Access Controls for SSCP®

Kevin Henry CISA, CISSP-ISSMP, SSCP
Pluralsight Author

kevin@kmhenrymanagement.com

Course Introduction

Access Controls

- Access Control Concepts
- The Identity Management Lifecycle

This domain is weighted for 15% of the SSCP examination

Access Controls

Perhaps the whole field of information security could be described as the discipline of access control:

Who can gain access to our assets?

And what can they do when they have access?

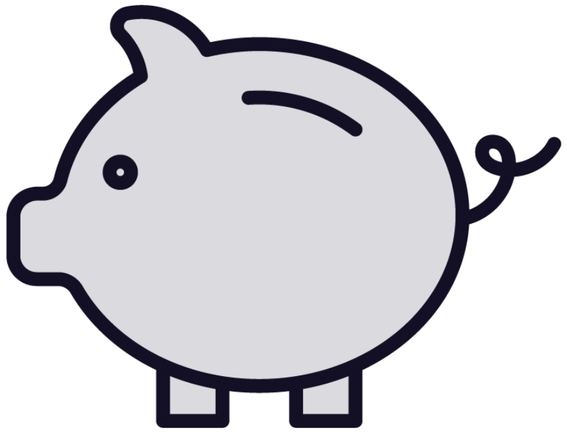
Access Controls for SSCP®

Access Control Concepts

Kevin Henry CISA, CISSP-ISSMP, SSCP
Pluralsight Author

kevin@kmhenrymanagement.com

Reminder: What Are Assets?



Anything of value [to its owner]

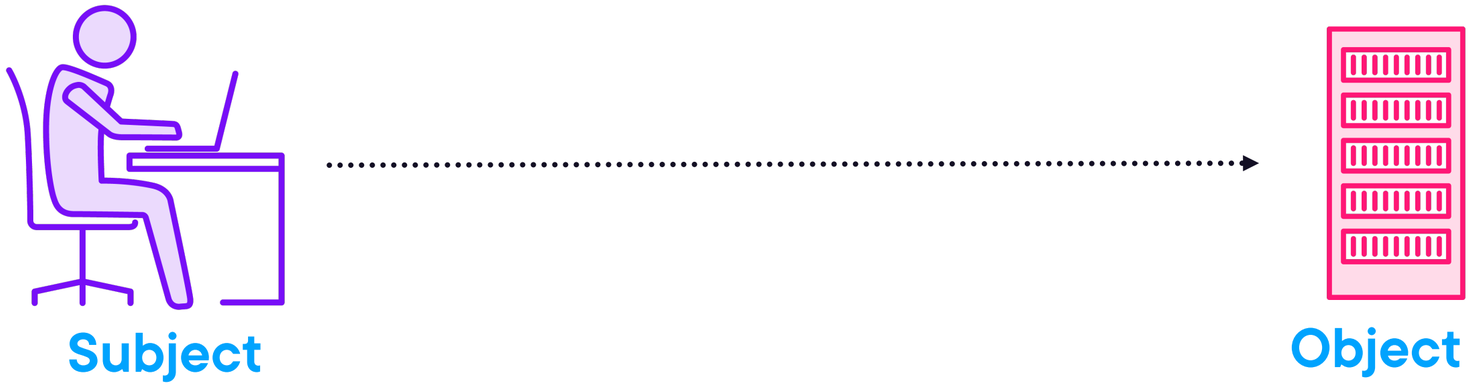
Tangible

- Physical

Intangible

- Data
- Reputation

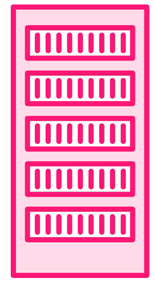
Core Concepts of Access Relationships



Core Concepts of Access Relationships

Subject

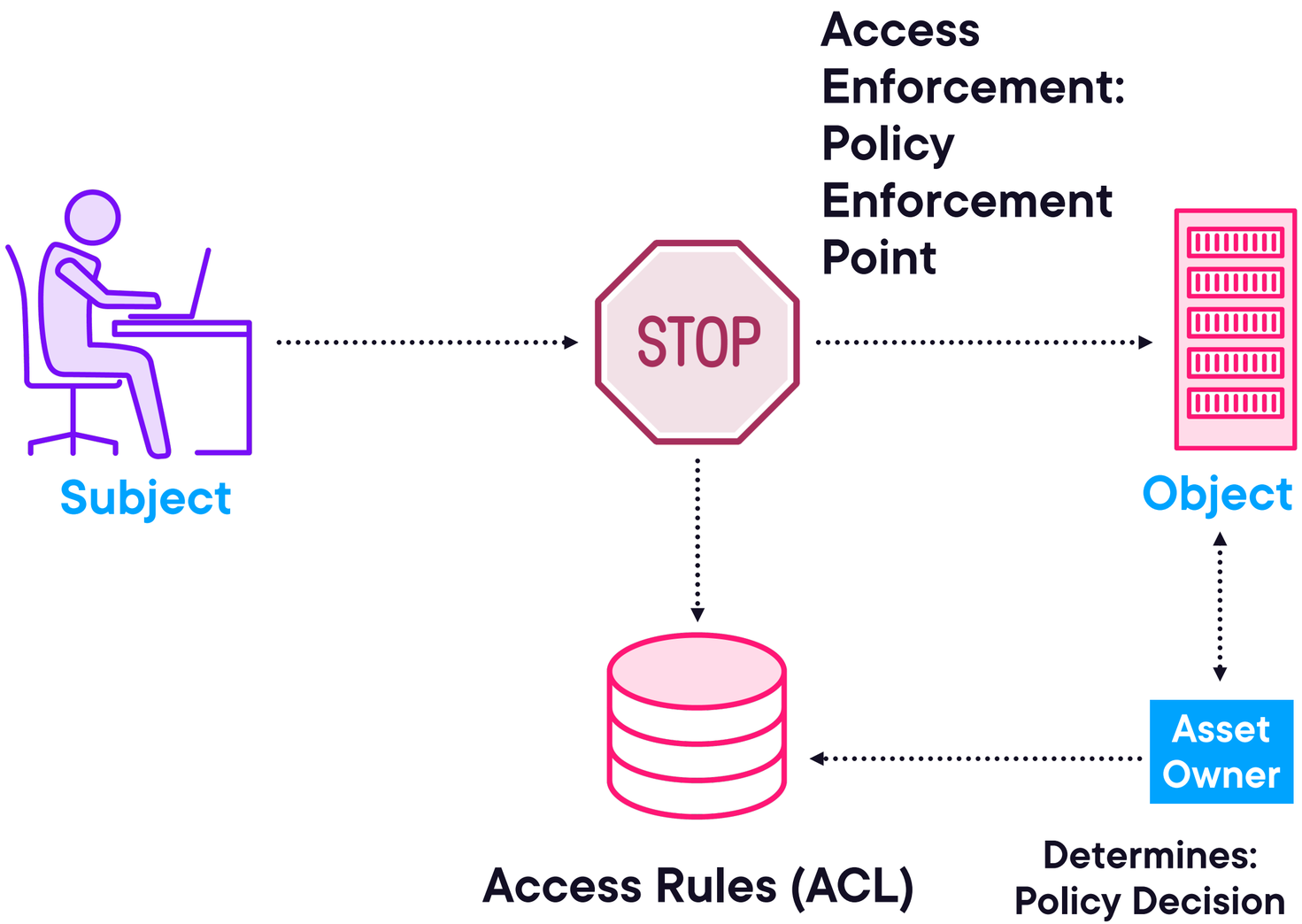
User
Process
Program
Client



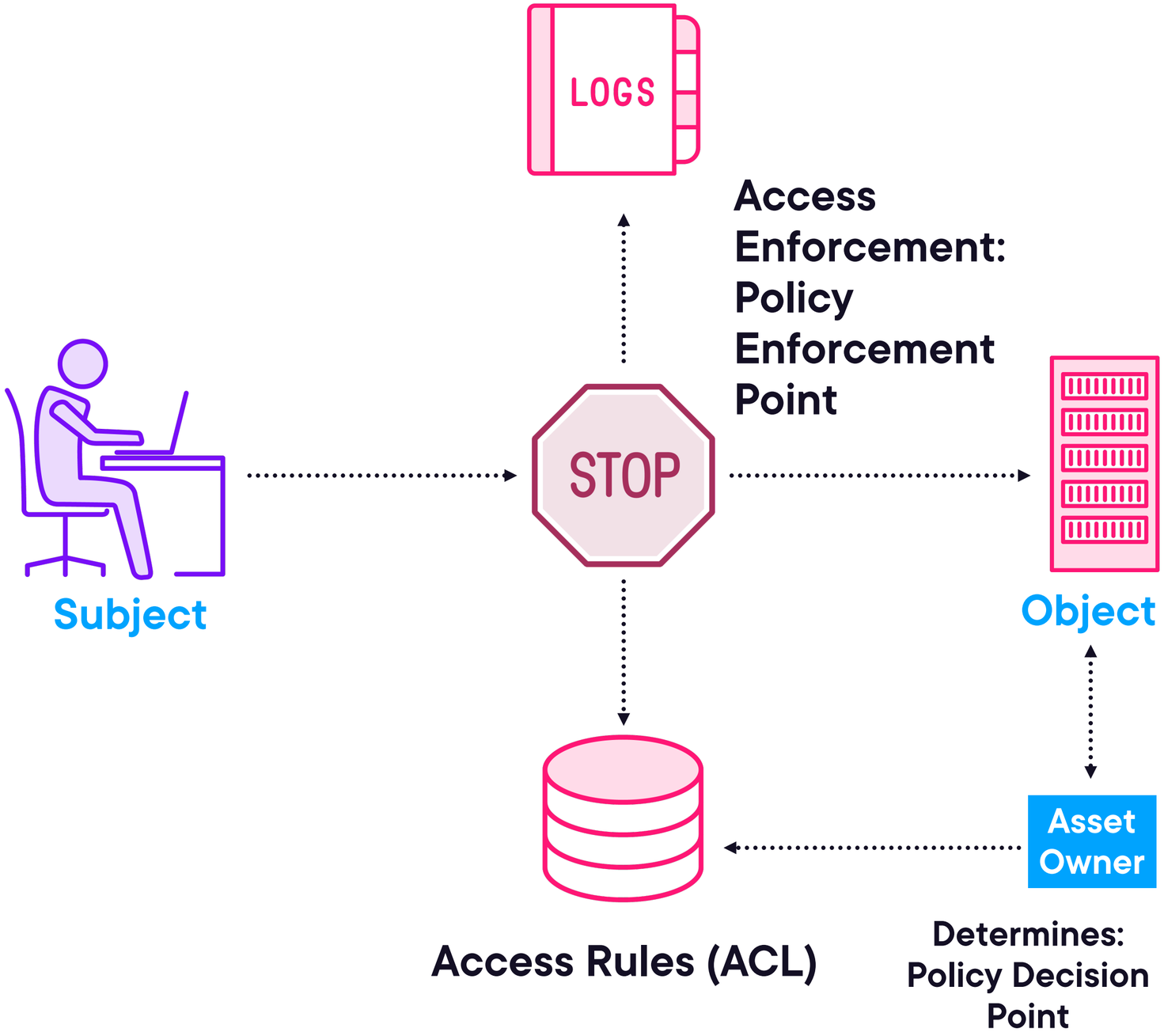
Object

Building
File
Database
Process
Program
Memory
Printer
Server

Access Relationships



Access Relationships



Access Administration Key Concepts

Separation of Duties

Least Privilege

Need-to-Know

Access Control Theory

Mandatory Access Control

High security systems

- Expensive
- Requires labels and separation of duties

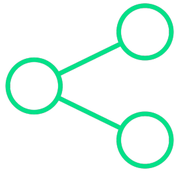
Access permissions are mandated by policy

- Access is only granted if the owner and the policy agree
- Access cannot be delegated

Discretionary Access Control

Most common form of access control

Access permissions are set by the owner



Access rights can be delegated

Common Methods of Access Control

Rule-based access control

RBAC – Role-based access control

Temporal access control

ABAC – Attribute-based access control

Access Control Implementations

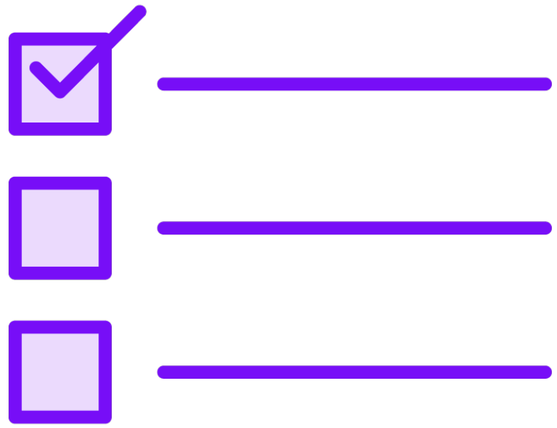
Access Control Structures

Subject-based

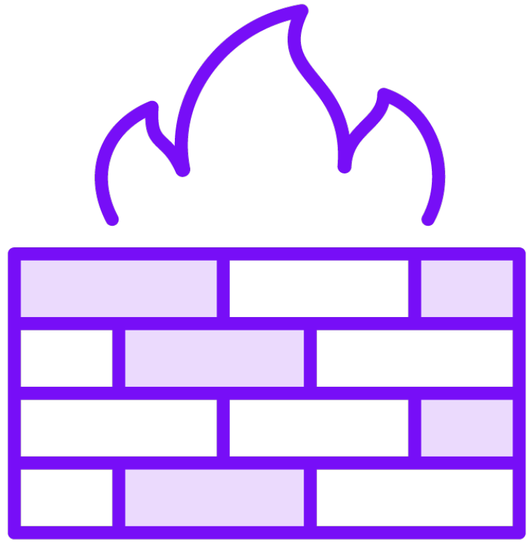
Object-based

Privileged Access Management (PAM)

Rule-based Access Control



Based on list of rules



Firewall rule sets is good example

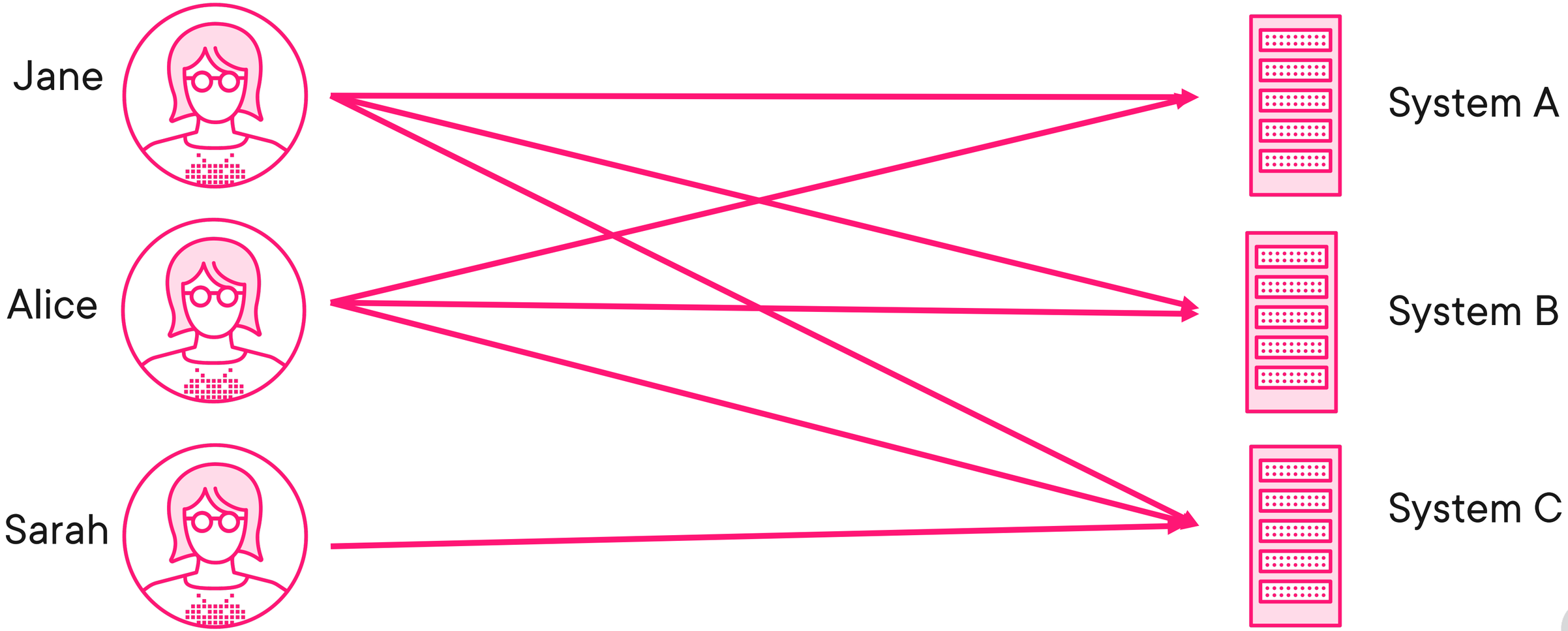
Role-based Access Controls (RBAC)

Based on the user's job position

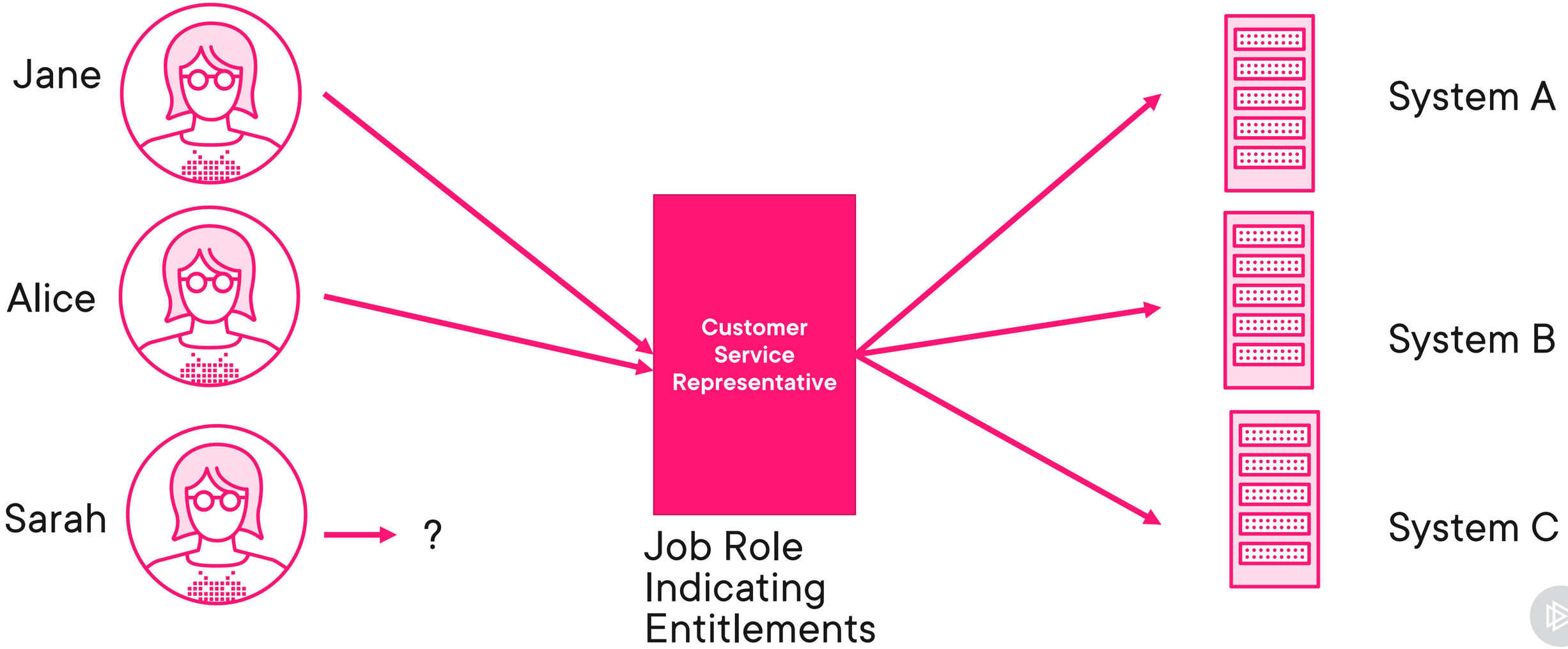
Cost-effect way to implement need-to-know

Easy to enforce through large enterprises with multiple business units

Reasons for RBAC



RBAC Implementation



Attribute-based Access Control

Evaluation and access granted based on attributes

- Entitlements

Flexibility

Decisions based on

- Subject attributes
- Objects attributes
- Environmental conditions
- Formal relationship or access control rule

Temporal Isolation

Separation based on hours of operation

Supports batch processing systems

Key Points Review

The purpose of access control is to protect assets of the organization

Access control requires active management of user permissions

Access is mandated by the owner and through policy