Automated Identity Management and the Person Lifecycle

Ted Bross, Ed.D.
Associate Director, Administrative Information Services
Office of Information Technology
Princeton University
tbross@princeton.edu

High Level Objectives of the Identity Management Project (we're in the third year of a 15 month project)

- Implement both OAM and OIM from Oracle
- Automate the creation of the university NetIDs
- Automate the provisioning and deprovisioning of user accounts and the services to which those users are entitled (e.g.-Unix, AD, Public Search Directory, "LDAP" etc.) (working at Princeton is like dying and going to heaven-in reality, using our old system, some of our faculty did die and go to heaven but stayed active in our directories).
- Establish self-service user account claiming and password reset processes
- Support Single Sign On (SSO)
- Strengthen application security, starting with the 9.0 version of the PeopleSoft HR and Student systems, by using "bank-like" functionality (second level authentication)

Key Considerations

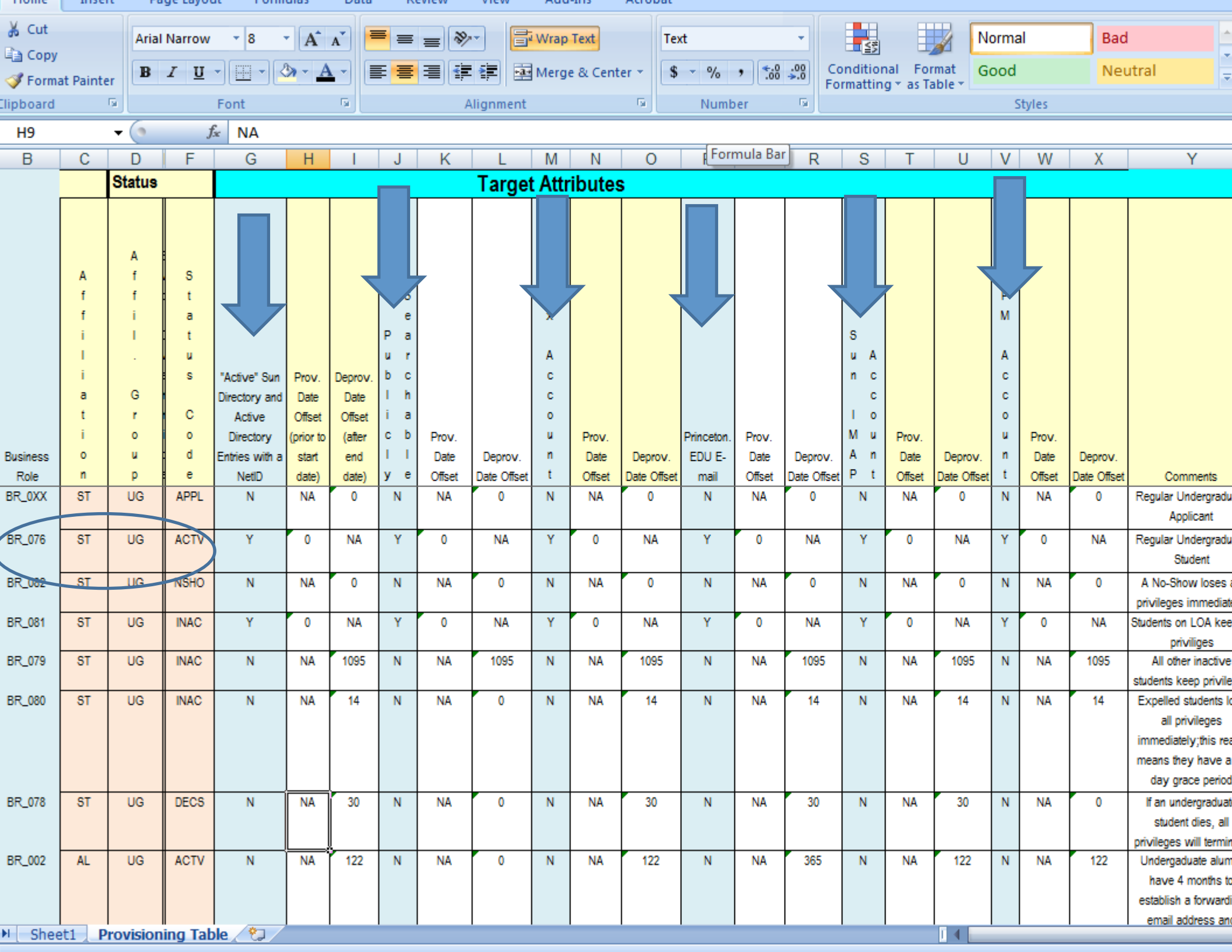
- Each Step in the Life Cycle=New Affiliation and Status
- Affiliation=How You are Related to the University (High Level)
  - Student, Employee, Alumnus, Kin, Miscellaneous
- Affiliation Group=Further Defines the Affiliation
  - Student: Undergraduate, Graduate, Special Student
  - Employee: Faculty, Staff, Casual Hourly
  - Miscellaneous: Departmental Computer User, Docent, Trustee, Corporate Vendor etc.
- Status=Temporal and Relative Relationship
  - Active, Inactive, Deceased, Retired (High Level)
    - On Leave, Voluntary Withdrawal, Suspended (Granular)
    - i.e.-a student on leave is still considered active; a student who is suspended is considered inactive

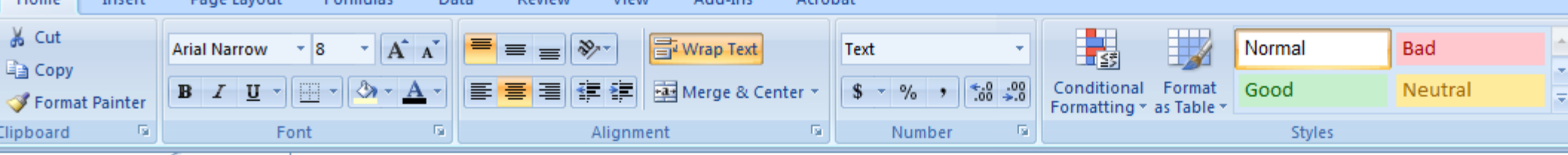
The Typical Employee Life Cycle

- ✓New Applicant (does not create a person record in PeopleSoft)
- ✓Pre-Hire (does create a record in PeopleSoft-only for faculty)
- ✓Hire (does create a record in PeopleSoft)
- ✓Change of Department
- ✓Enrollment as a Graduate or Special Student
- ✓Leave of Absence, Short or Long Term Disability
- ✓Emeritus Status
- ✓Termination
- ✓Retirement
- ✓Death

The Typical Student Life Cycle

- ✓ Prospect (creates a skeletal record in PeopleSoft)
- ✓ Applicant
- ✓ Admitted (we admit the student)
- ✓ Accepted (the student accepts our offer of admission)
- ✓ Matriculated (creates a student record)
- ✓ Progress Towards Degree
  - ✓ Change in Class Year; qualifying events for Graduate students
  - ✓ Stop In/Stop Out Events (leaves, withdrawals)
  - ✓ Graduation
  - ✓ Post Graduation Relationship(s)-(Second Student Career/ Employee/Trustee/Parent/Other)


Cut
Copy
Format Painter
Arial Narrow
8
Wrap Text
Merge & Center
Text
Conditional Formatting
Format as Table
Normal
Bad
Good
Neutral
Clipboard
Font
Alignment
Number
Styles
H9
NA
Formula Bar
Status
Target Attributes
Business Role
Affiliation
Affil. Group
Status Code
"Active" Sun Directory and Active Directory Entries with a NetID
Prov. Date Offset (prior to start date)
Deprov. Date Offset (after end date)
Public Policy
Prov. Date Offset
Deprov. Date Offset
Separate Page Account
Prov. Date Offset
Deprov. Date Offset
Princeton. EDU E-mail
Prov. Date Offset
Deprov. Date Offset
SunIMAP Account
Prov. Date Offset
Deprov. Date Offset
PMAccount
Prov. Date Offset
Deprov. Date Offset
Comments
BR_0XX ST UG APPL N NA 0 N NA 0 N NA 0 N NA 0 N NA 0 N NA 0 Regular Undergradu Applicant
BR_076 ST UG ACTV Y 0 NA Y 0 NA Y 0 NA Y 0 NA Y 0 NA Y 0 NA Regular Undergradu Student
BR_082 ST UG NSHO N NA 0 N NA 0 N NA 0 N NA 0 N NA 0 N NA 0 A No-Show loses a privileges immediat
BR_081 ST UG INAC Y 0 NA Y 0 NA Y 0 NA Y 0 NA Y 0 NA Y 0 NA Students on LOA kee priviliges
BR_079 ST UG INAC N NA 1095 N NA 1095 N NA 1095 N NA 1095 N NA 1095 N NA 1095 All other inactive students keep privile
BR_080 ST UG INAC N NA 14 N NA 0 N NA 14 N NA 14 N NA 14 N NA 14 Expelled students lo all privileges immediately;this rea means they have a day grace period
BR_078 ST UG DECS N NA 30 N NA 0 N NA 30 N NA 30 N NA 30 N NA 0 If an undergraduat student dies, all privileges will termin
BR_002 AL UG ACTV N NA 122 N NA 0 N NA 122 N NA 365 N NA 122 N NA 122 Undergaduate alum have 4 months to establish a forwardi email address an
Sheet1
Provisioning Table



H9 NA

Formula Bar

B	C	D	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	W	X	Y
		Status		Target Attributes																	
Business Role	Affiliation	Affil. Group	Status Code	"Active" Sun Directory and Active Directory Entries with a NetID	Prov. Date Offset (prior to start date)	Deprov. Date Offset (after end date)	Policy Separable	Prov. Date Offset	Deprov. Date Offset	Unix Account	Prov. Date Offset	Deprov. Date Offset	Princeton. EDU E-mail	Prov. Date Offset	Deprov. Date Offset	SunIMAP Account	Prov. Date Offset	Deprov. Date Offset	OPM Account	Prov. Date Offset	Deprov. Date Offset	Comments
BR_0XX	ST	UG	APPL	N	NA	0	N	NA	0	N	NA	0	N	NA	0	N	NA	0	N	NA	0	Regular Undergradu Applicant
BR_076	ST	UG	ACTV	Y	0	NA	Y	0	NA	Y	0	NA	Y	0	NA	Y	0	NA	Y	0	NA	Regular Undergradu Student
BR_082	ST	UG	NSHO	N	NA	0	N	NA	0	N	NA	0	N	NA	0	N	NA	0	N	NA	0	A No-Show loses privileges immediat
BR_081	ST	UG	INAC	Y	0	NA	Y	0	NA	Y	0	NA	Y	0	NA	Y	0	NA	Y	0	NA	Students on LOA kee priviliges
BR_079	ST	UG	INAC	N	NA	1095	N	NA	1095	N	NA	1095	N	NA	1095	N	NA	1095	N	NA	1095	All other inactive students keep privile
BR_080	ST	UG	INAC	N	NA	14	N	NA	0	N	NA	14	N	NA	14	N	NA	14	N	NA	14	Expelled students l all privileges immediately;this rea means they have a day grace period
BR_078	ST	UG	DECS	N	NA	30	N	NA	0	N	NA	30	N	NA	30	N	NA	30	N	NA	0	If an undergraduat student dies, all privileges will termin
BR_002	AL	UG	ACTV	N	NA	122	N	NA	0	N	NA	122	N	NA	365	N	NA	122	N	NA	122	Undergaduate alum have 4 months to establish a forwardi email address an

IDM and Affiliates

Affiliate

- More than a guest
- Less than a Student, Staff and Faculty

Examples

- Affiliated ORU
  - UCSD School of Medicine and Childrens Hospital
    - Howard Hughes Medical Institute
- Public Service
  - Research Divers Registry
- Contractors

The Model

- Departmental Sponsorship
  - Sponsored for a specific period of time
  - Sponsored for a specific activity
  - Only required information collected

Different Levels

- Low level sponsorship
  - Non-sensitive systems
- High level sponsorship
  - Identity proofing
  - Access to sensitive/transactional systems
  - Departmental officer approval

UC Berkeley
Guest Access Management

March 2010
JASig Conference Presentation

Dedra Chamberlin
Manager, CalNet - Identity and Access Management

Current CalNet Affiliates

- Variety of affiliations with varying levels of access
  - Contractor
  - Retired
  - Visiting Scholar
  - Volunteer
  - LBL/DOE Post Doc
  - LBLOP Staff
- Must be added to HR system by HR administrators
- One year maximum with option for renewal

Problems with Current Systems

- Affiliations have been created ad hoc over the years - don't always meet access needs for particular guests
- HR administration creates a lot of overhead for establishing guest access
- Many departments have created their own stand-alone user account systems, with local administration and inconsistent de-provisioning (costly and insecure)

Sample Stand-Alone Guest Systems

- Guest Wireless Access
- Residential and Student Services Co-habitants
- Sakai (bSpace)
- Active Directory ! accounts
- The list goes on

Guest Account Management Project

Guest Account Taskforce created

Plan A

Quick project to centralize guest accounts for departmental apps - save the complicated stuff for later

Plan B

Oops.

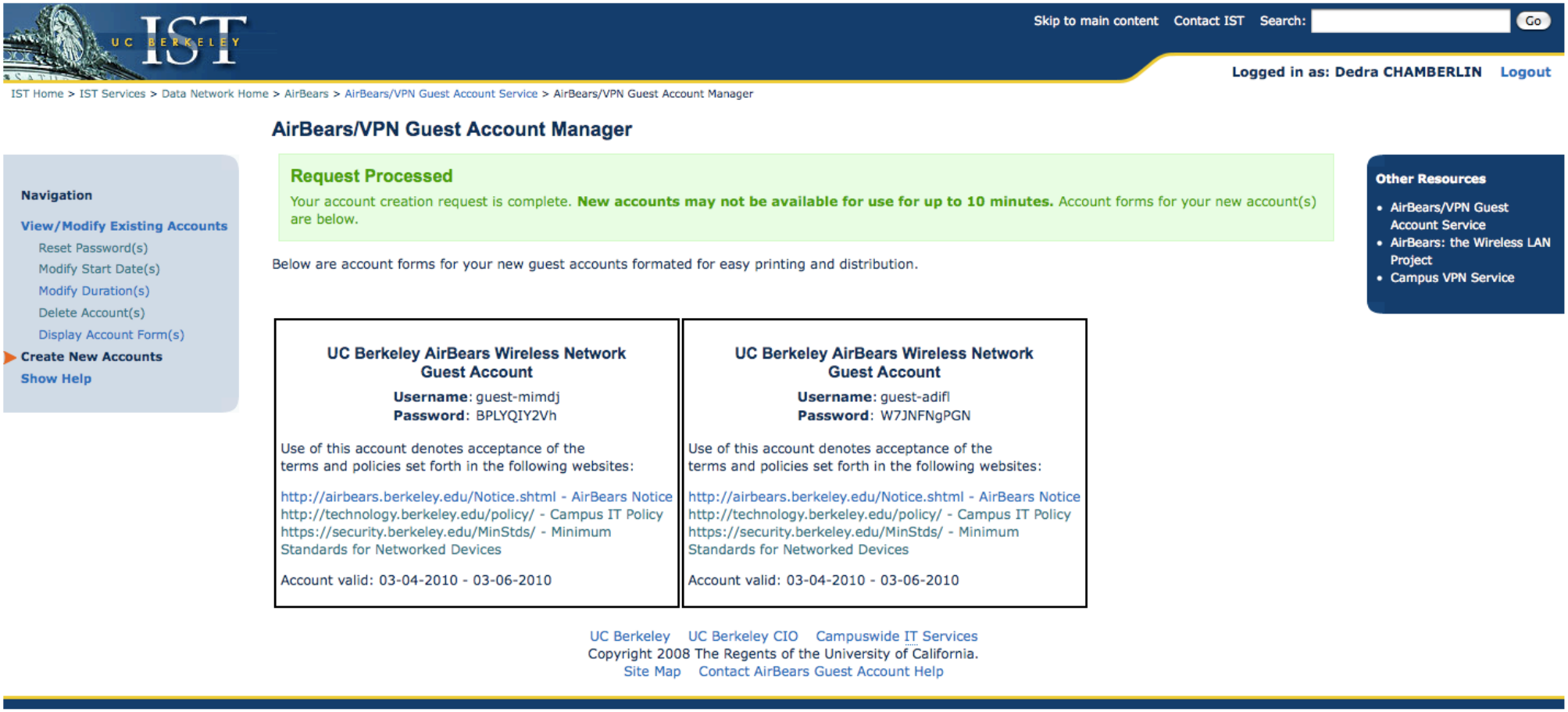
- movement between guest and non-guest systems
- accounts vs. authorizations

Plan C

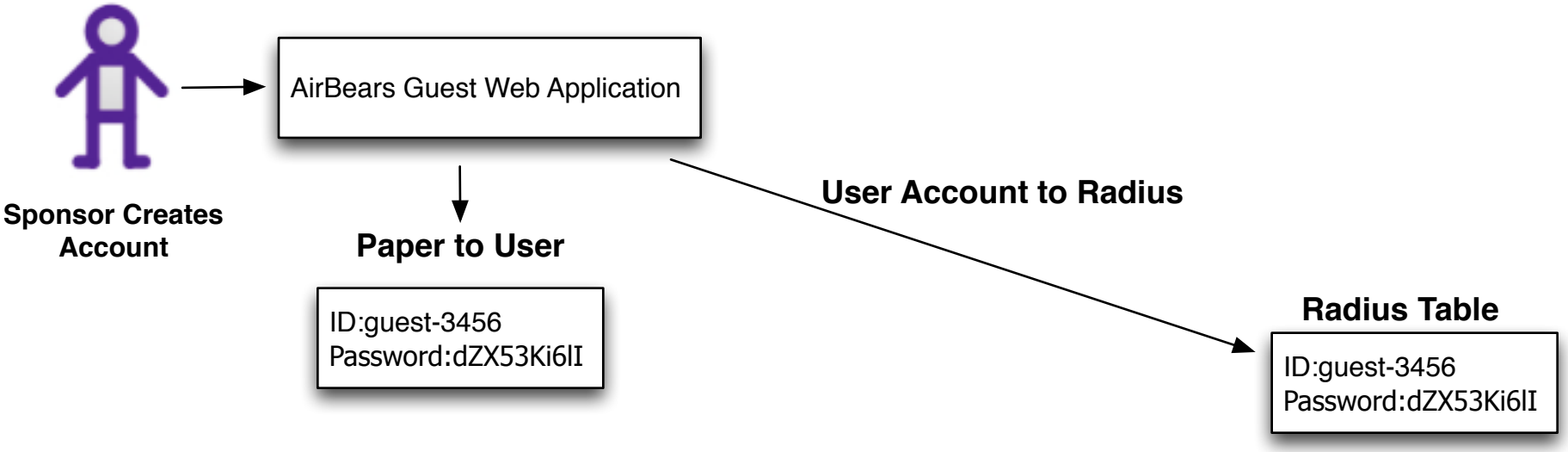
Just start integrating something!

Guest Wireless - AirBears

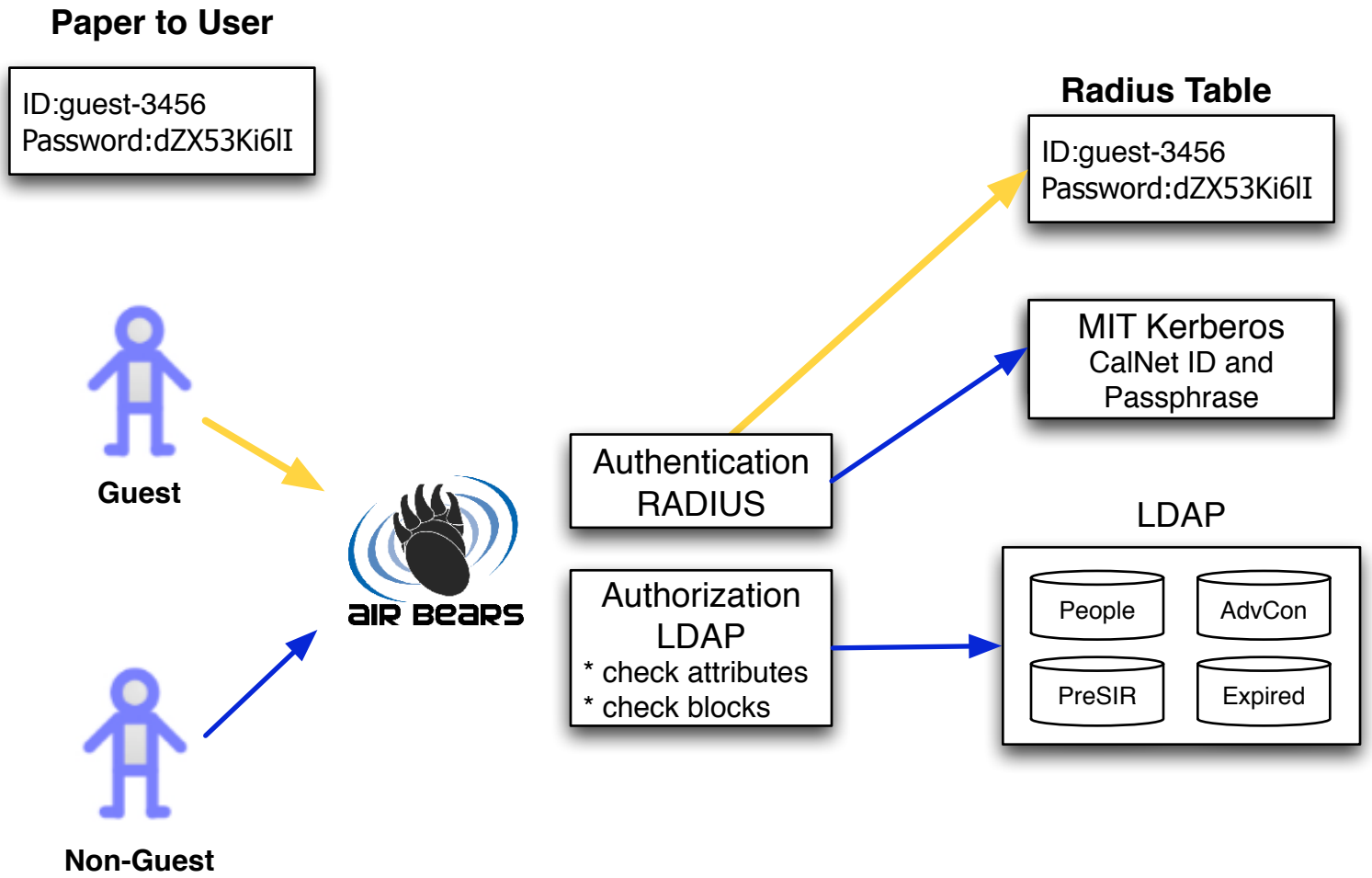
Guest Wireless - AirBears



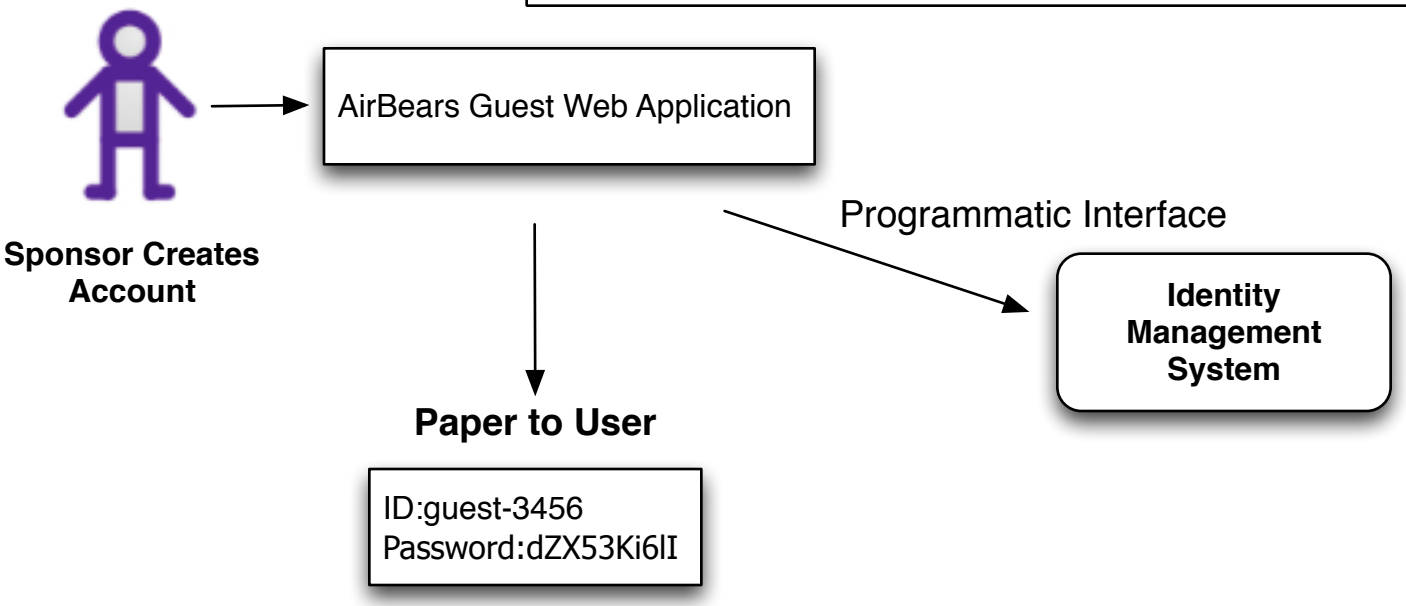
Guest Access Management - AirBears
How it worked in the past



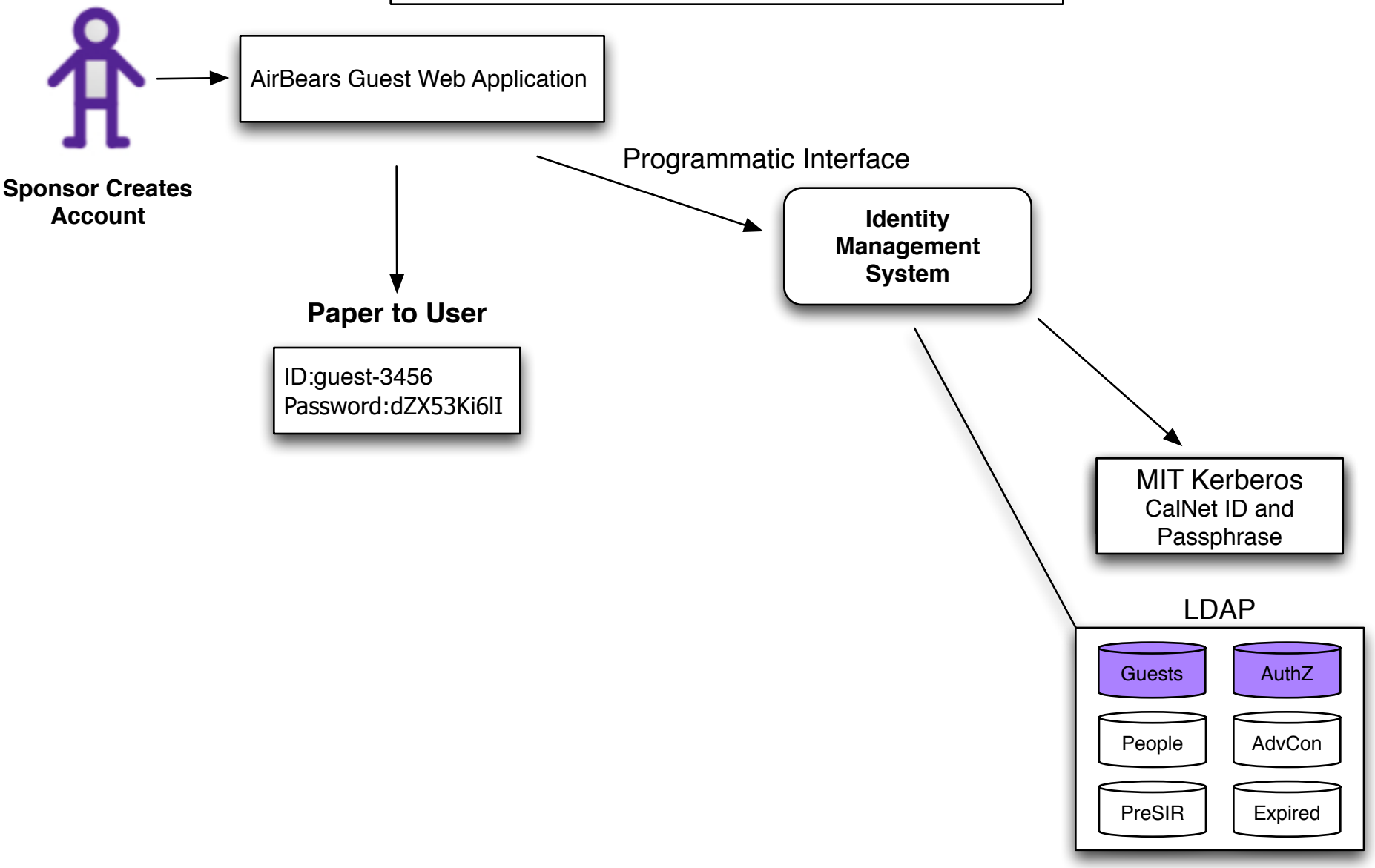
Guest Access Management - AirBears
How it worked in the past



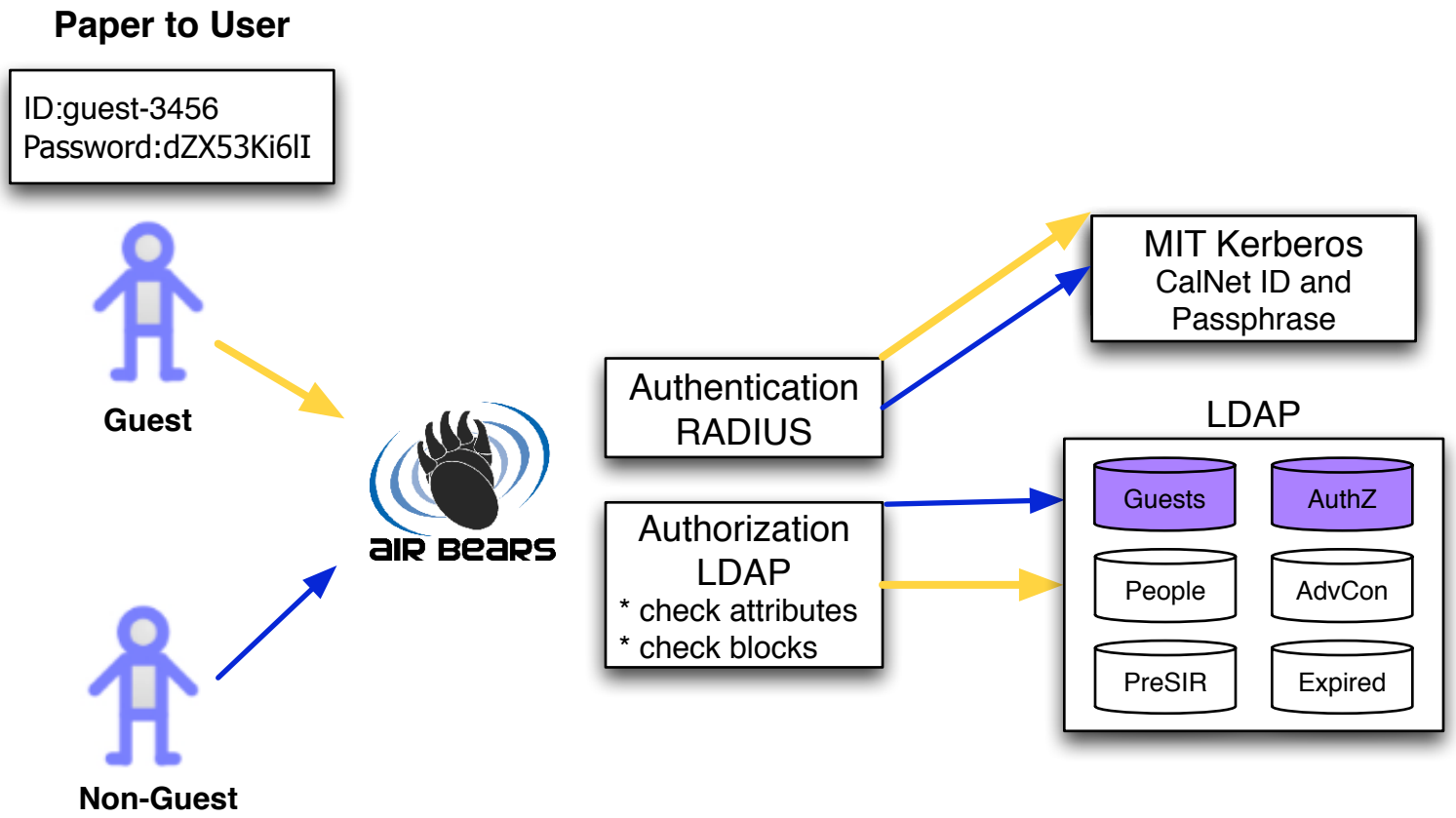
Guest Access Management - AirBears
How it Works Now



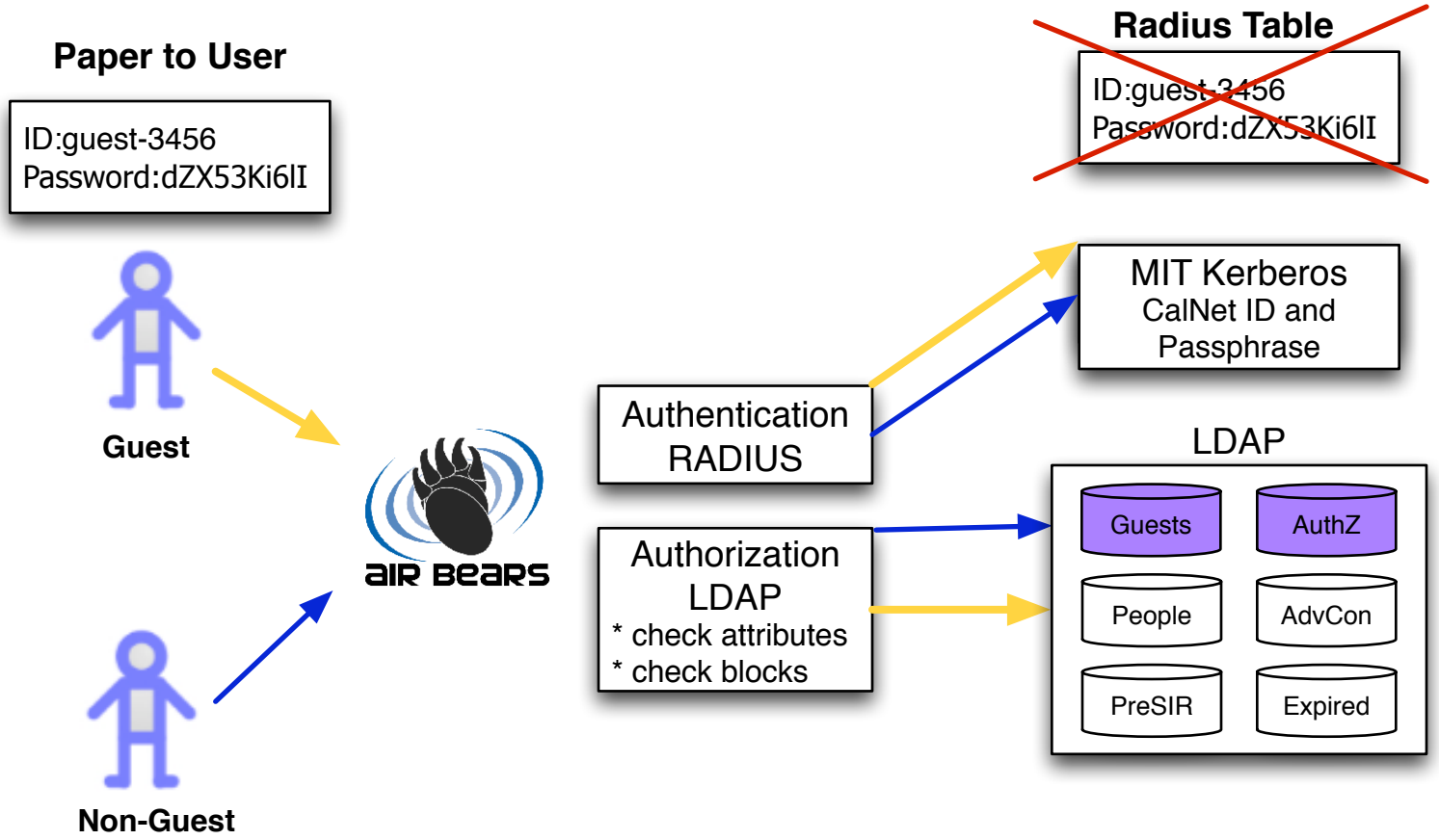
Guest Access Management - AirBears
How it Works Now



Guest Access Management - AirBears
How it Works Now



Guest Access Management - AirBears
How it Works Now



AirBears and RSSP Co-habitant Access
Programmatic Input vs IMS Interfaces

Sponsor Creates Account

AirBears Guest Web Application

Programmatic Interface

Identity Management System

RSSP Co-habitant Application

* Access Request
* Approval Workflow
* Account provisioning and de-provisioning

User Requests Co-habitant Account Access to:

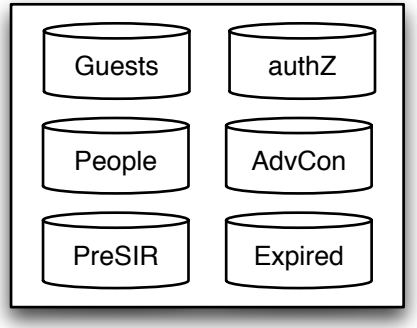
- **Residential Computing Centers**
- **Residential Wireless**
- **Residential Helpdesk application**

Sponsor Confirms Account Administrator Approves Account

MIT Kerberos
CalNet ID and Passphrase

Active Directory

LDAP



Postgres

Thoughts on Overall Guest Account Design

Role: Short-Term Guest

Guest types:

- Wireless access
- Conference Guests
- AFS document sharing

Account Parameters:

- Duration - Maximum 1 month
- Namespace - defined by required prefix: "guest-"
- Sponsorship - required
- Level of Assurance - None
- De-provisioning - one year after sponsorship expires

Role: Extended Guest

Guest types:

- Guest lecturers
- Visiting Scholars
- Co-habitants
- Auditors
- Current CalNet affiliates?

Account Parameters:

- Duration - Maximum 1 year (allow renewal)
- Namespace - use standard CalNet ID to facilitate migration of account and associated authorizations if person obtains non-guest status (gets hired or becomes a student)
- Sponsorship - required
- Level of Assurance: Tiered
- De-provisioning - one year after last sponsored authorization expires

Questions and Discussion