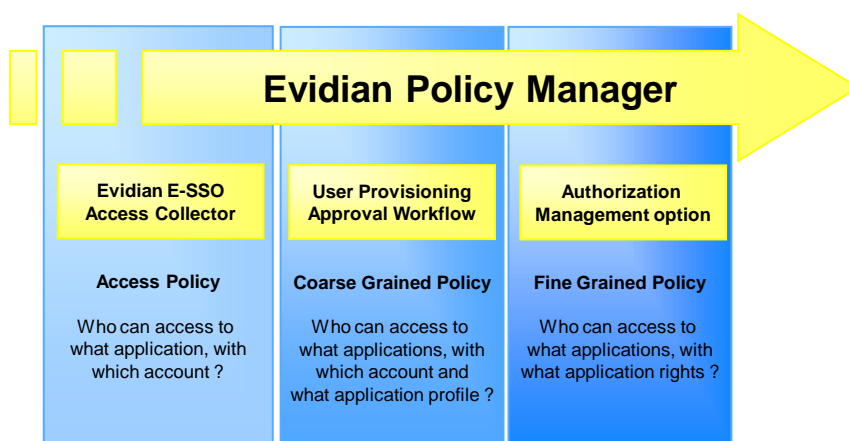
## New approach for IAM



### Major advantages

- **Keep a quick ROI**
- **Every step brings value:**
  - Step 1**
    - > SSO for users and helpdesk
    - > Immediate reporting and auditing of the accesses to the applications
  - Step 2**
    - > Centralized approval workflow
    - > Clear vision of approval responsibilities
  - Step 3**
    - > Reduce administration cost of major applications
    - > Ensure the policy is enforced on the systems

## Evidian's new approach for IAM



***Evidian, a new and unique approach  
to IAM Projects***

***Thank you***

Page 29 - LSEC Conference, November 2008

**EVIDIAN**  
A Groupe Bull Company