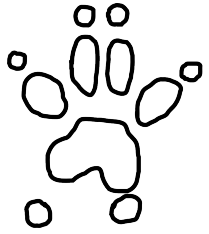
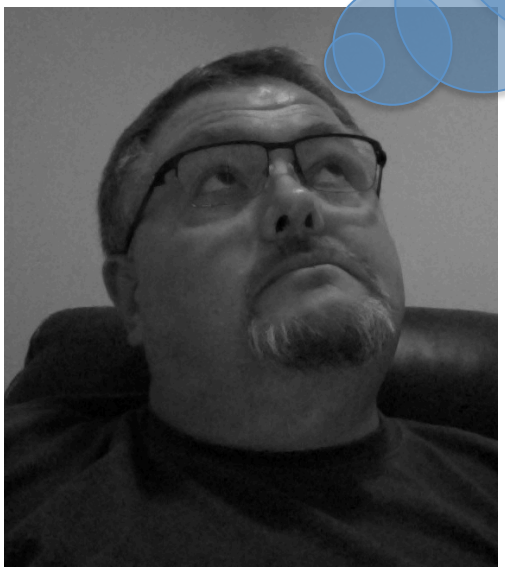
IAM Complicated

Why you need to know about IAM



Secret Chipmunk
Ron Parker | @scmunk




OVERSTUFFED MY BURRITO
NOW IT'S TOO MESSY TO EAT
memegenerator.net

What went wrong?

Bad tools and ingredients.

No burrito processes.

Bad burrito skills.*

But you have had good burritos…

*skills = skillz or 5k1ll5 for all you 1337

Bad tools and ingredients.

No burrito processes.

Bad burrito skills.*

But you have had good burritos…

Where did you have a good burrito?

Welcome to Joe's!

Joe's
Burrito Barn

What do burritos have to do with

Identity and Access Management?

What do burritos have to do with

Identity and Access Management?

Making a burrito consistently and efficiently requires a lot of processes, ingredients, and tools

IAM has lots of parts, needs lots of tools, requires lots of process plus people with skills.

IAM complicated

Just like Burritos

There are a lot of reasons Joe's can build a better burrito.

- Menu
- Specialized stations
- Prepared ingredients
- Standards
- Correct tools
- Skilled people
- Processes to tie it altogether

Good **People**.
Good **Process**.
Good **Technology**.

People

Trained People

Enough People

Process

HR

Menu

Recipes

Technology

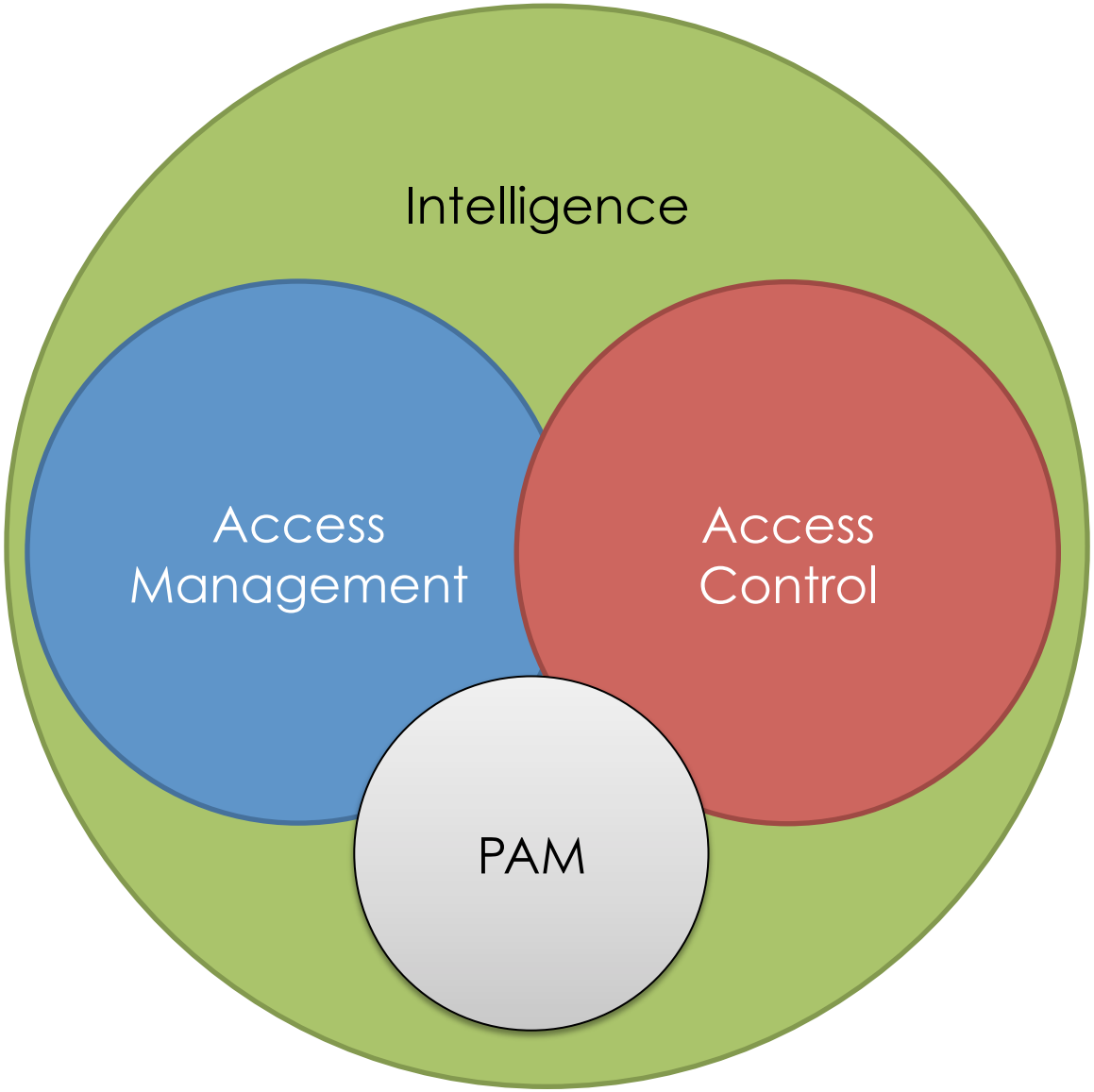
Stations

Grills

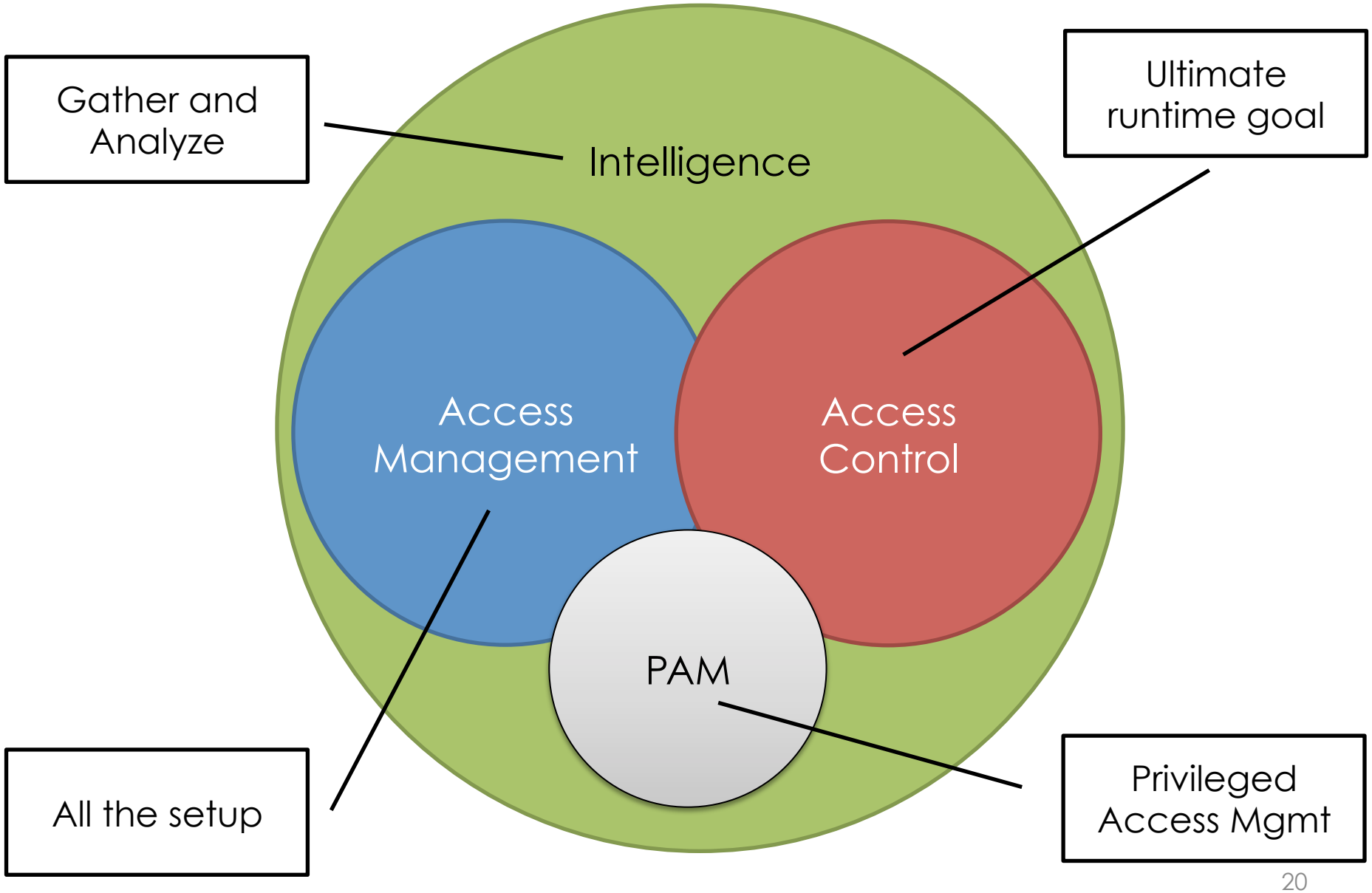
Steamers

Warmers

The World of IAM



The World of IAM



Why does IAM matter?

People

IAM sets things into place so we can do security – so we can protect what is important.

Joe's Burrito Barn

Brand

Thangs and Stuff

Information

It drives the policy for firewalls, ACLs, segmented networks, and accounts.

Access Management

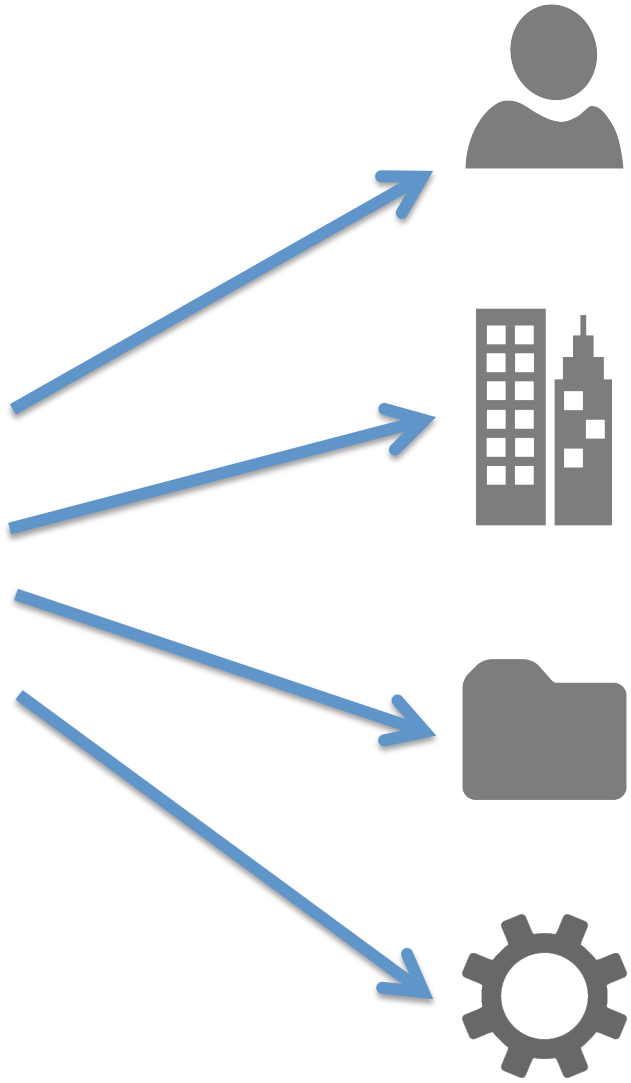
Access Management

- Security Model
- Entitlements
- Identities
- Provisioning

Access Management: Selecting a Model

Importance of

- People
- Brand
- Physical assets
- Data
- Privacy
- Process



Joe's Burrito Barn

Brand

Alarms

HR/Payroll

POS

Access Management: Goal of Models

- Efficiently apply security
- Get the right security controls in the right places

These models try to control the **Confidentiality**, **Integrity**, and **Availability** of the resource.

Access Management: Common Security Models

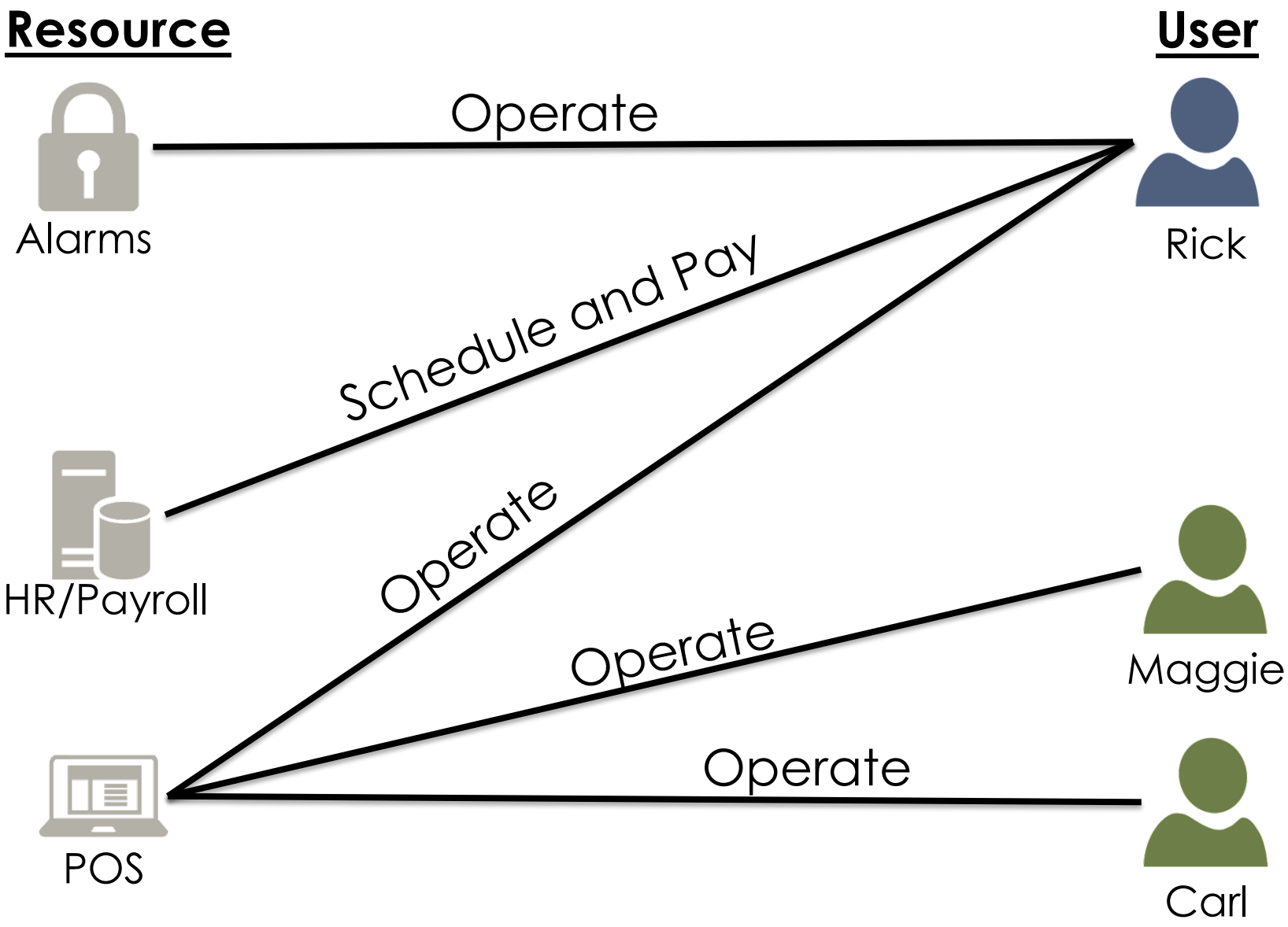
- Direct assignment, discretionary (DAC)
  - Assigned to user and resource
  - No model model
- Mandatory Access Control (MAC)
  - Labels and attributes
  - Low level
  - Security Enhanced Linux (SELinux)
- Roles Based Access Control (RBAC)
  - Permissions given to roles
  - People/entities are assigned to roles
  - LDAP

Access Management: Security Models

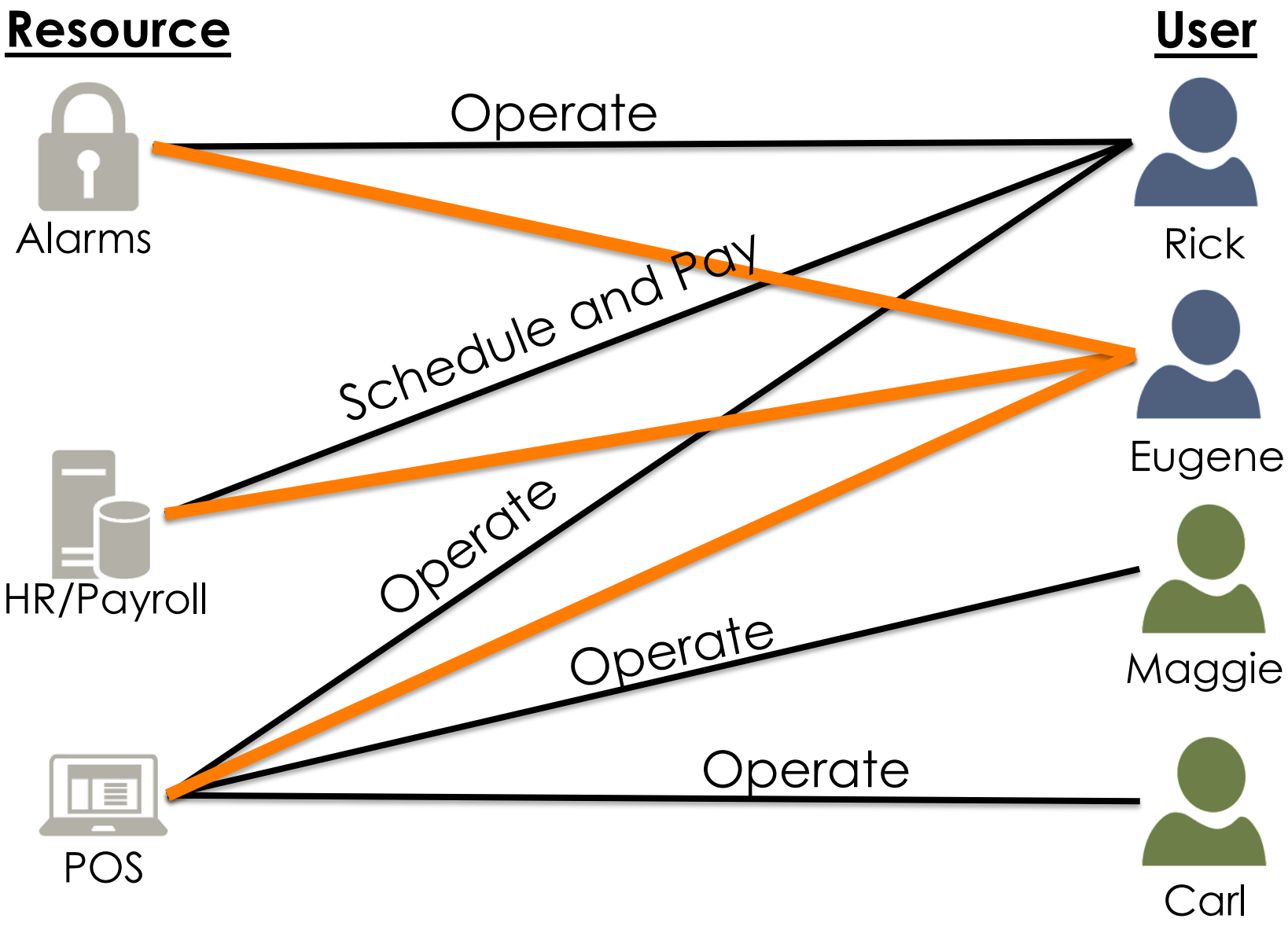
- Attribute Based Access Control (ABAC)
    - Rules or polices based on attributes

- Many others named only in the depths of Government basements

Access Management: Rights and Resources at Joe's



Access Management: Adding more people



Access Management: Looking at Entitlements

Managers

- Operate the alarm
- Schedule
- Pay people
- Operate the POS

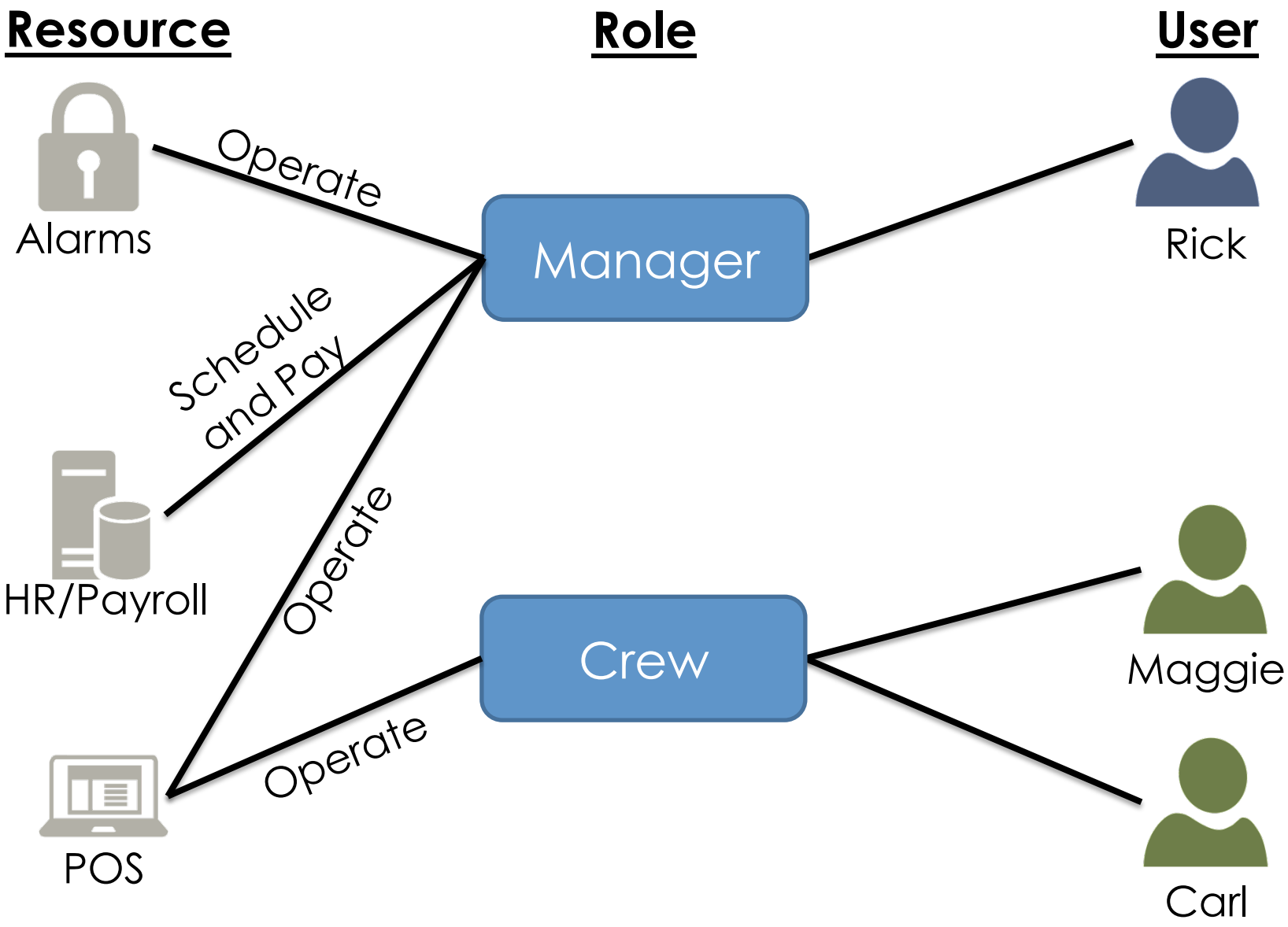
Crew

- Operate the POS

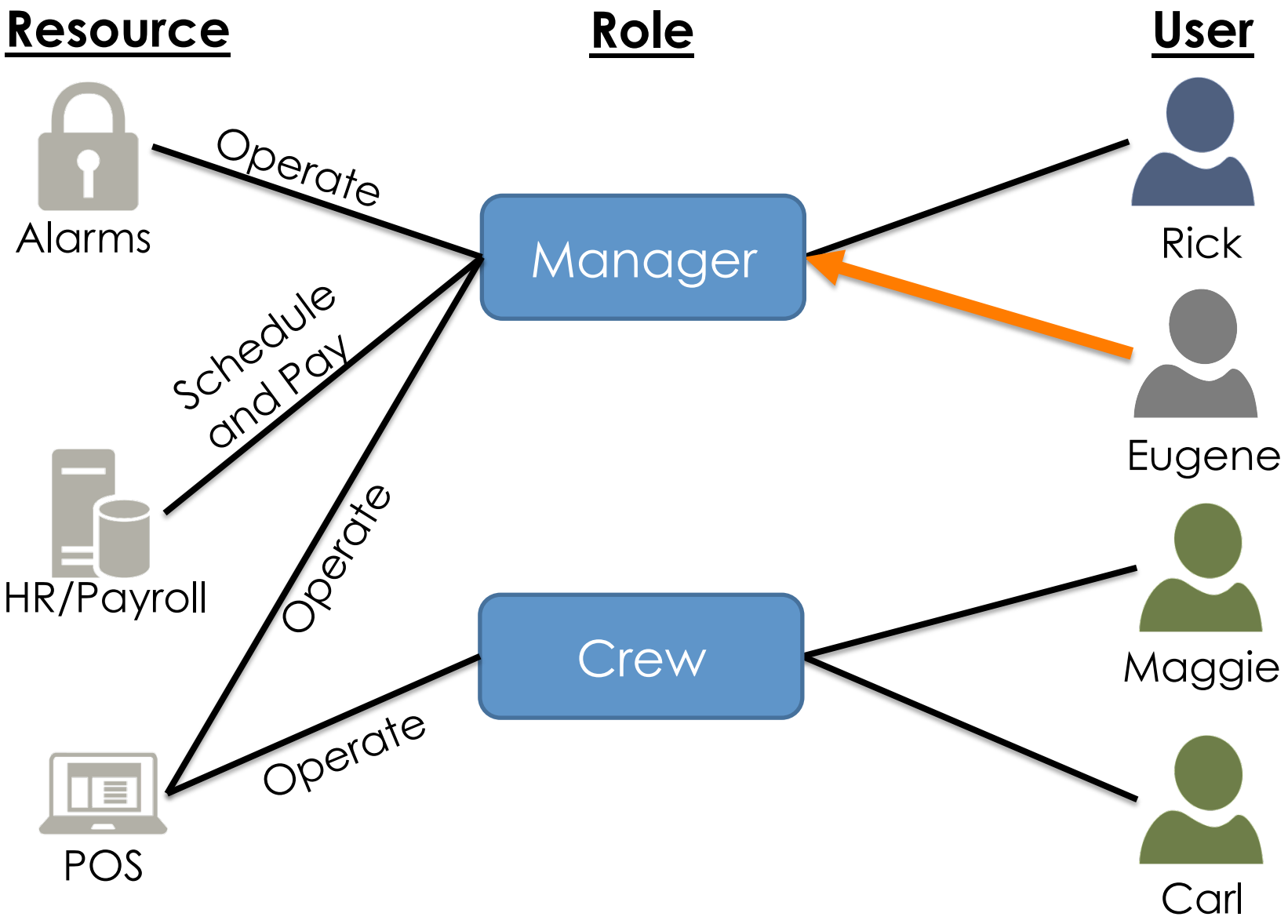
Entitlements are the authorizations, permissions, and rights that let you do things

They are the basis for Access Control

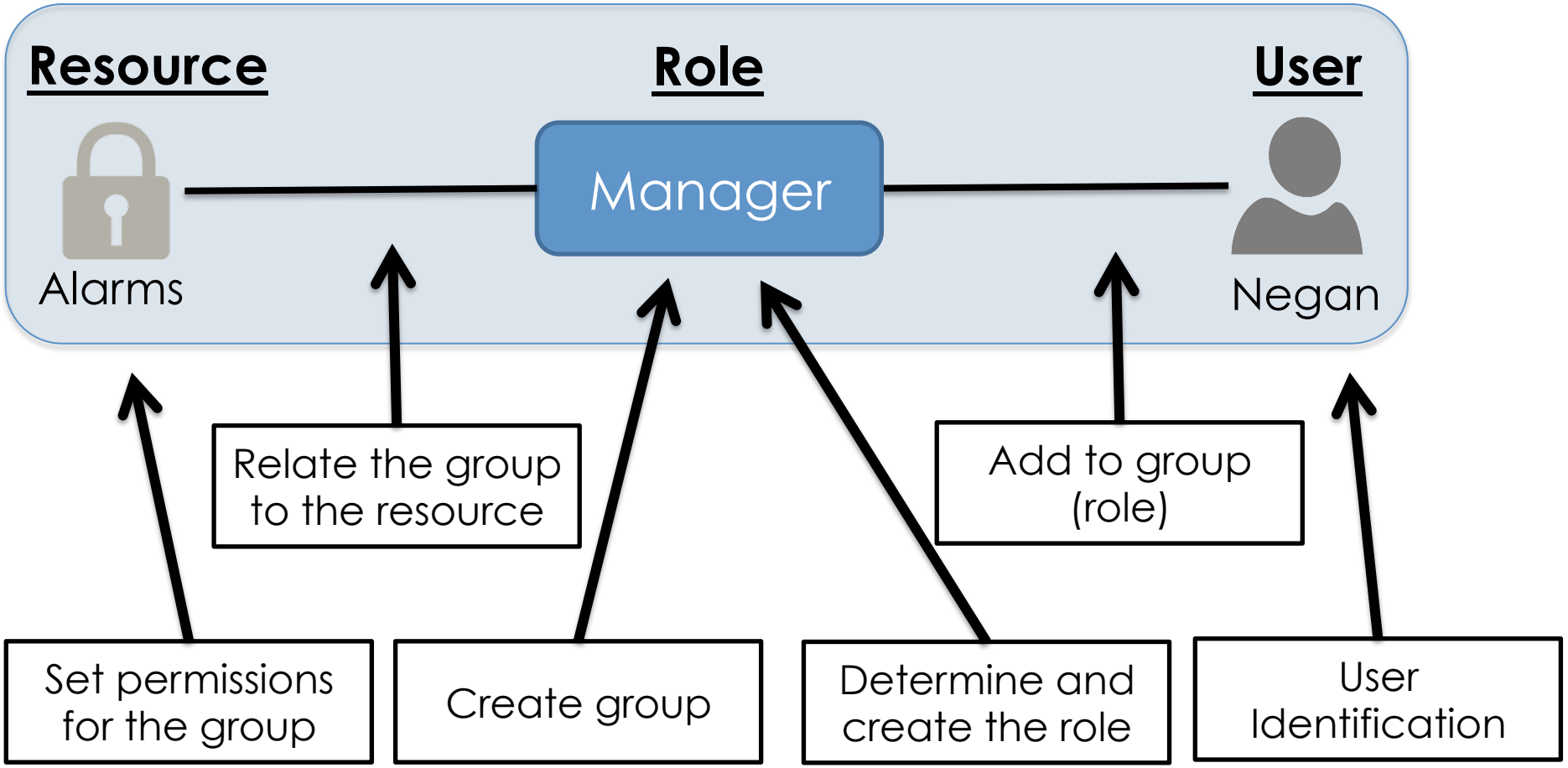
Access Management: Roles and RBAC (Roughly Right)



Access Management: Adding more people with roles



Access Administration: What is really happening



All of this has to happen to enable Access Control

Access Administration: Users, Identities, Accounts

User	Identity	Account
 Rick	Rick@Joes.com	Rick27@SFDC.com RickG@WorkDay.com
 Eugene	Eugene@Joes.com	Eporter@SFDC.com Eugene21@WorkDay.com
 Maggie	Maggie@Joes.com	
 Carl	Carl@Joes.com	

Access Administration: Identities and Attributes

Identity Attributes

- Name
- Employee ID
- Department
- E-mail
- Passwords
- Certificates

One collection of these for efficiency – important for centralized security

Account Attributes

- Employee ID
- System specific info
  - Account limits
  - Preferences
  - Defaults

You may have one set of these per system – some of these may not be in your control

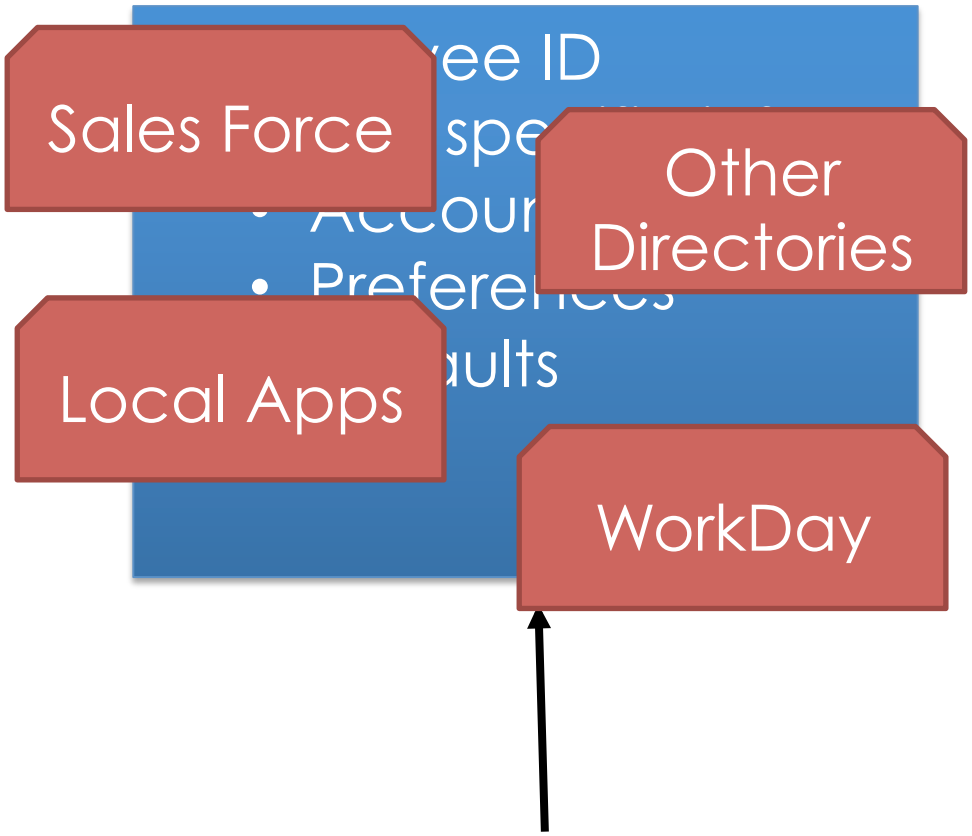
Access Administration: Identities and Attributes

Identity Attributes

- Name
- Employee ID
- Department
- E-mail
- Passwords
- Certificates

One collection of these for efficiency – important for centralized security

Account Attributes



You may have one set of these per system – some of these may not be in your control

Access Administration: Directories

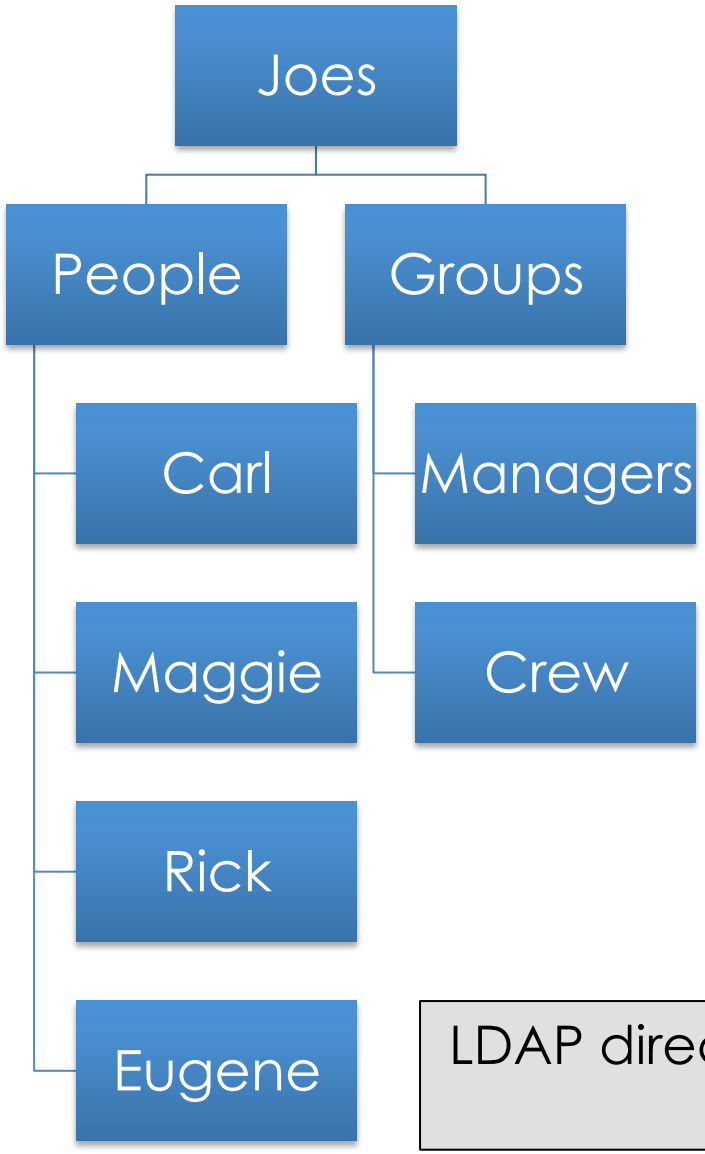
LDAP

- Hierarchical
- Very fast reads
- Standard layout
- Standard Protocol
- Can be used for identities
- Can be used for entitlements
- Can be SQL-based

Example Systems

- OpenLDAP
- Active Directory
- OpenDJ
- RadiantOne
- IBM Directory

Access Management: Directory Contents



dc=joes,dc=com

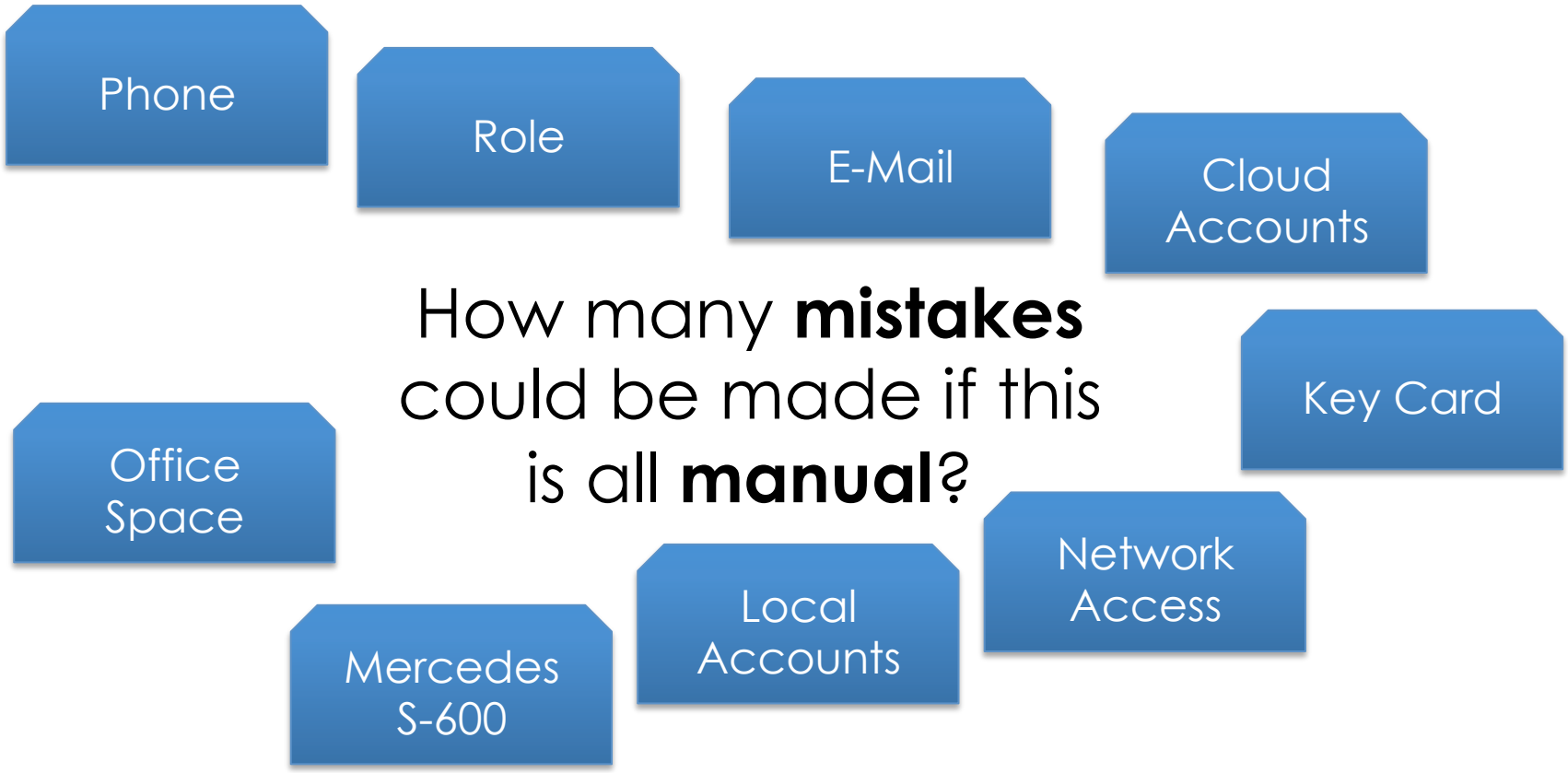
dc=Carl,ou=people,dc=joes,dc=com
dc=Maggie,ou=people,dc=joes,dc=com
dc=Rick,ou=people,dc=joes,dc=com
dc=Eugene,ou=people,dc=joes,dc=com

cn=groups,dc=joes,dc.com
ou=managers,cn=groups,dc=joes,dc.com
ou=crew,cn=groups,dc=joes,dc.com

LDAP directories can house both identities and entitlement information

Access Management: Provisioning

Provisioning is the act of creating all the necessary logical and physical items necessary to for a new identity or modifying an existing identity to make it functional in the environment



Access Management: Workflows

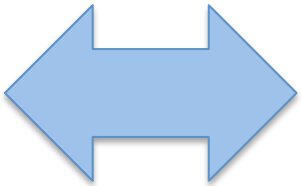
Joe's Menu

Big Burrito

Small Burrito

The Vegan

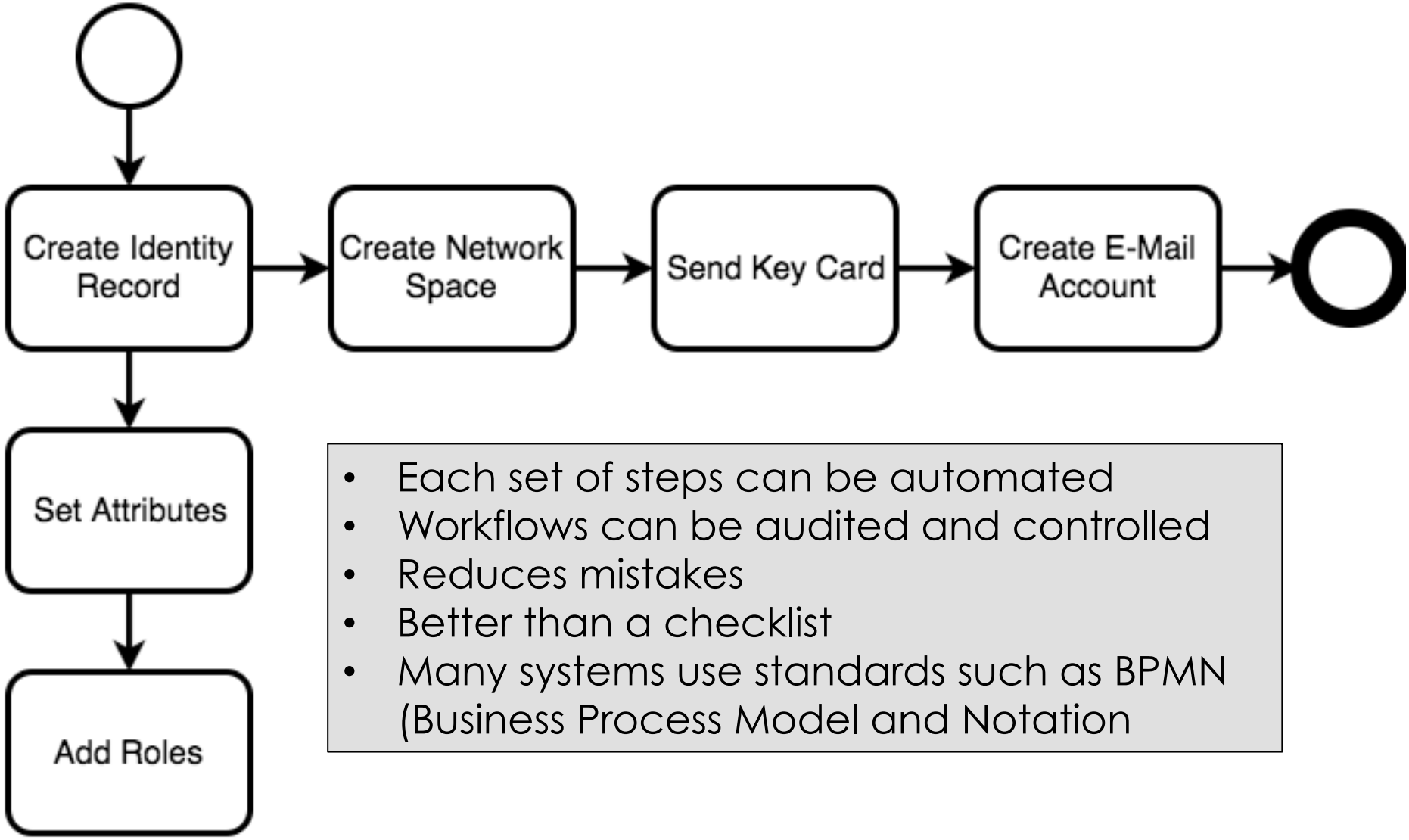
The Glenn



Service Menu

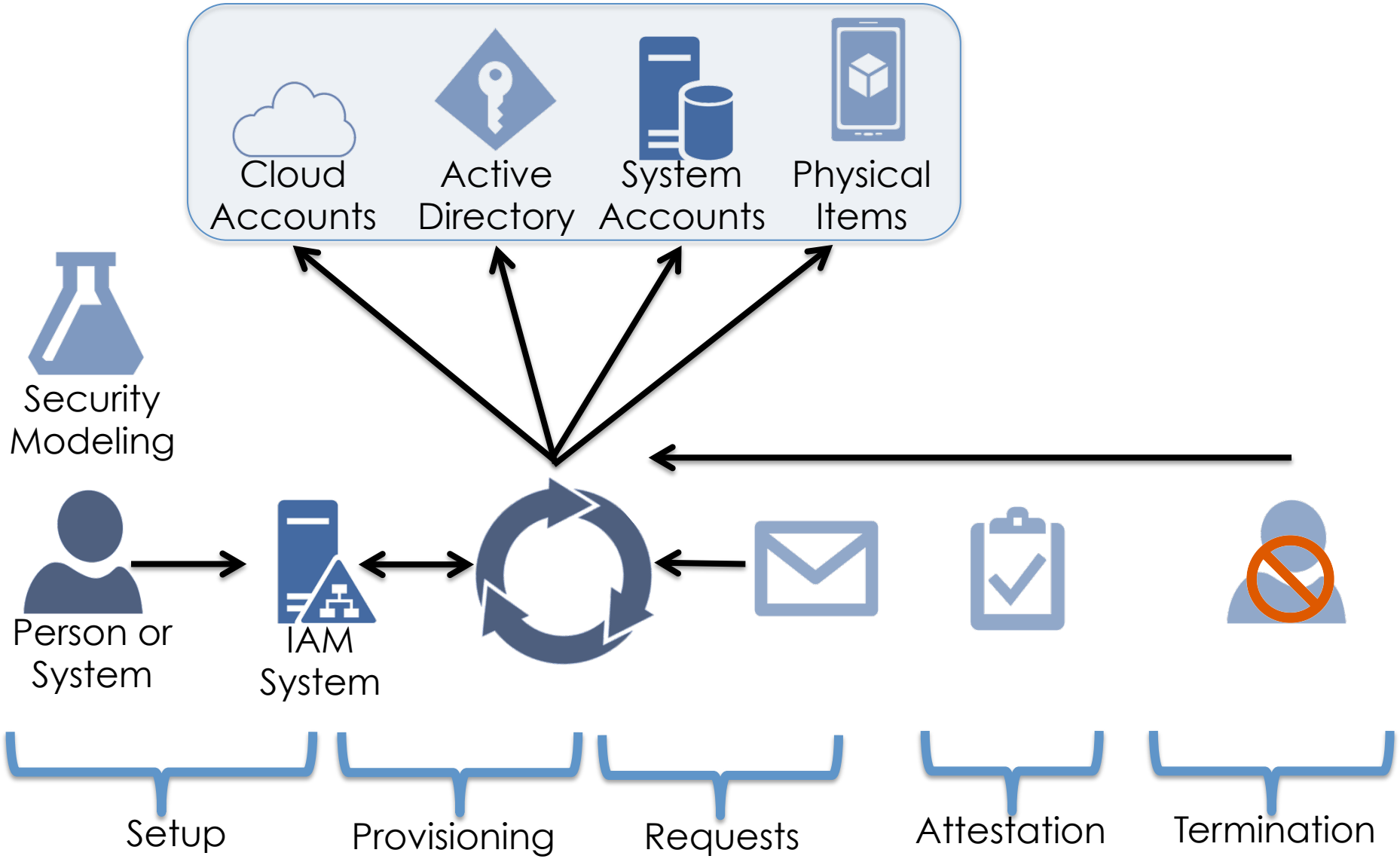
- New Hire
- Add Crew Role
- Add Manager
- Transfer
- Terminate

Access Management: Provisioning Workflows



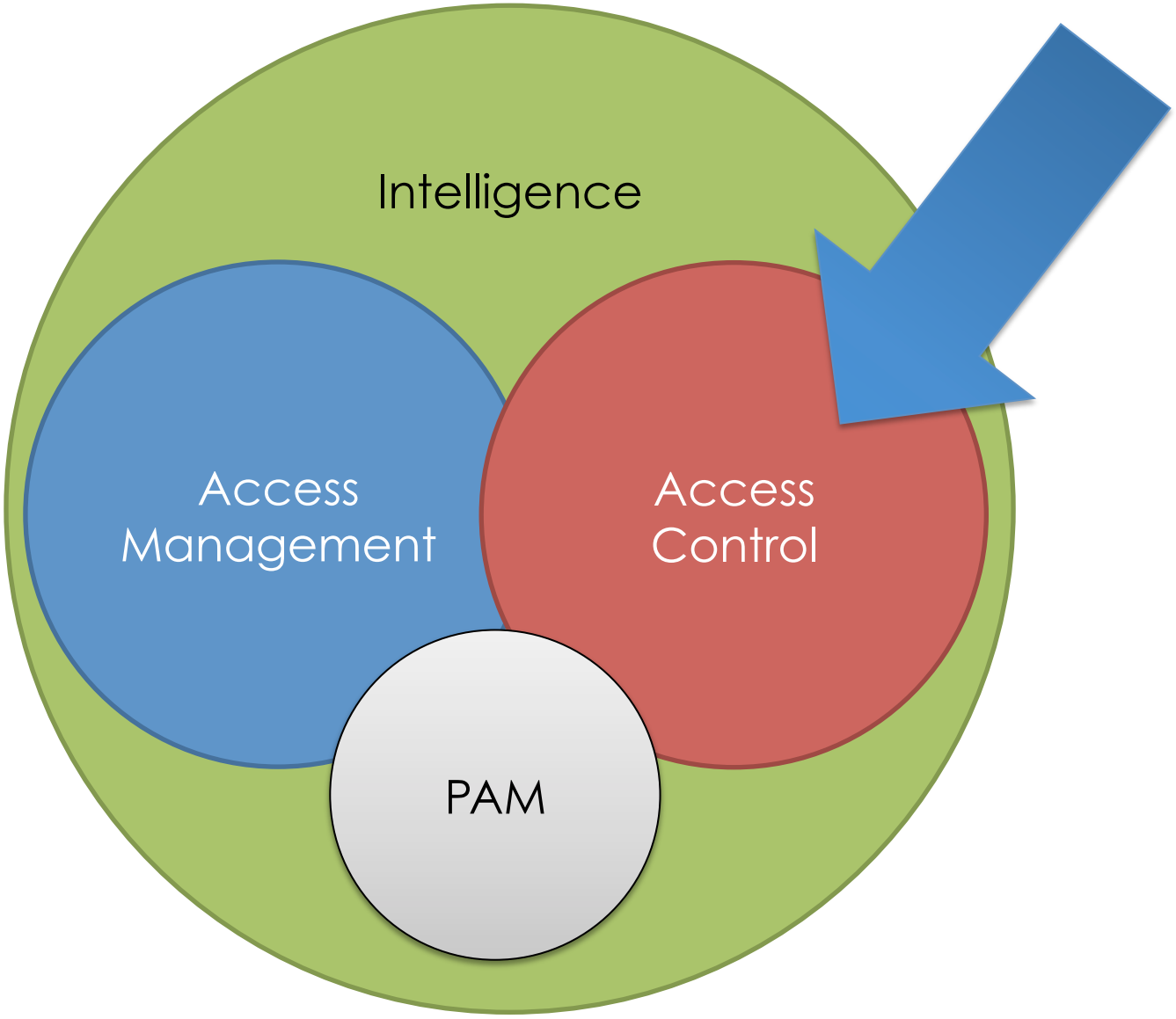
- Each set of steps can be automated
- Workflows can be audited and controlled
- Reduces mistakes
- Better than a checklist
- Many systems use standards such as BPMN (Business Process Model and Notation

Access Management Lifecycle



Access Control

The World of IAM



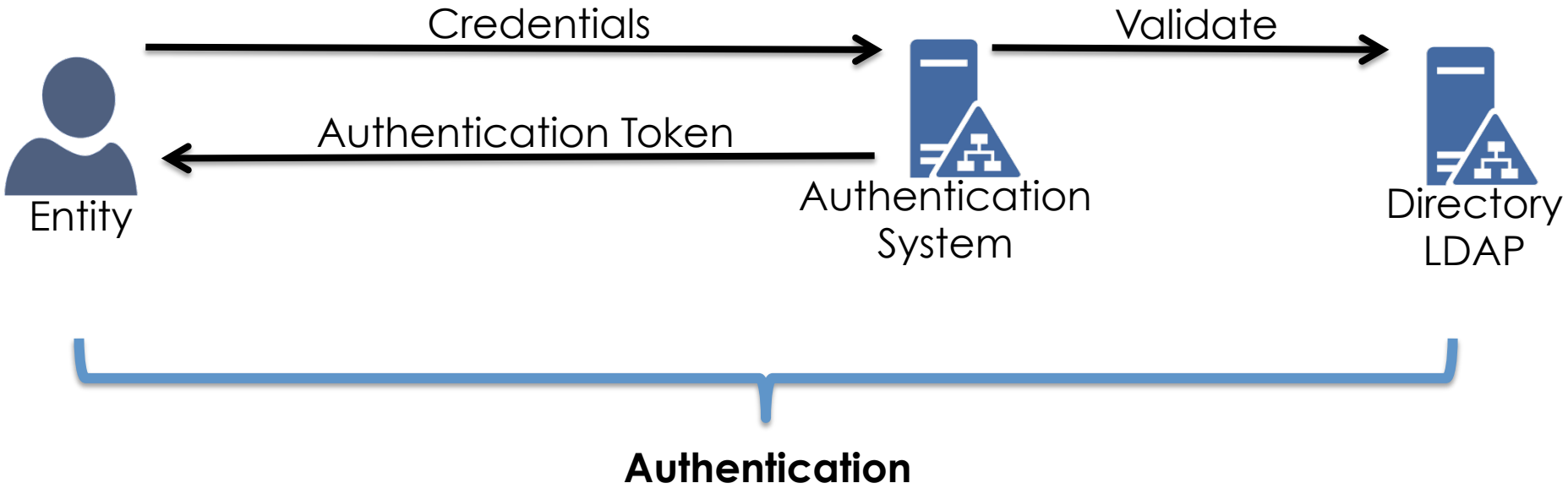
Access Control

- **Authentication**
  - Multi-factor Authentication
  - Single Sign On/Reduced Sign On
  - Federation
- **Authorization**
  - Entitlements
  - Federation (again)

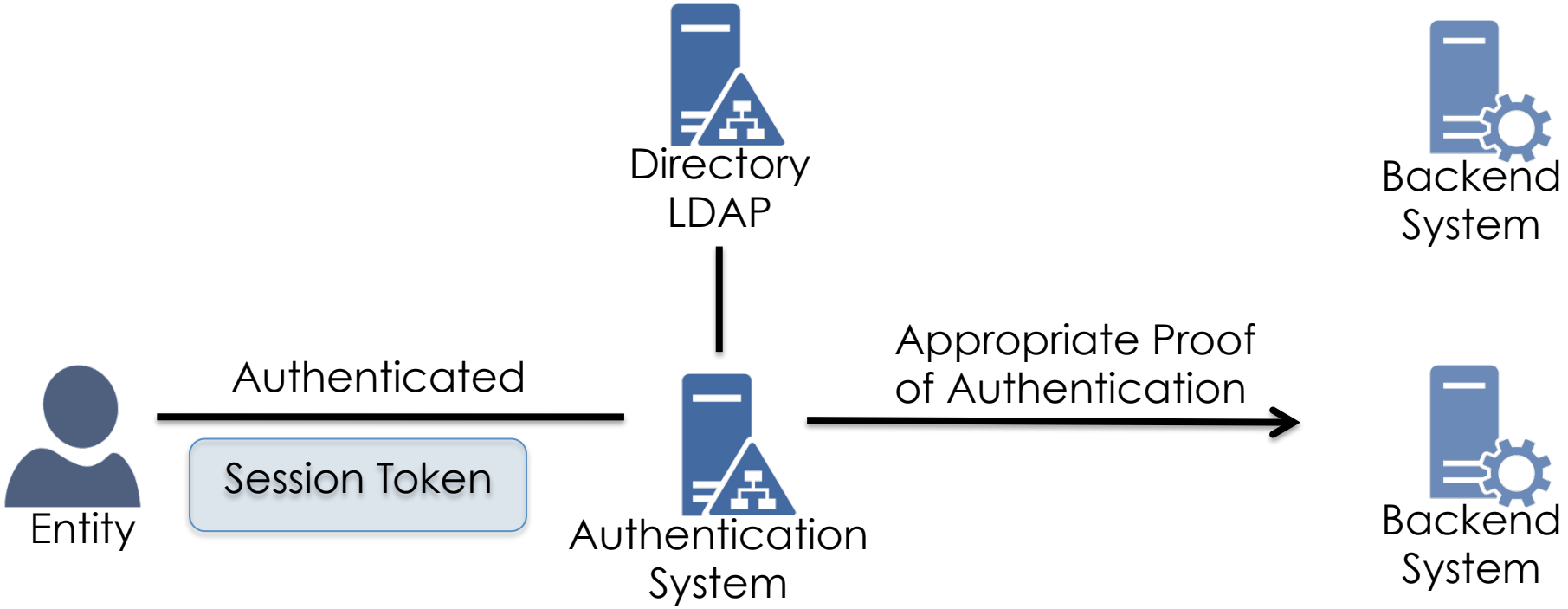
Authentication

One of the many definitions:

Authentication is the process of confirming who you (**Entity**) claim to be (**Identification**) by matching provided credentials to those expected. This information is tied to a **Digital Identity**.

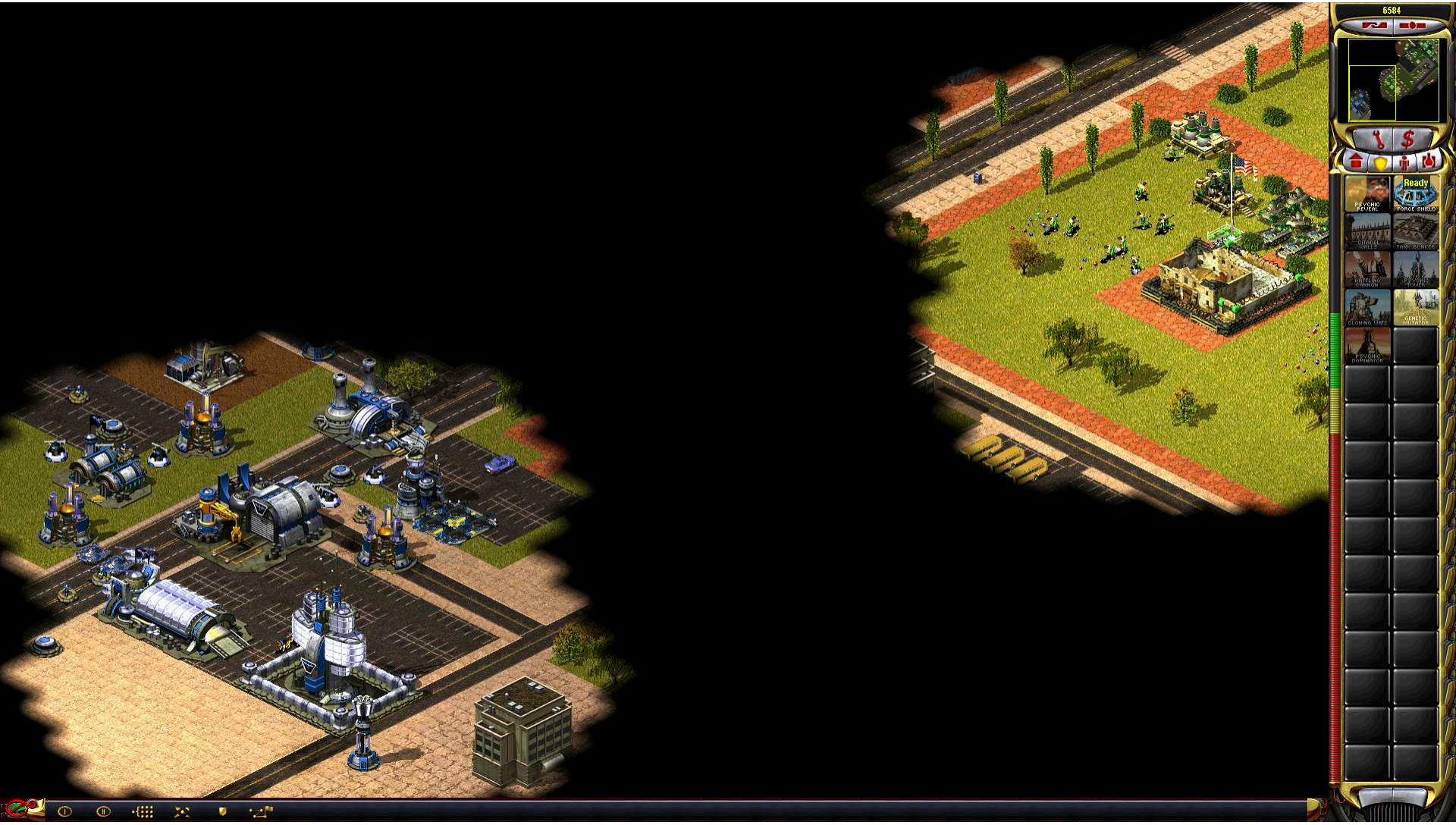


Authentication: Single Sign On/Reduced Sign On

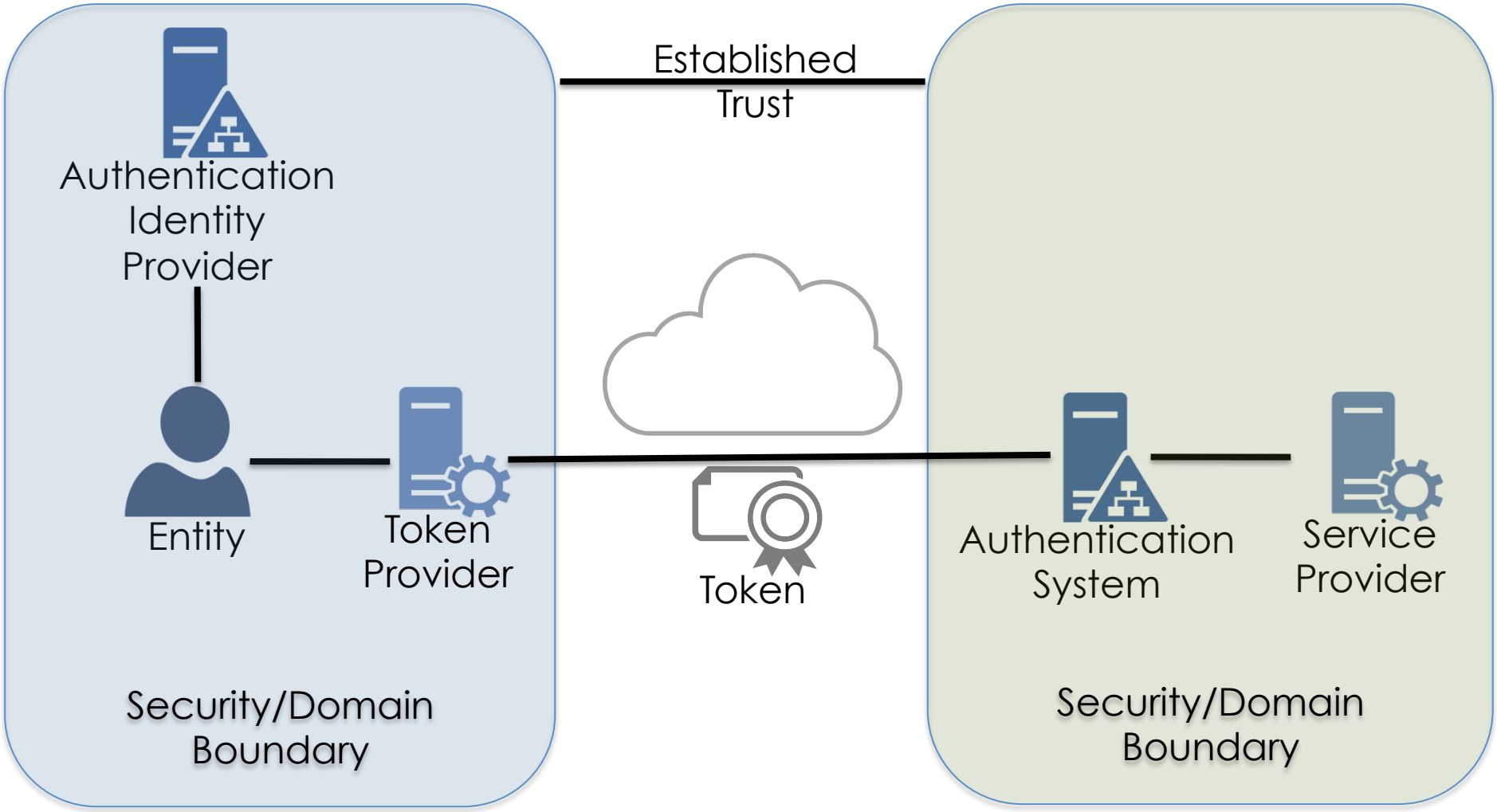


Most SSO systems use a session token. A cookie, or HTTP header.

The Authentication System may send a session token to the backend system or even an ID/Password.


6584
Ready

Authentication: Federation



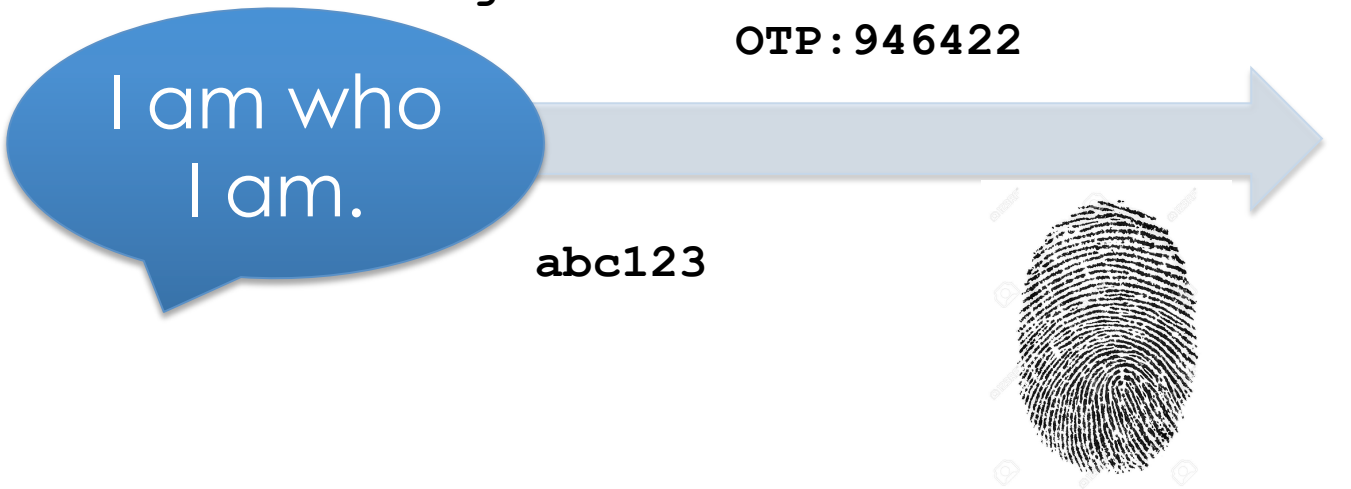
Do I really know who you are saying you are is really who you say you are?

Social Login

I am who I am.

OTP:946422

abc123

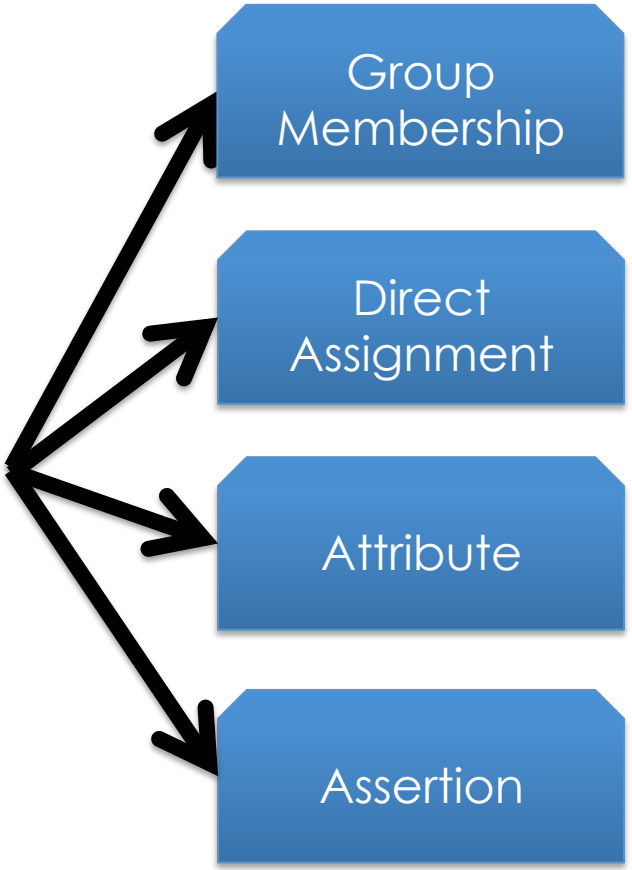


Authorization

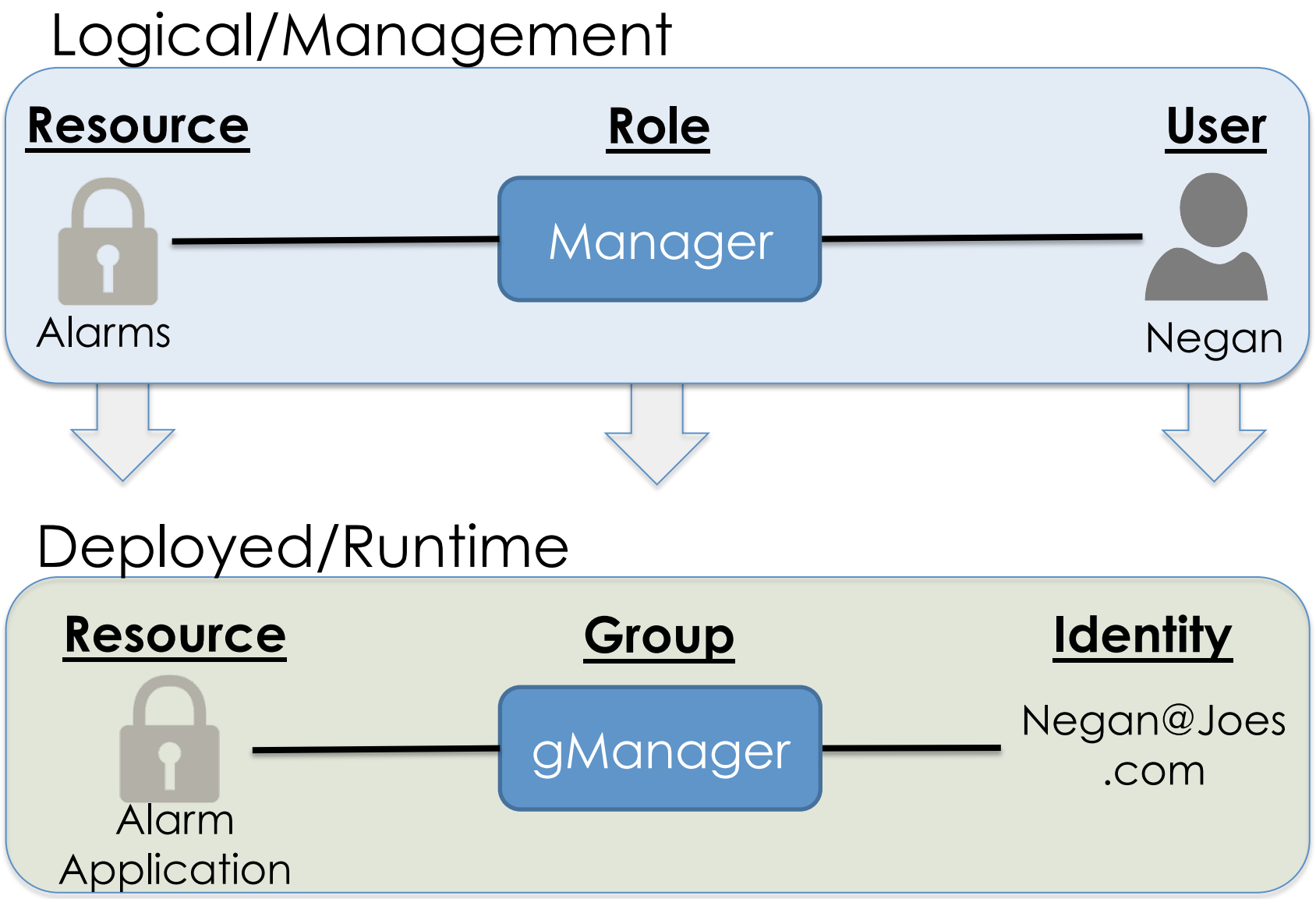
Authorization is determining when and what an entity is entitled to do. It is the other half of the access policy.

The way authorization decisions are made and applied at runtime are greatly determined by the security model.

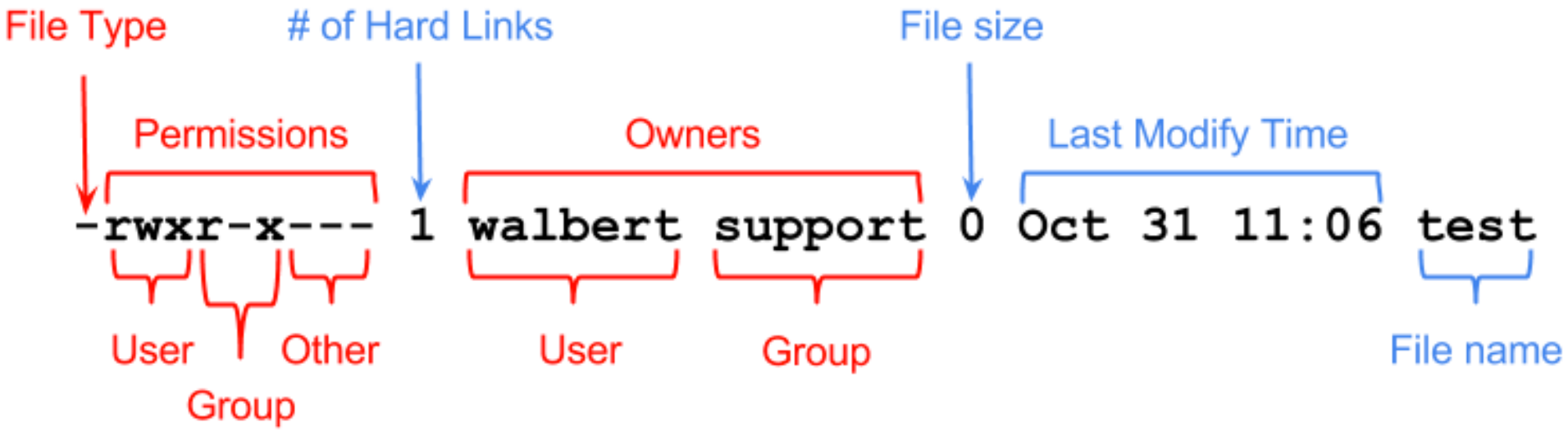
Some models are purely policy (code).



Access Control: Logical to Runtime



Access Control: Linux permission examples




```
drwxr-xr-x 22 root root   4096 Apr 14  2015 ..
drwxr-xr-x  5 root root   4096 Apr  8 06:32 backups
drwxr-xr-x 11 root root   4096 May 21  2015 cache
drwxrwxrwt  2 root root   4096 Apr 17  2014 crash
drwxr-xr-x 49 root root   4096 May 21  2015 lib
drwxrwsr-x  2 root staff  4096 Apr 10  2014 local
lrwxrwxrwx  1 root root      9 Apr 17  2014 lock ->
drwxrwxr-x 11 root syslog 4096 Apr 11 06:45 log
```

Authorization: AWS Policy

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"AddPerm",
      "Effect":"Allow",
      "Principal": "*",
      "Action":["s3:GetObject"],
      "Resource":["arn:aws:s3:::joesbucket/
*"]
    }
  ]
}
```

Authorization: Entitlements - SAML

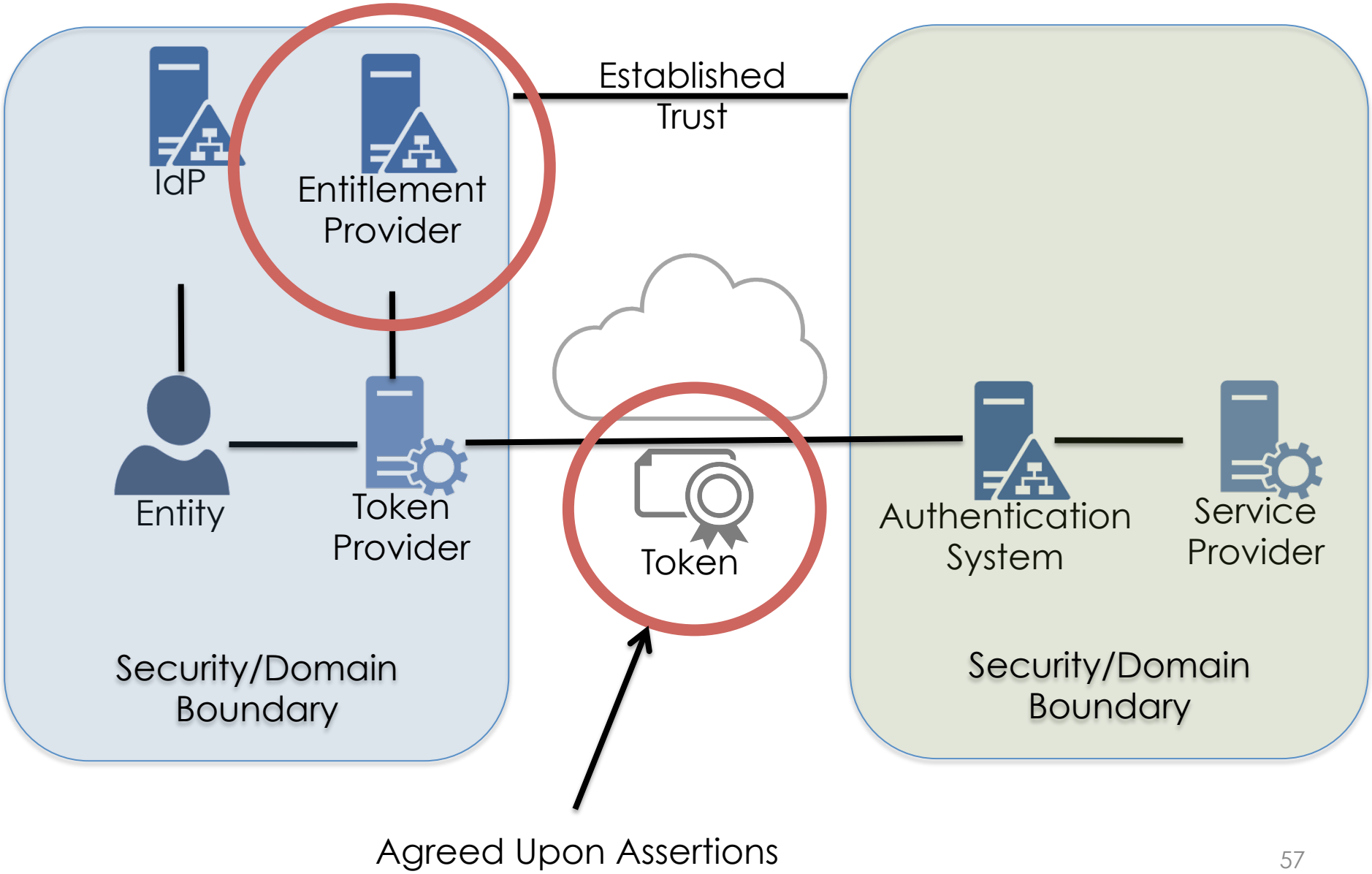
```
saml:AttributeStatement>
   <saml:Attribute Name=”User_name">
      <saml:AttributeValue
xsi:type="xs:anyType">Rick Grimes</
saml:AttributeValue>
   </saml:Attribute>

   <saml:Attribute Name=”user_email">
         <saml:AttributeValue
xsi:type="xs:anyType">rick@joes.com</
saml:AttributeValue>
   </saml:Attribute>
</saml:AttributeStatement>
```

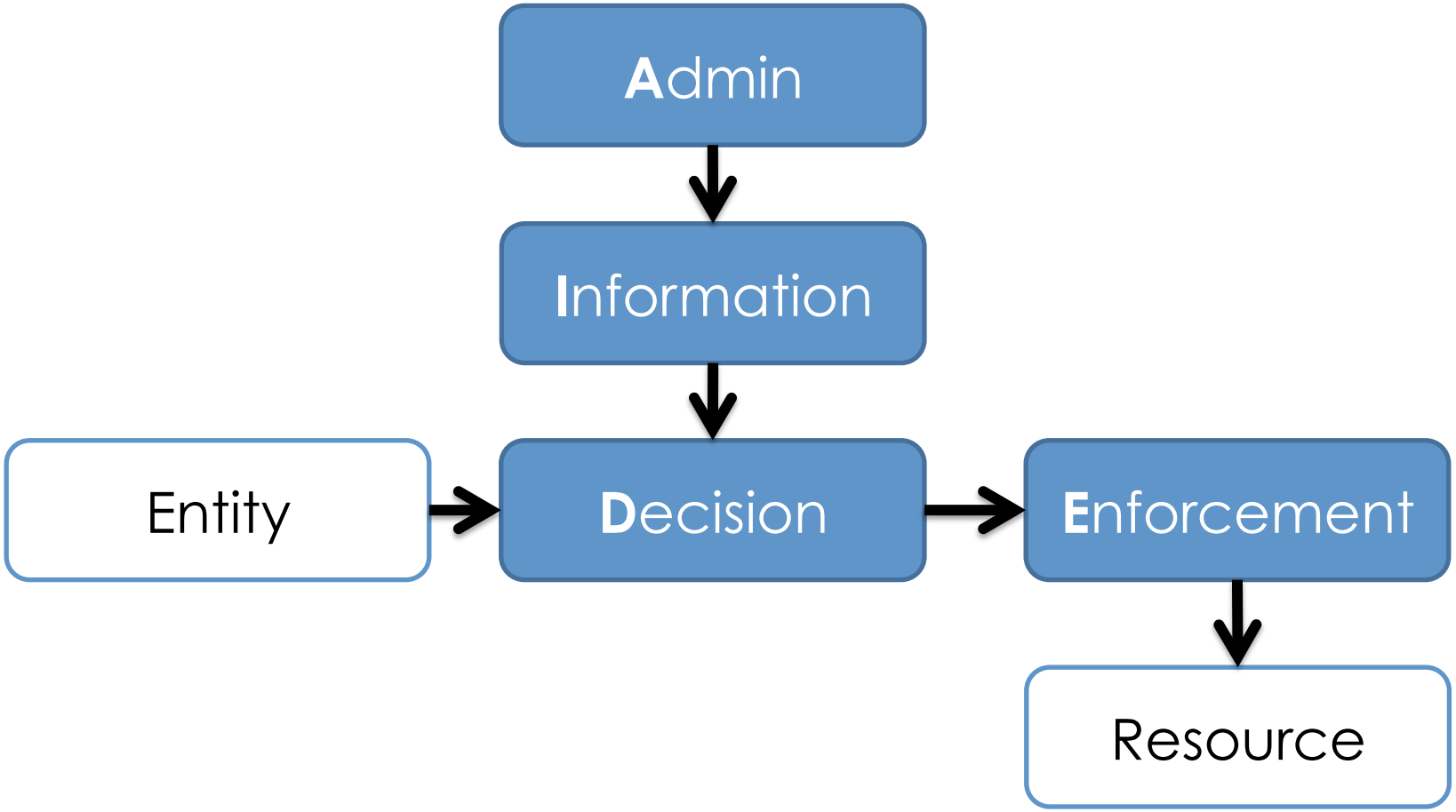
Authorization: Entitlements – Oauth 2 Token

```
{"access_token":"ACCESS_TOKEN",
    "token_type":"bearer",
    "expires_in":2592000,
    "refresh_token":"REFRESH_TOKEN",
    "scope":"read",
    "uid":100101,
    "info":{"name":”Rick Grimes",
        "email":”Rick@joes.com"}
}
```

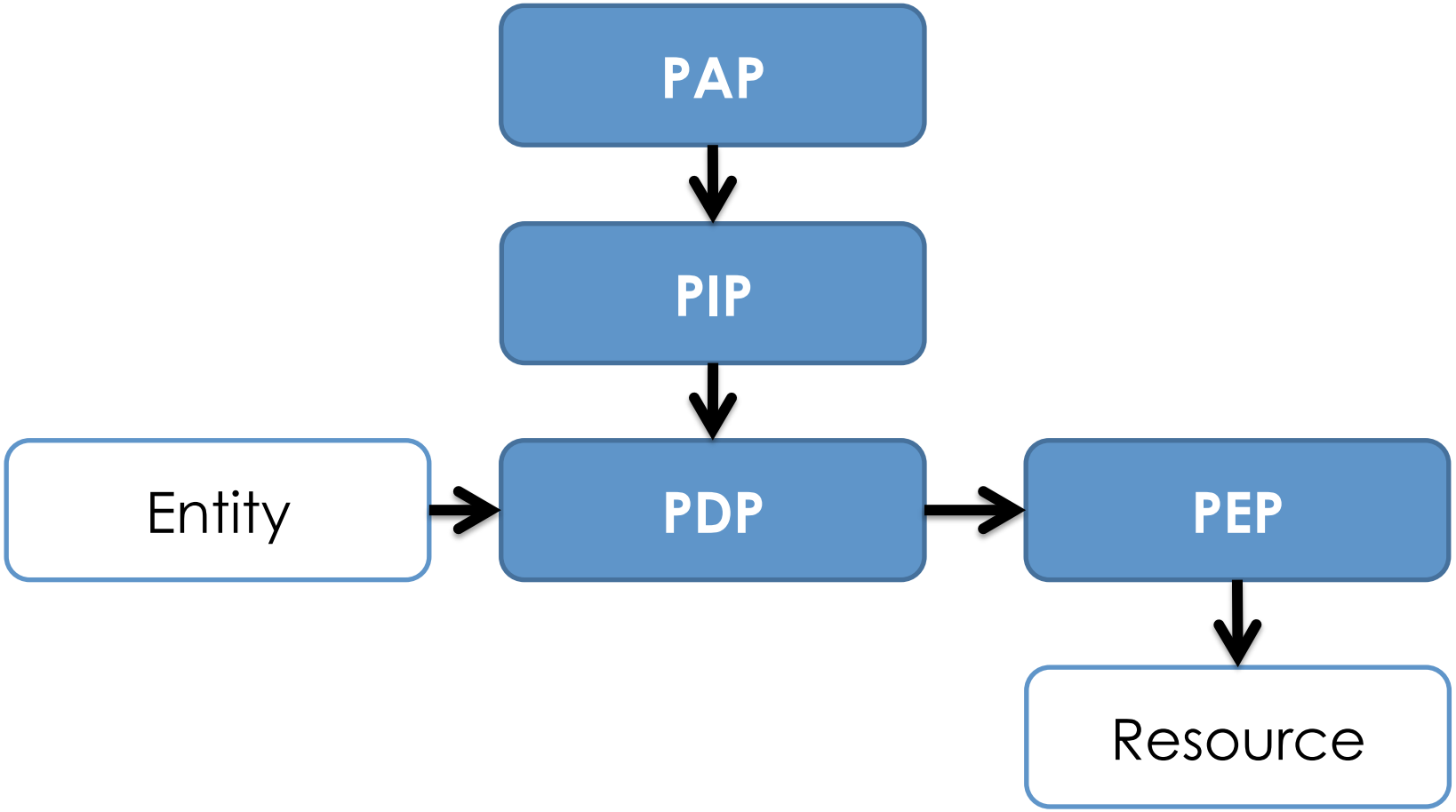
Authorization: Federation of Entitlements



Authorization: Points of the Basic Model



Authorization: Policy Model with P's



Disco Night
At
Joe's Burrito Barn!

Authorization: All-in-one

PIP

PDP

PEP

Resource

Authorization: Ticket System/Certificates

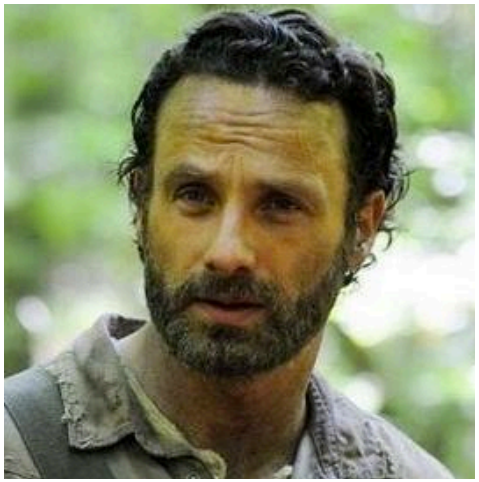
->PIP

PDP

PEP

Resource

Authorization: Distributed model



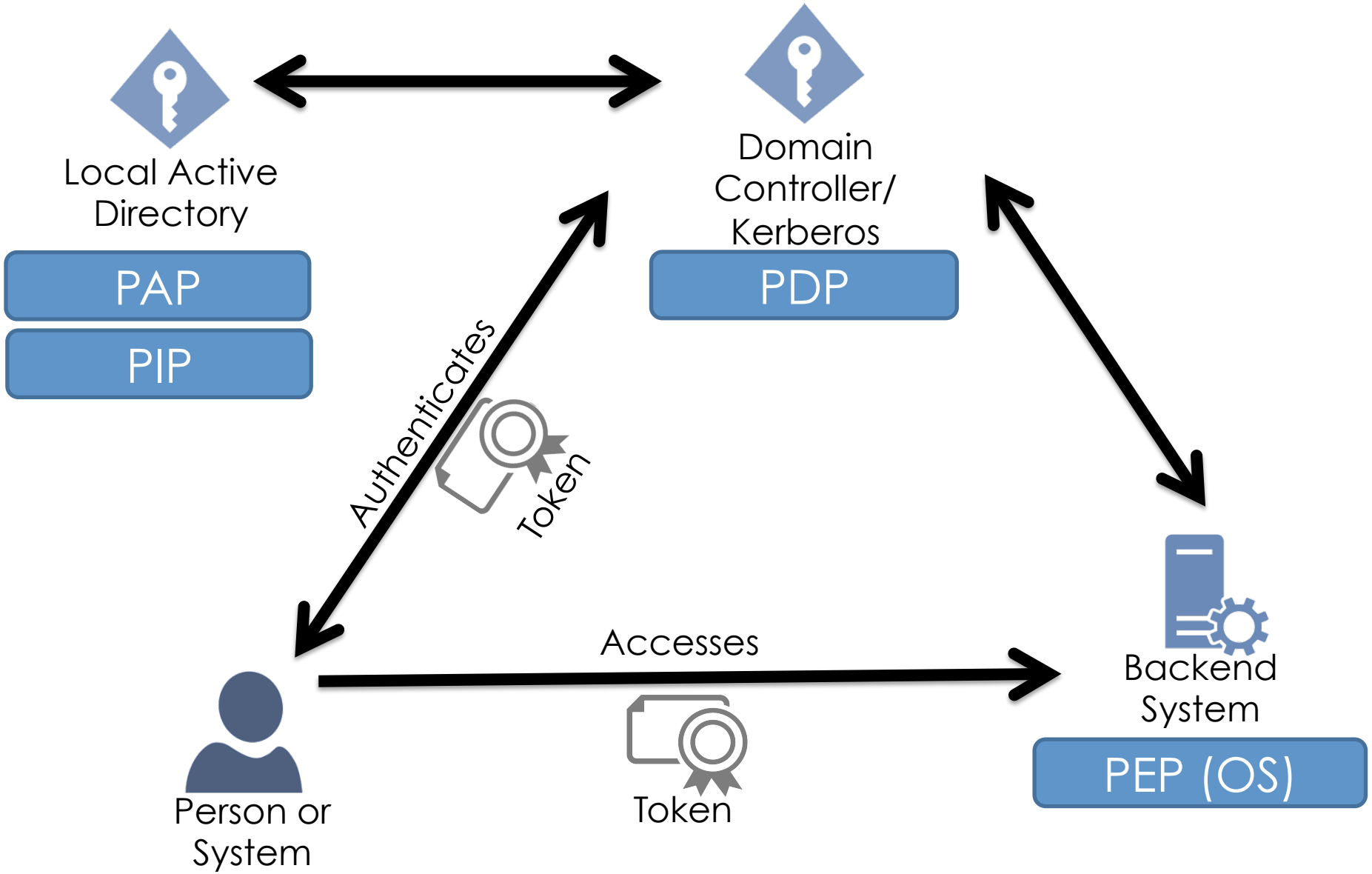
PIP

PDP

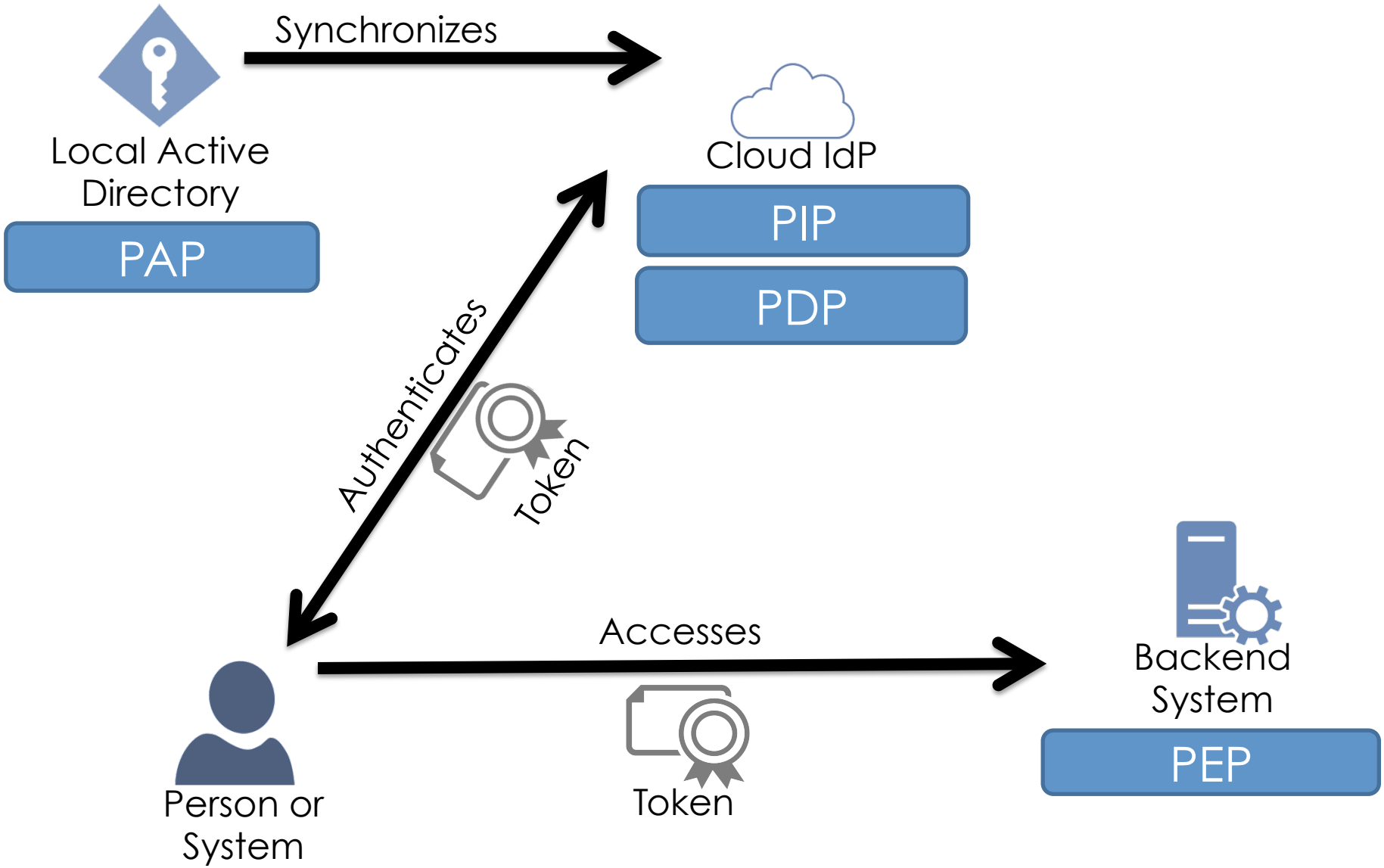
PEP

Resource

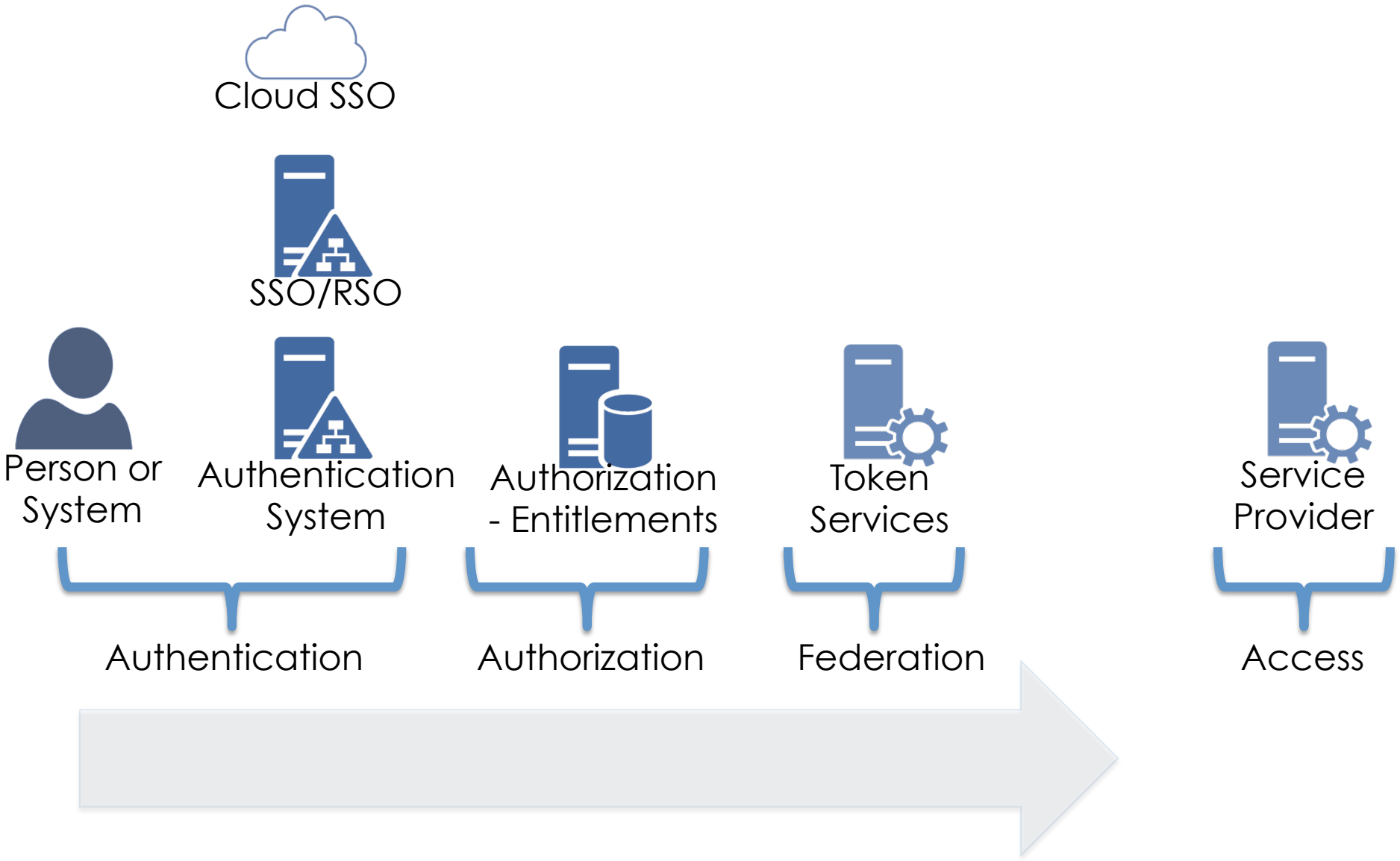
Authorization: Active Directory/Kerberos



Authorization: Cloud SSO Model



Access Control Runtime



Privileged Access Management (PAM)

PAM is the approach, processes, and technology that helps control, audit, and reduce risk when administrative actions.

1. Identify administrative actions
2. Identify roles
3. Separate those from others
4. Monitor and audit actions
5. Temporary passwords
6. Technology
7. Automate to reduce the need
8. Segment operations
    1. Networks
    2. Consoles
    3. Virtualization/VDI

VMWare Administrator
sudo
AWS Administrator
Active Directory Admin
Network Hardware Admin
Workday Administrator
SFDC Administrator

Intelligence

Intelligence is the process of gathering data, analyzing data, and monitoring data in order to increase the level of security, and efficiency in the environment.

1. Log information
2. Monitor and alert
3. Analyze and correlate
4. Audit

Additions to privileged groups
Creation of admin accounts
Creation and quick deletion
Inactive accounts
Inactive groups
Correlate network to IAM
Determine normal actions

Summary

Access Management

1. Establish standards
2. Understand your security approach
3. Resources, Entitlements, & Roles
4. Identities and Attributes
5. Use a single directory
6. Repeatable workflows – automate
7. Attestation/Monitoring

Access Control

1. Establish standards
2. Centralize your authentication
3. Try to use Policy-based or Rules-based authorization when possible
4. Treat Federation as a foundational element
5. Tie in Intelligence from the beginning

PAM

1. Inventory privileged actions/roles
2. Put administrative controls in place
3. Put technical controls in place
4. Automate, monitor

Intelligence

1. Centralize your intelligence
2. Integrate intelligence from the beginning
3. Work closely with Network Security
4. Look at Open Source technologies

IAM Complicated

Why you need to know about IAM

Thanks!

Secret Chipmunk

Ron Parker
@scmunk
http://www.secretchipmunk.com