

# *Access Management*

## *The Application Security Challenge*

Carol Burt  
President & CEO  
2AB, Inc.  
[cburt@2ab.com](mailto:cburt@2ab.com)



2AB, Inc.



# Access Management

## ⇒ A Simple Business Concept!

- Information needs to be protected from unauthorized disclosure
- Business Services need to be restricted to authorized users
- Business Policy governs who accesses specific classes of information and/or services



2AB, Inc.



# Typical Examples

## ⇒ Healthcare

- HIV Test: Physical Therapists can see nothing (not even the order); Medical Technician can see that it was ordered (but not results)

## ⇒ Online Financials

- 401K Account: Broker can only see accounts for his clients; Client can only see accounts they own;

## ⇒ Telecommunications

- Wireless device: anyone can ring; employees can message; e911 can locate

## ⇒ Equipment Manufacturers

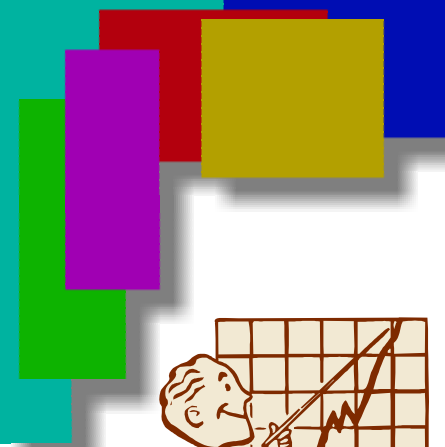
- Orders: Any Dealer representative may view orders; Only dealer buyers may place orders for equipment

## ⇒ Government

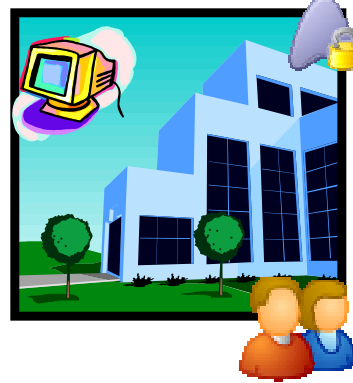
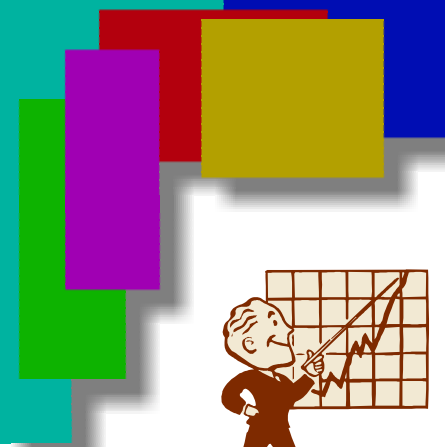
- Documents: Access to sensitive info requires a specific “clearance level”



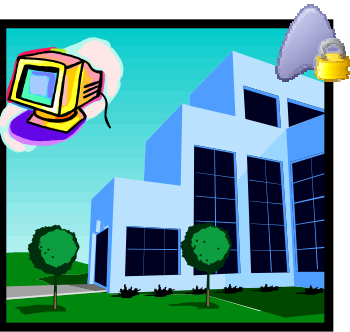
2AB, Inc.



How are resources guarded?



## *Internet Communications*



## Business Partner Connectivity



## Online Consumer Services



## Employee Services



2AB, Inc.

How are resources guarded?



*With the explosion of cyber crime,  
protecting access to the services and the  
information provided on-line is critical!*



The demands of consumers and the requirements of many government regulations make it mandatory that access to business and personal information be protected.



2AB, Inc.



# Access Management Software

## ⇒ A Simple Goal!

- Allow the human who previously “guarded” sensitive information to be removed from the process without loss of access control

## ⇒ A Challenging Task!

- Software that “guards” sensitive information must be deployed as part of business applications
- Concise, comprehensive, and consistent access policy must exist – machines depend upon programmatic logic
- Business applications are distributed!





# Business View

- ➔ Business people identify sensitive information or application features (guarded resources) without concern for the technology that controls the resource
  - Proprietary Business Information
  - Customer Information (e.g. contract terms)
  - Private Personal Information (e.g. medical record, debt)
  - Billable Product Features (e.g. ring, message, call forward no answer, locate)
  - Sensitive Application Features (deny service, credit payment, locate user)
- ➔ Information or services may be accessible from different “applications”.
- ➔ The same “application” may be utilized by many businesses with different access policy requirements.







# Technical View

Delegation of identity and context-based credentials acquisition must be possible across technology platform boundaries!

## ⇒ Web Tier

- Web Pages, JSPs (URLs)
- Servlets
- XML documents (or parts of XML documents)

## ⇒ User Interfaces

- Panels, Buttons, Fields
- Features

## ⇒ Database Services

- Tables, Rows, Fields

## ⇒ J2EE Tier

- Application Servers (EJB's and operations on EJB's)
- Connectors
- Naming

## ⇒ CORBA Tier

- Objects and operations on Objects
- Naming, Trading, Events

## ⇒ Messaging Tier

- JMS, MQ, ...



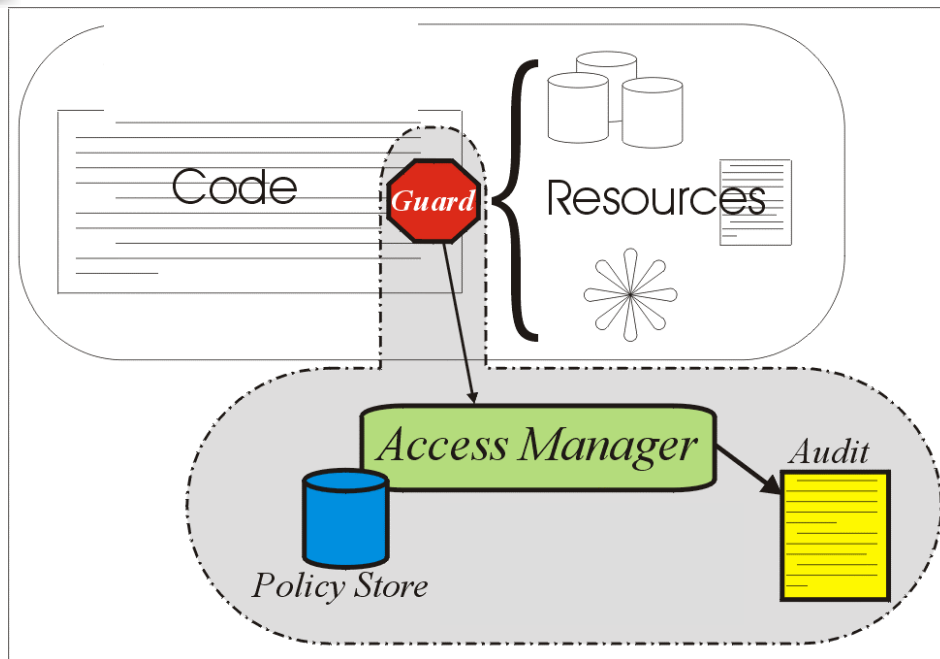


# A Costly Problem Lurks

- ➔ Access Management is being included as “business logic” in every application
  - User repositories (ids & passwords) are being managed for every modernized business application
    - A Provisioning nightmare!
  - Policy is being coded as “business rules” directly into applications
    - When policy changes, the application must be changed, tested, and re-deployed
    - Auditing access policy for legislated conformance requires code reviews!
  - Every purchased product introduces a new access management tool!



# Application Software Guards



➔ Address the business requirements for access control that network and operating system security does not address!

- The need to restrict “who” can perform certain functions that an application provides
- Business responsibilities (legal or ethical) to restrict access to sensitive business or personal information

➔ Driven by Legislation



2AB, Inc.



# Challenges...

- ⇒ Applications span multiple technology environments; in fact, SOA encourages this.
  - Web Services front-end, J2EE middle tier and access back-end business information / services via CORBA/IIOP, JDBC/SQL, JMS/MQ, IMS/CICS, ...
  - How do I know who the user really is?
- ⇒ Business Services and Sensitive information may be exposed via numerous “applications” and/or application functions
- ⇒ Standards in the area of Access Management standards are currently all specific to a particular technology platform





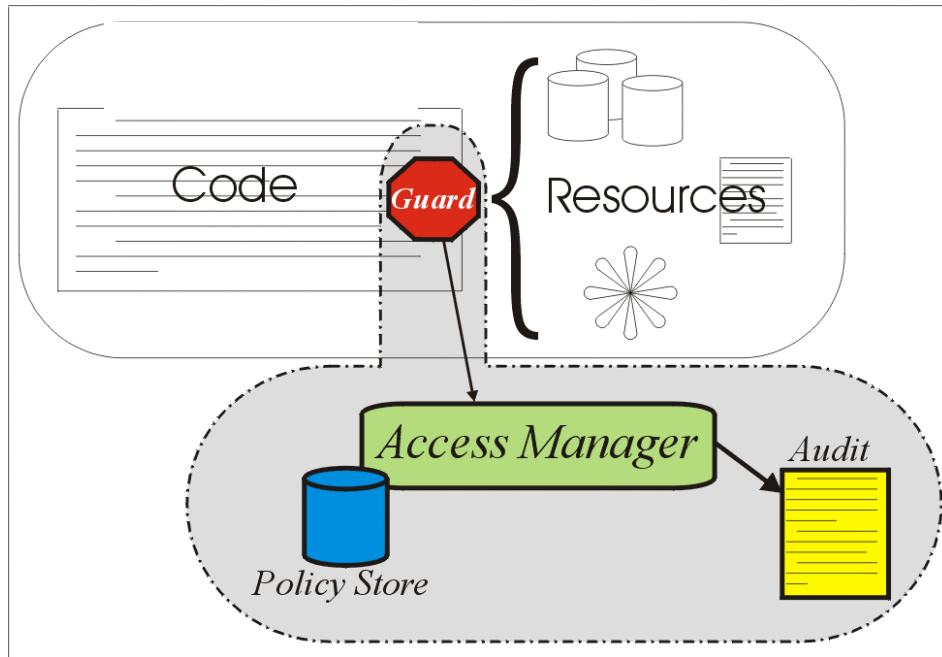
META Group predicted in late 2003:

*“as business begins to put more focus on design for application securability and service-oriented architecture, application-specific security mechanisms will migrate to infrastructure.”*



2AB, Inc.

# Leveraging an Identity and Access Manager

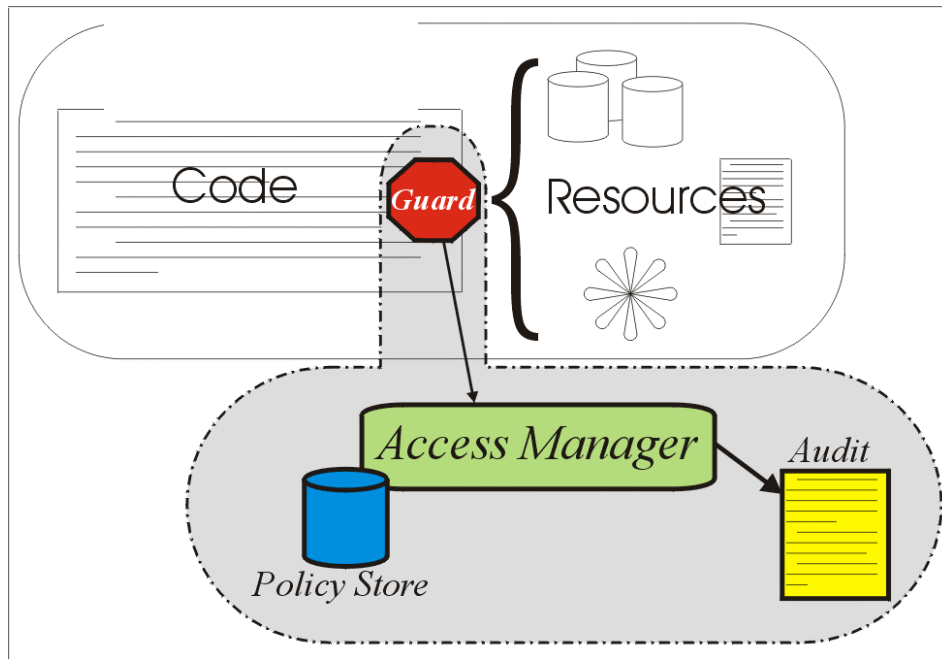


- ➔ Identity Managed independently
- ➔ Access Policy can be independently
  - Modified
  - Tested
  - Deployed
- ➔ Dynamic Policy updates supported
- ➔ Policy shared across business applications



2AB, Inc.

# Architecture supports Systematic Methodology



- ➔ Who is responsible for access policy?
- ➔ What resources need to be protected?
- ➔ What kind of access policy does my application require?
- ➔ How does the access management solution plug in?





# Who is responsible?

- ⇒ Although implemented with technology, it is the business that must assess the risk!
- ⇒ Typically requires a major classification effort
  - Information
  - Application Features
  - People
- ⇒ What must be considered for access policy?
  - Business Policy
  - Legislation
  - Increasingly... Individuals!







# What do you need to protect?

Granularity of Protected Resource	Access Policy that protects salary
Machine and/or network	Only people with the authority to run the HR application have User IDs on the machines where the HR application is installed.
Entire Application	Only people with the authority to view HR information are granted User IDs for the human resources application.
Specific Application Feature (e.g. Screen, Menu, Button, or URL...)	Only people with the authority to view HR information will be allowed to request salary information from the HR application.
Entire Database	Only people with the authority to view HR information have User IDs in the human resources database. The database is accessed using requestors' ID.
Table (in a database)	Only managers can view employee records.
Row (in a table in a database)	Only the employee and people in the chain of management for an employee have the authority to view an employee's record.
Field (in a Row in a table in a database)	Only the employee and people in the chain of management for an employee have the authority to view an employee's salary.
Concept (information that contains multiple fields – potentially from different sources)	Only managers have access to employee's compensation information (compensation information is a classification or concept that includes salary, commission and bonus).



2AB, Inc.

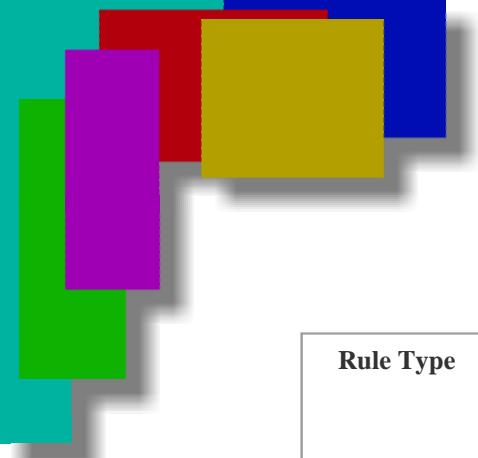
# What kind of Access Policy do you need?

Policy Type	Question answered with regard to protected resource (information or application feature)	Example(s)
Identity-Based	Are you an individual that has been specifically granted access?	User ID / Password, Private Key, Electronic Token, Biometrics
Role-Based	Are you currently in a role that has been specifically granted access?	Manager, Emergency Room Personnel
Group-Based	Are you part of a group that has been specifically granted access?	Accounting, Engineering
Context-Based	Is the context of the request such that access should be granted to this individual?	Time of Day, Location, Emergency, Account Balance
Entitlement-Based	Is this individual entitled to access this class of information?	Clearance Level
Relationship-Based	Is this individual entitled to access the personal/business information because of a relationship with the person or business?	Primary Care Physician, Manager of Employee, Account Representative, Parent
Rule-Based	Does the policy governing access to the resource allow this individual to access the resource?	Combination(s) of above



2AB, Inc.

## Examples of Business Driven Access Policy Types



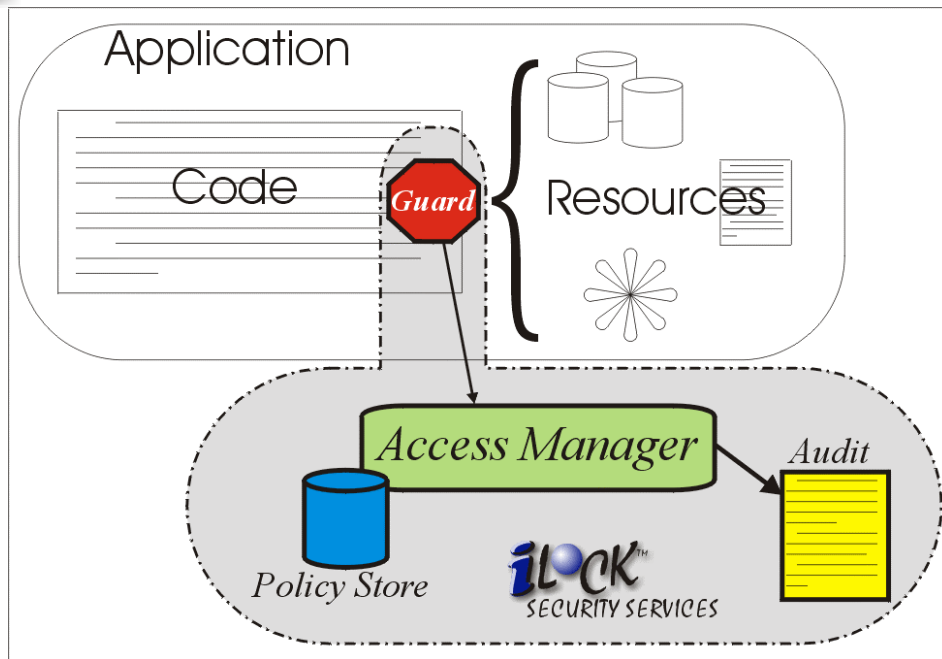
Rule Type	How the rule is evaluated	Example of usage
Nobody	Deny access to everyone.	In a Context-Based Policy, access may be denied during certain times of the day.
Deny	Deny access to anyone that has any of these credentials (access ID, group, role).	A security alert is in place. You may wish to temporarily deny certain groups who normally have access.
Required	Allow access only if the requestor has all the credentials.	Allow only owners who are officers (you must be both an officer and an owner).
Any	Allow access to anyone with any of these credentials.	You wish to allow users who are in the group <i>administrators</i> -or- have the ID <i>mike</i> -or- are in the role <i>accountant</i> .
Anybody	Allow access to anyone.	You may wish to audit the request for the resource even though you do not restrict access.



2AB, Inc.

## Examples of Business Driven Rule Types

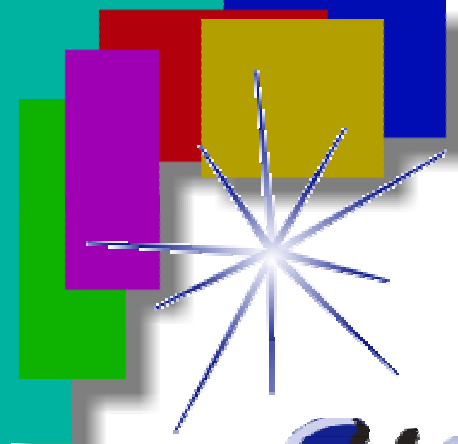
# How does it “plug in”?



- ➔ Look for products that leverages Industry Standards for “plug-in” technology
- ➔ Talk to vendors about how they are working to progress secure interoperability solutions



2AB, Inc.



**iLOCK™**  
SECURITY CENTER

**JAVA**  
AGENT

**orb™**

**CORBA**  
AGENT

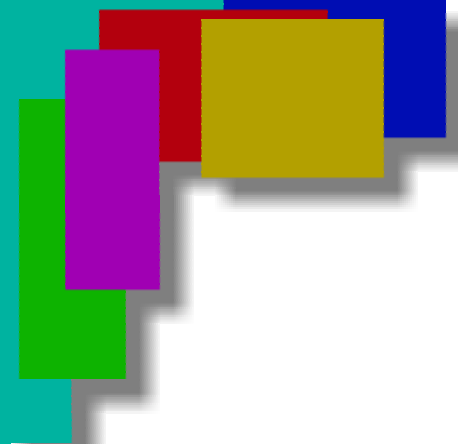
**WEB**  
AGENT

**C**  
AGENT



2AB, Inc.

*Infrastructure for  
Integrated Trusted Solutions*



Carol Burt  
President & CEO  
[cburt@2ab.com](mailto:cburt@2ab.com)

