What Constitutes an Authoritative Source?

Roger Westman, CISSP

September 2, 2009

Case: 09-3195
Approved for Public Release.
Distribution Unlimited

MITRE

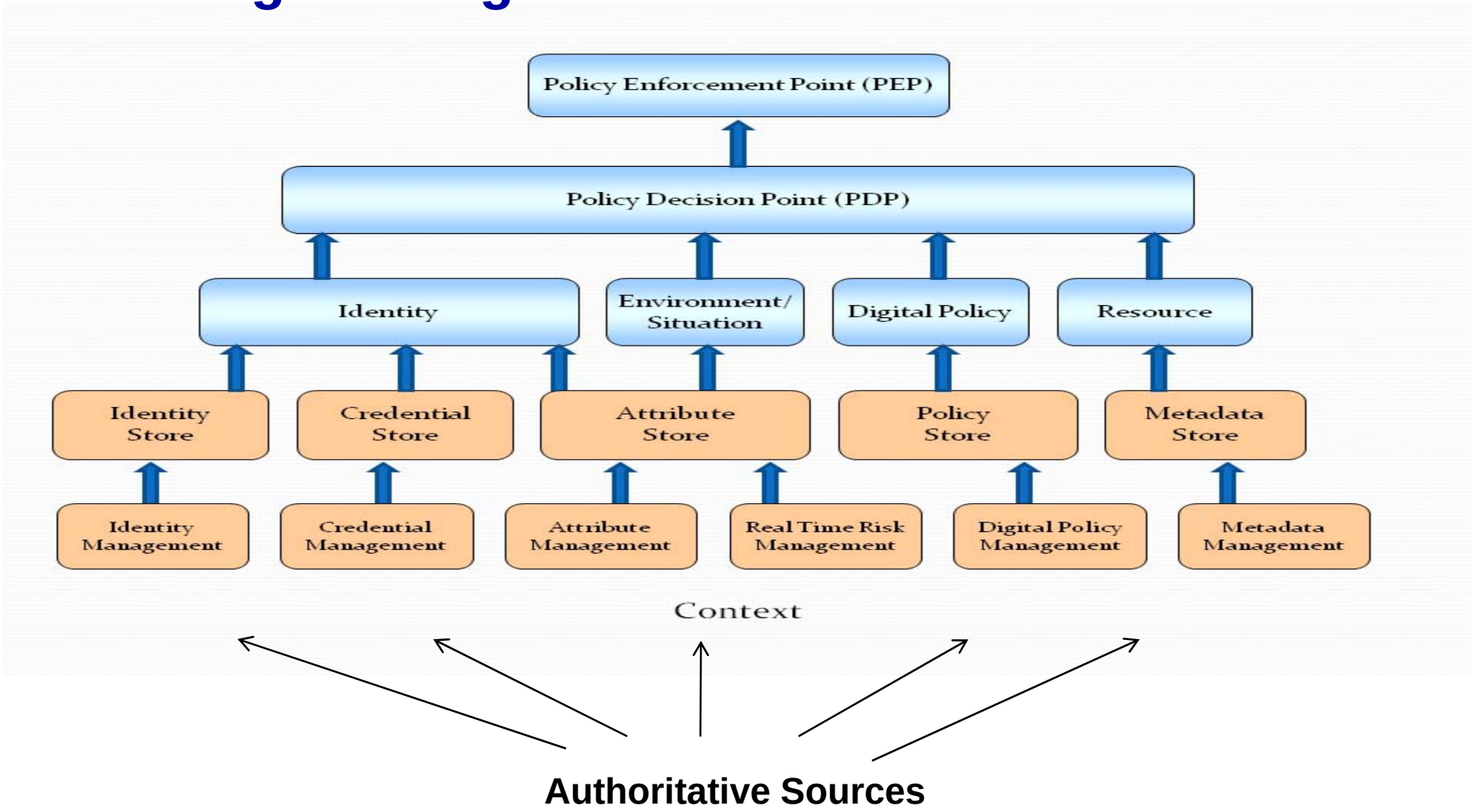
Agenda

- Authoritative Sources Relationship within the Privilege Management Framework
- Authoritative Source Considerations
- Proposed Definitions
- Authoritative Sources Levels
- Types of Attributes
- Proposed Next Steps
- Summary

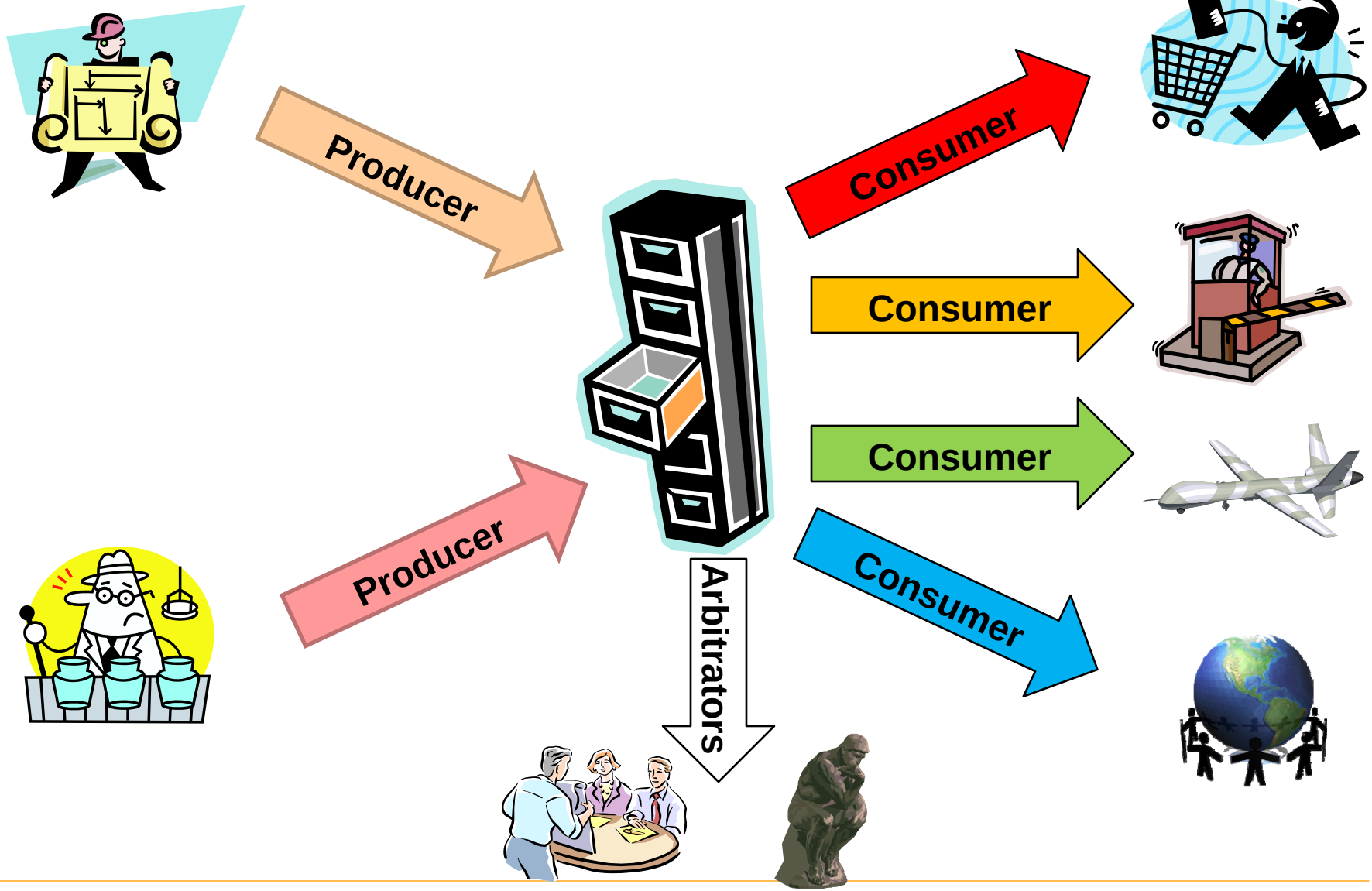
Purpose, Assumptions, and Constraints

- **Purpose**
  - Propose a starting definition for the Community
  - Highlight some known items of interest
- **Assumptions**
  - Privilege Management focus
  - Audience has understanding of access control
- **Constraints**
  - Not addressing information management aspects of authoritativeness
  - Not addressing all Producer vs. Consumer authoritative issues
  - Not addressing all technical implementation issues

Authoritative Sources Relationship within the Privilege Management Framework



Who Decides What Is Authoritative?



Today's Approach – Authoritative Source Selection

- It is on the Internet, so it must be correct
- The Boss said it was ok
- John told me it had useful information even though Sandi disagreed
- The Systems Integrator delivered it with the system
- It was the only source that would allow a connection
- We do not need an Authoritative Source; our data comes from the Human Resources

Authoritative Source Considerations

- Authoritative normally refers to legal authority to collect
- Authoritative also needs to include
  - Why was the data collected (e.g., Priv Mgt or Human Resources)
  - Data usage (What is the data to be used for?)
  - Correctness of the data
  - Accessibility of the data
  - Availability of the data
  - Freshness of the data
  - Lifecycle management process for the data
  - Cache-ability of the data
  - Can data be used to derive other data?
  - Governance process used to declare “authoritative” for a specific environment
    - Use this type of data
    - Criteria for authoritativeness
    - Use this as source of data

Existing Related Definitions

- **CNSSI 4009 (glossary), OASIS, ITU: not explicitly defined**
- **Medical, Financial Communities: Not found (limited search)**
- **AATT: Authoritative Attribute Source (AAS): The official source that originates and maintains the attributes of entities. [AATT]**
- **DoD 8320.2: Authoritative Source: A source of data or information that is recognized by members of a Community of Interest (COI) to be valid or trusted because it is considered to be highly reliable or accurate or is from an official publication or reference (e.g., the United States (U.S.) Postal Service is the official source of U.S. mailing ZIP codes). (DoD 8320.2)**

There is no USG, industry, or standards body agreed-to Authoritative Source definition

Proposed Definitions (1 of 2)

- **Authoritative Source:**

  A managed repository of valid or trusted data that is recognized by an appropriate set of governance entities and supports the governance entity's business environment.

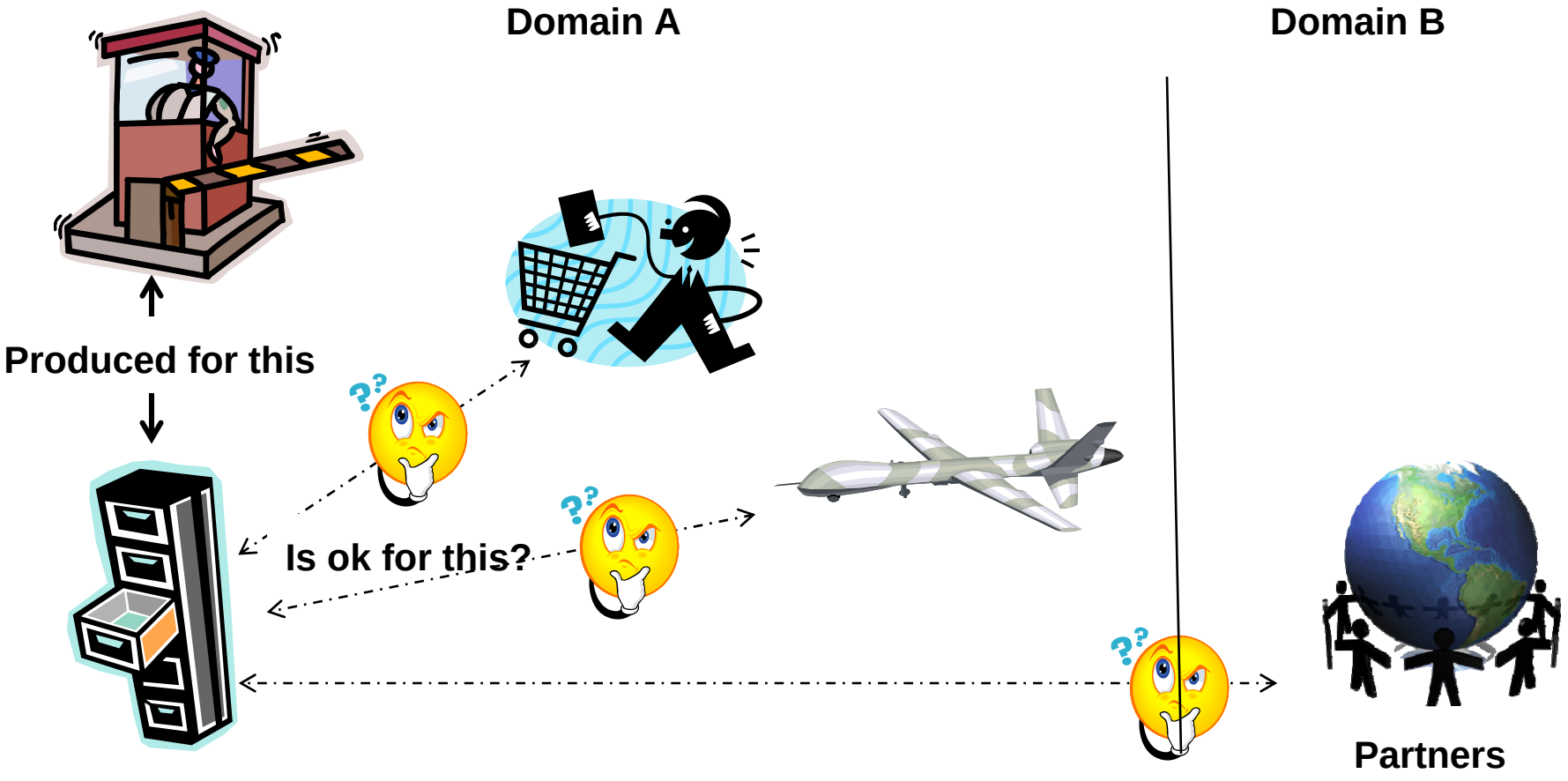
- **Each governance entity establishes its criteria in the following areas, which may vary per business environment, subset of operations within the business environment, and by Authoritative Source.**
  - **Data that needs to be collected**
  - **Data that is collected**
  - **Data quality (accuracy, reliability, freshness, …)**
  - **Data usage (aka what data can be used for)**
  - **Assurance requirements**
  - **Compliance requirements**

Proposed Definitions (2 of 2)

- **Authoritative Data: Data coming from an Authoritative Source**
  - **Note: Authoritative data, authoritative information, and authoritative attribute can be considered interchangeable terms.**
- **Attribute Service: A service that provides a consumer of data with a common access point to authoritative data obtained from one or more Authoritative Sources.**

Governance Aspects

- Producer: Who can use this data?
- Consumer(s): Is this data good enough for my use?
- Governance processes must manage this trade space



Authoritative Source Does NOT Default to a …

- Does not default to
  - A Human Resources system
  - A security database
  - A single centralized entity

- However, an Authoritative Source can be
  - A Human Resources system
  - A security database
  - A specialized Privilege Management System
  - A department's managed set of data
  - A project's managed set of data
  - An Excel spreadsheet

The set of Authoritative Sources depends on your environment

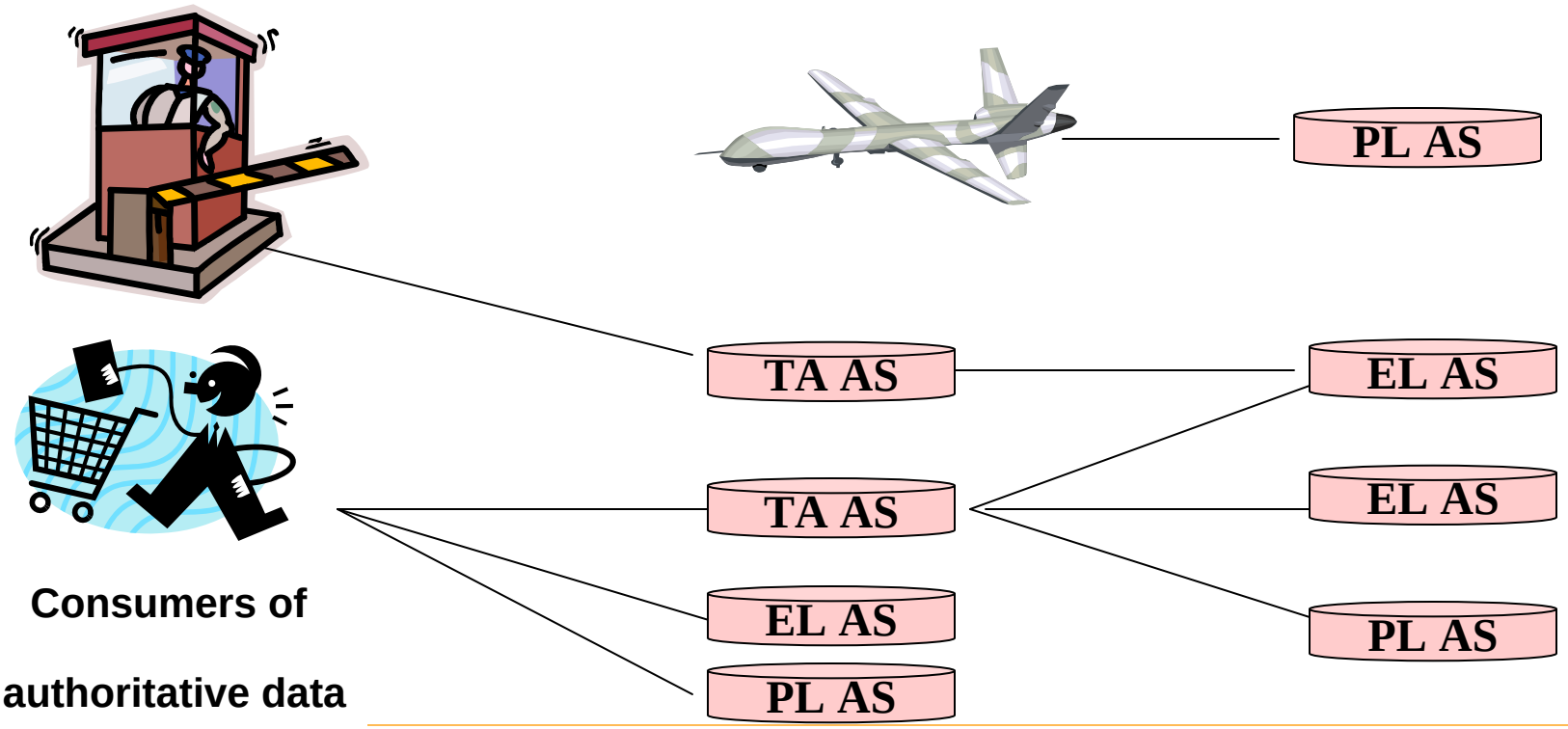
Authoritative Source Implementation Options

- One size does not fit all
- Centralized, Distributed, Federated
  - Your environment influences the approach
- Technical implementation approaches vary
  - A person providing real-time data
  - A paper list
  - Electronic spreadsheet
  - Database management system
  - Directory
- An attribute source does NOT default to a Directory
  - But a directory can be an Authoritative Source

Implementation details depend on your environment.
Most likely multiple approaches within your environment.

Authoritative Sources Level Concept

- At least three known levels
  - Enterprise Level (EL) Authoritative Source
  - Project Level (PL) Authoritative Source
  - Trusted Aggregator (TA) Authoritative Source
- Does not mean one level is more trusted than another level



Enterprise Level (EL) Authoritative Source

- EL Authoritative Source contains a set of attributes that covers that Community's operating environment
  - Is ground truth for the attribute within an enterprise?
- Protection Requirements
  - Must satisfy a base set of Authoritative Source requirements
  - Will have more than a project-level Authoritative Source
- EL Authoritative Source can be
  - Centralized
    - Only one Authoritative Source within that environment
  - Distributed
  - Federated
    - Multiple distributed Authoritative Sources managed IAW Enterprise Policy
- Example of an authorization attribute in an EL Authoritative Source
  - Employee type
  - Example: Employee of the organization, contractor to the organization

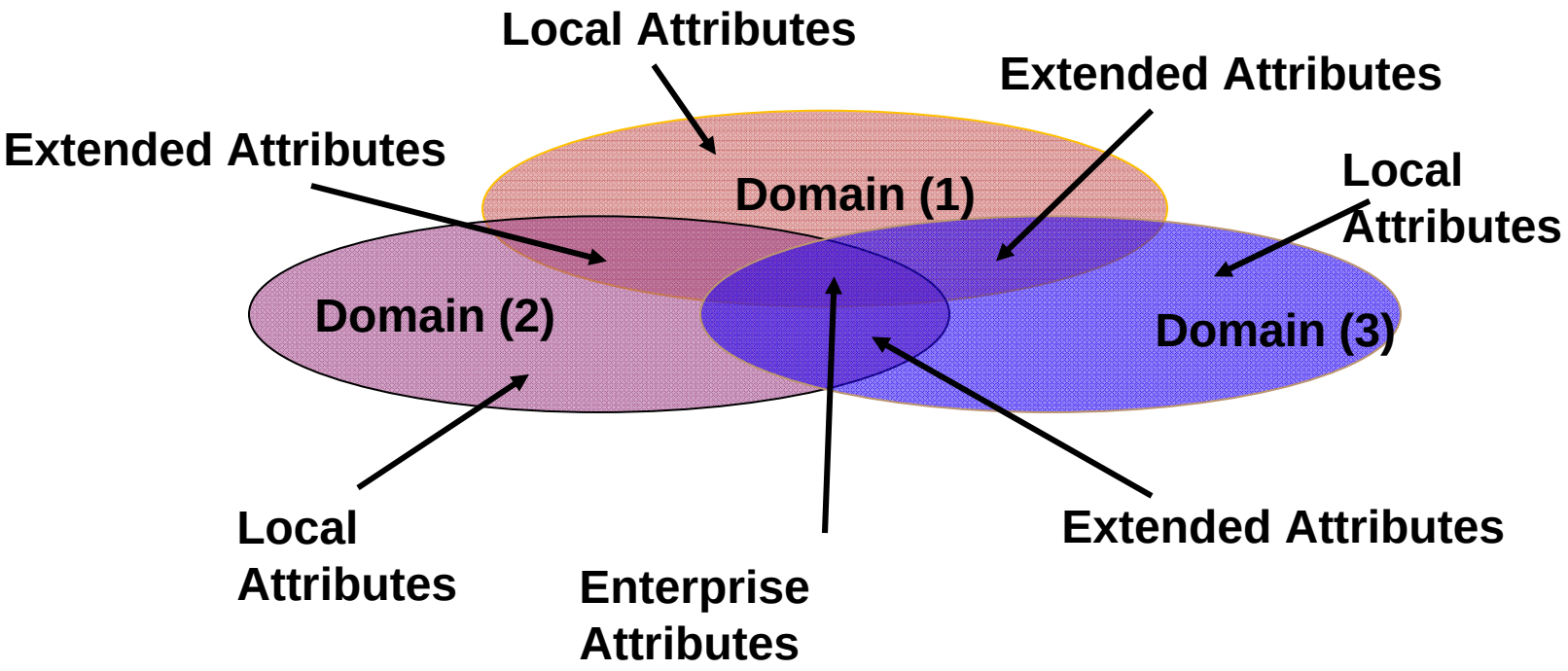
Project Level (PL) Authoritative Source

- Contains the set of attributes that is specific to a set of projects
  - These attributes are not normally at the Enterprise level
- Protection requirements
  - May have fewer requirements than any other Authoritative Source
    - Only affects one project and not the entire organization
- Governance by the project
  - Normally conforms to overall organization's governance guidance
- Implementation approaches vary
  - Unique to that project
  - Supports a set of projects
  - Incorporated into a TA Authoritative Source
- Example of an authorization attribute in an PL Authoritative Source
  - Need-to-Access/Need-to-Know requirement
  - Example: Only the project leader knows which assigned investigator is allowed to "access" case A data

Trusted Aggregator (TA) Authoritative Source

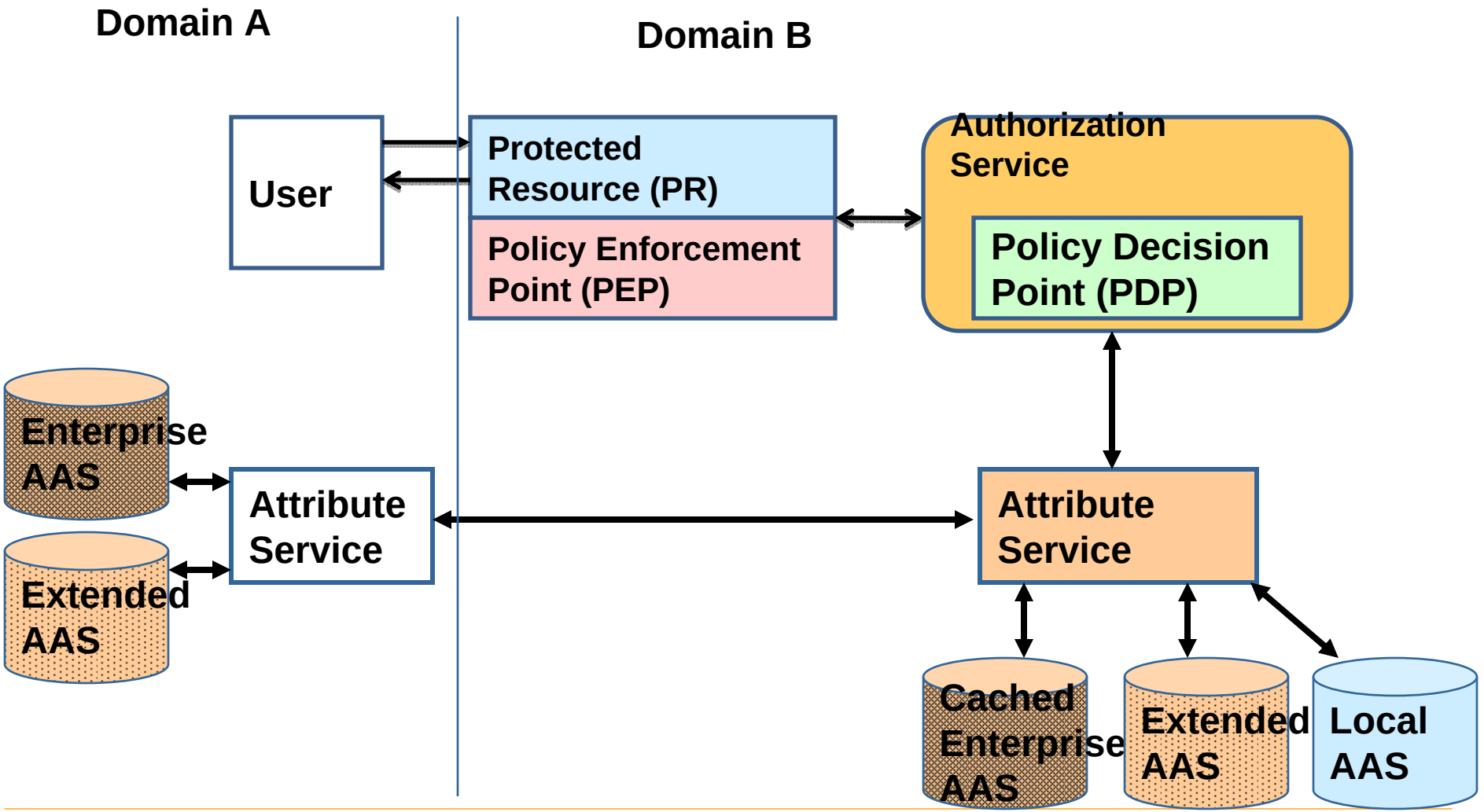
- Acts as a trusted intermediary between the originating Authoritative Source and consumer of authoritative data
  - AKA Attribute Service
- Protection Requirements
  - Must satisfy a base set of Authoritative Source requirements
  - Will have more than a Project Level Authoritative Source
  - Could have more requirements than an EL Authoritative Source
  - Could have additional unique requirements due to aggregation issues
- TA Authoritative Source
  - Can provide better performance, availability, and accessibility
  - Can be used by multiple consumers of authoritative data
  - Can contain authoritative data from multiple Authoritative Sources
- Is considered to be as authoritative as the originating Authoritative Source

Quick Reminder of Different Classes of Authorization Attributes



Enterprise Authorization Attributes – Exchanged by all domains
Extended Authorization Attributes – Exchanged between a subset of domains
Local Authorization Attributes – Never exchanged with any domain

Example of Different Attribute Sources Supporting Access Control Decision Within a Federation



Suggested Next Steps

- Further refine and standardize the Authoritative Source concept
  - Standardize terminology
  - Reach agreement on basic concepts
- Leverage existing guidance and practices to make a Best Practices document that addresses
  - Data quality
  - Information Assurance
  - Governance
- Publish the information in a NIST Special Publication

Summary

- **Proposed definition:**

  Authoritative Source: A managed repository of valid or trusted data that is recognized by an appropriate set of governance entities and supports the governance entity's business environment.

- **An Authoritative Source does not default to**
  - **A single centralized repository**

- **Multiple levels of Authoritative Source**
  - **Enterprise level, Project level, Trusted Aggregator level**

- **Proposed Next Steps**
  - **Refine concept, standardize terminology, and develop guidance**