Computer Security: Principles and Practice

Fourth Edition

By: William Stallings and Lawrie Brown

Chapter 4

Access Control

Access Control Definitions 1/2

NISTIR 7298 defines access control as:

> “the process of granting or denying specific requests to: (1) obtain and use information and related information processing services; and (2) enter specific physical facilities”

Access Control Definitions 2/2

RFC 4949 defines access control as:

> “a process by which use of system resources is regulated according to a security policy and is permitted only by authorized entities (users, programs, processes, or other systems) according to that policy”

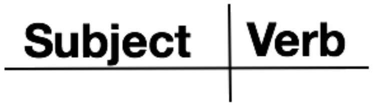
But first …
a journey back to the fourth grade

- Do you remember how to Diagram English Language Sentences?

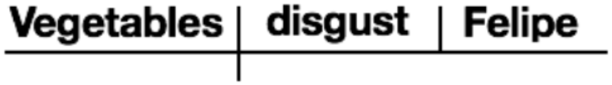
Part 2

Diagramming Sentences

1 **Draw a horizontal line with a small vertical line through the middle.** To the left of the vertical line, write your subject. To the right of the vertical line, write your verb. This is the most basic complete sentence.

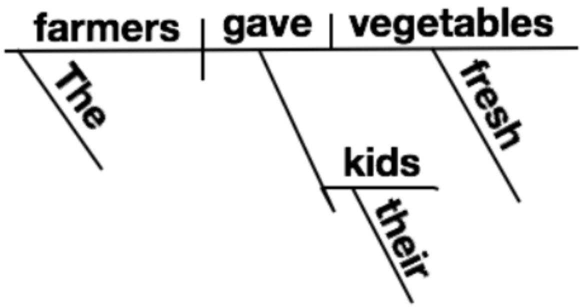


2 **Draw another vertical line stopping at the horizontal line if there is a direct object.** To the right of this line, write the direct object.



- In the above sentence, *Vegetables disgust Felipe*, **vegetables** is the subject, **disgust** is the verb, and **Felipe** is the direct object.

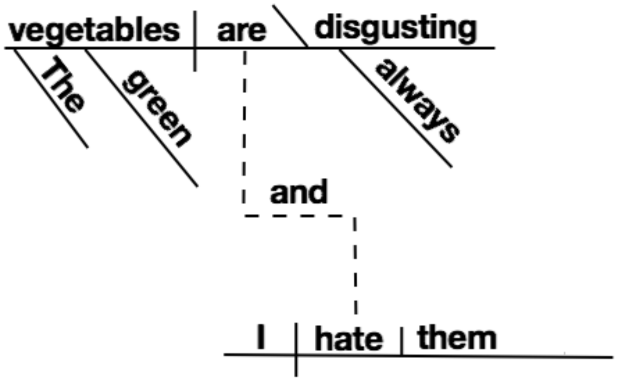
3 **Place indirect objects beneath the verb.** In general, indirect objects could take a preposition and so are drawn with a diagonal line coming off of the word they modify. See step 6 for prepositions.



- In the above sentence, *The farmers gave their kids fresh vegetables*, **farmers *is the subject,*** *gave* is the verb, **vegetables** is the direct object, **kids** is the indirect object, **the** is an article, **their** is a possessive pronoun, and **fresh** is an adjective modifying *vegetables*.

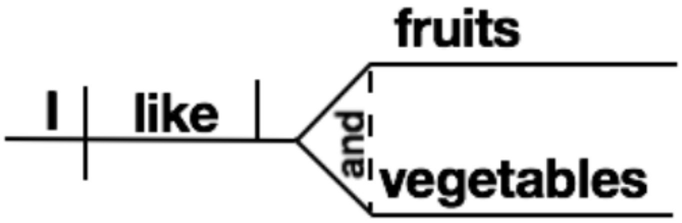
7 Determine how any conjunctions are being used.

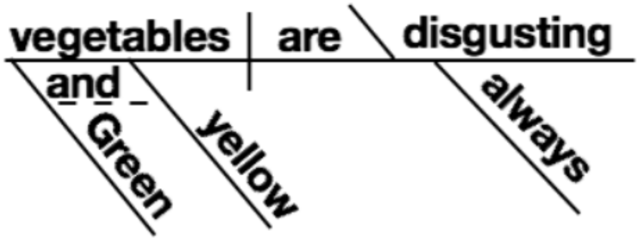
- If the sentence is a compound sentence made up of two independent clauses, the coordinating conjunction will connect via a bent, broken line.



  - In the above sentence, *The green vegetables are always disgusting, and I hate them*, there are two independent clauses. **Vegetables** is the subject of the first clause, **are** is a linking verb, **disgusting** is the predicate adjective, **the** is an article, **green** is an adjective, and **always** is an adverb. **I** is the subject of the second clause, **hate** is the verb, and **them** is the direct object (it is a pronoun whose antecedent is *vegetables*). The two clauses are linked by the coordinating conjunction **and**.

- If the sentence is a simple sentence and the conjunction is joining words within it, you will split the line and join it by a broken line, or you will join two existing lines with a broken line.

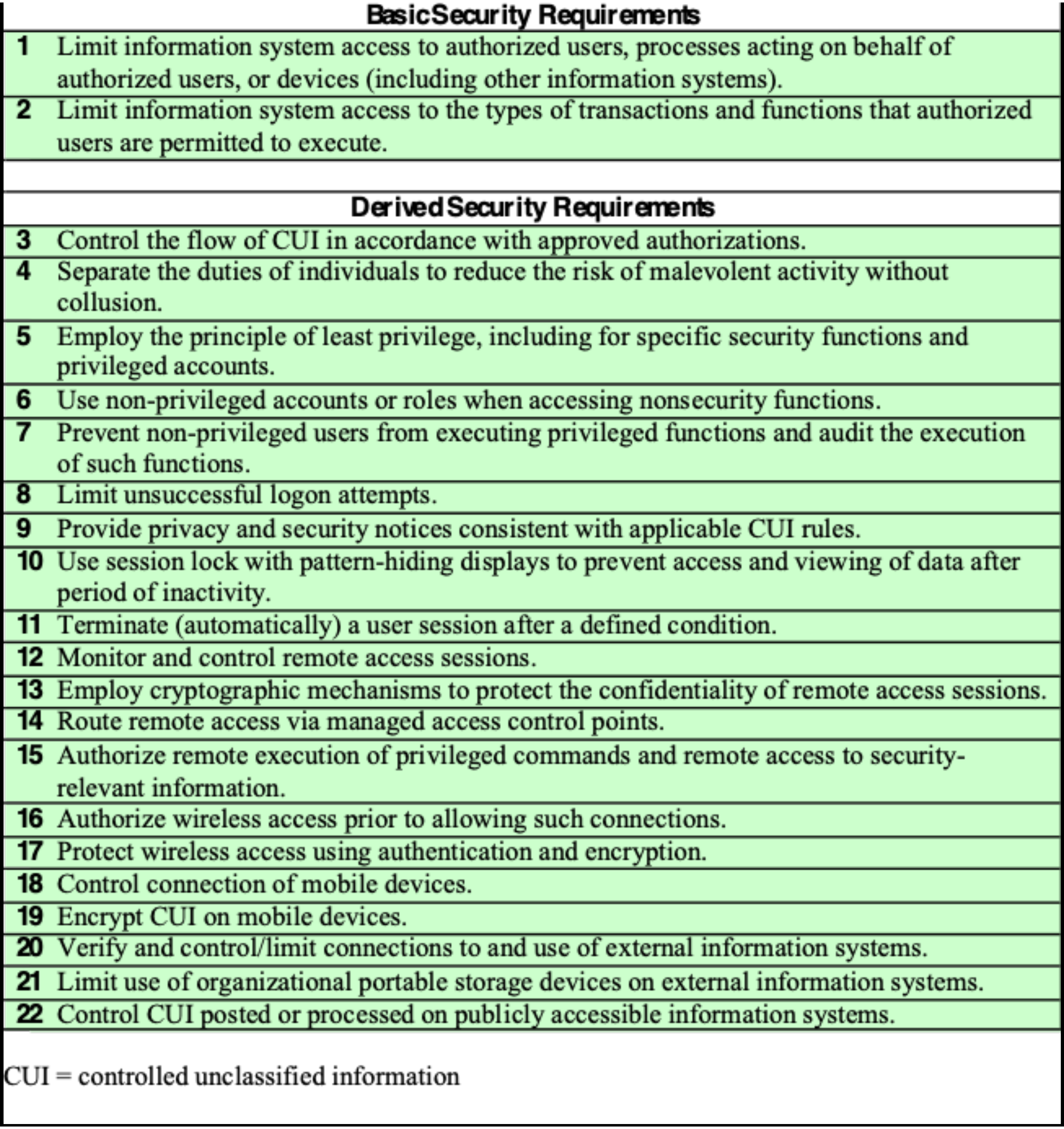




Back to our regularly scheduled program

Table 4.1

Access Control Security Requirements (SP 800-171)



	BasicSecurity Requirements
1	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
2	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
	DerivedSecurity Requirements
3	Control the flow of CUI in accordance with approved authorizations.
4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.
5	Employ the principle of least privilege, including for specific security functions and privileged accounts.
6	Use non-privileged accounts or roles when accessing nonsecurity functions.
7	Prevent non-privileged users from executing privileged functions and audit the execution of such functions.
8	Limit unsuccessful logon attempts.
9	Provide privacy and security notices consistent with applicable CUI rules.
10	Use session lock with pattern-hiding displays to prevent access and viewing of data after period of inactivity.
11	Terminate (automatically) a user session after a defined condition.
12	Monitor and control remote access sessions.
13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.
14	Route remote access via managed access control points.
15	Authorize remote execution of privileged commands and remote access to security-relevant information.
16	Authorize wireless access prior to allowing such connections.
17	Protect wireless access using authentication and encryption.
18	Control connection of mobile devices.
19	Encrypt CUI on mobile devices.
20	Verify and control/limit connections to and use of external information systems.
21	Limit use of organizational portable storage devices on external information systems.
22	Control CUI posted or processed on publicly accessible information systems.

CUI = controlled unclassified information

(Table is on page 107 in the textbook)

Access Control Principles

- In a broad sense, all of computer security is concerned with access control
- RFC 4949 defines computer security as:

> "measures that implement and assure security services in a computer system, particularly those that assure access control service"

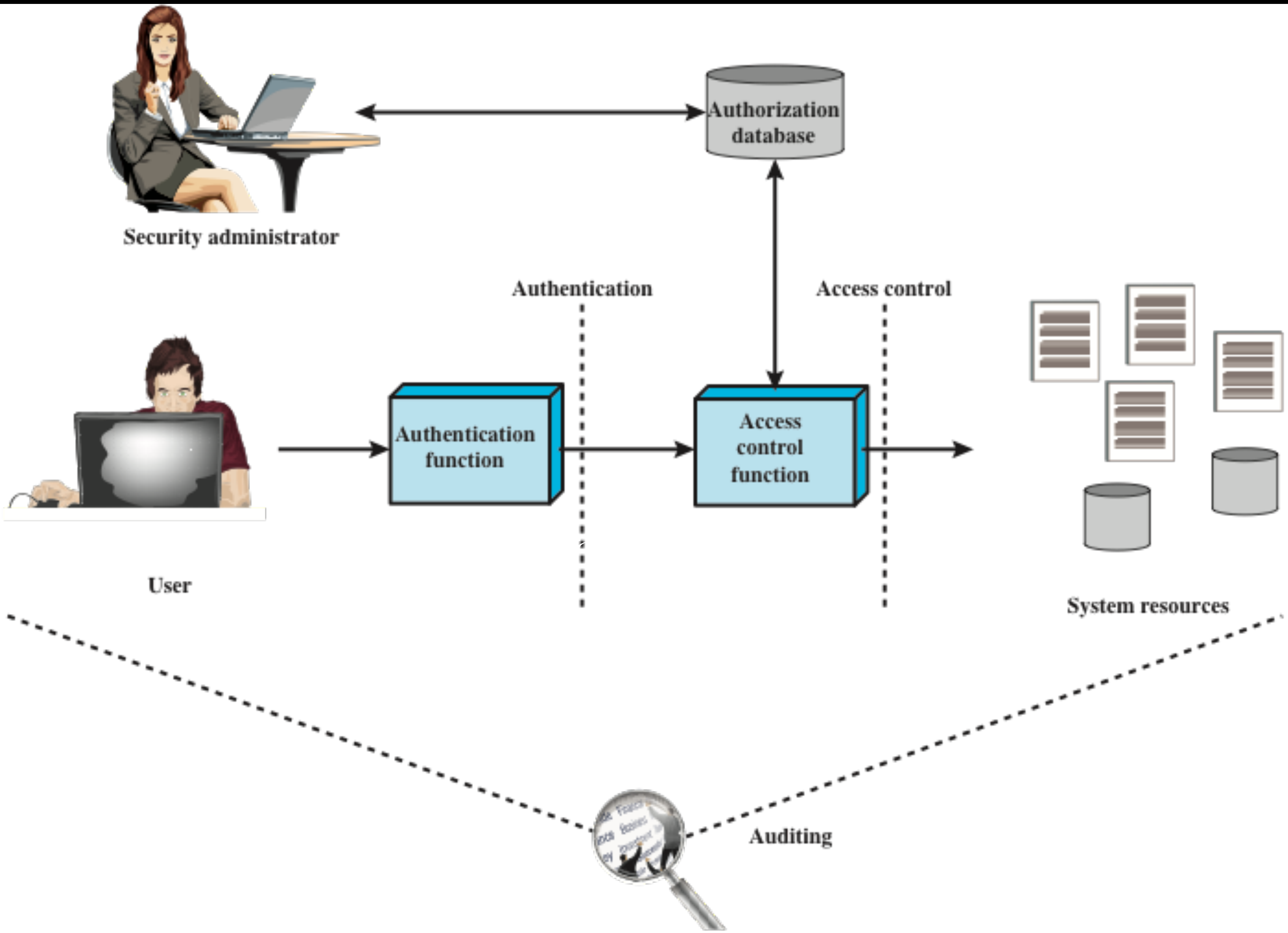


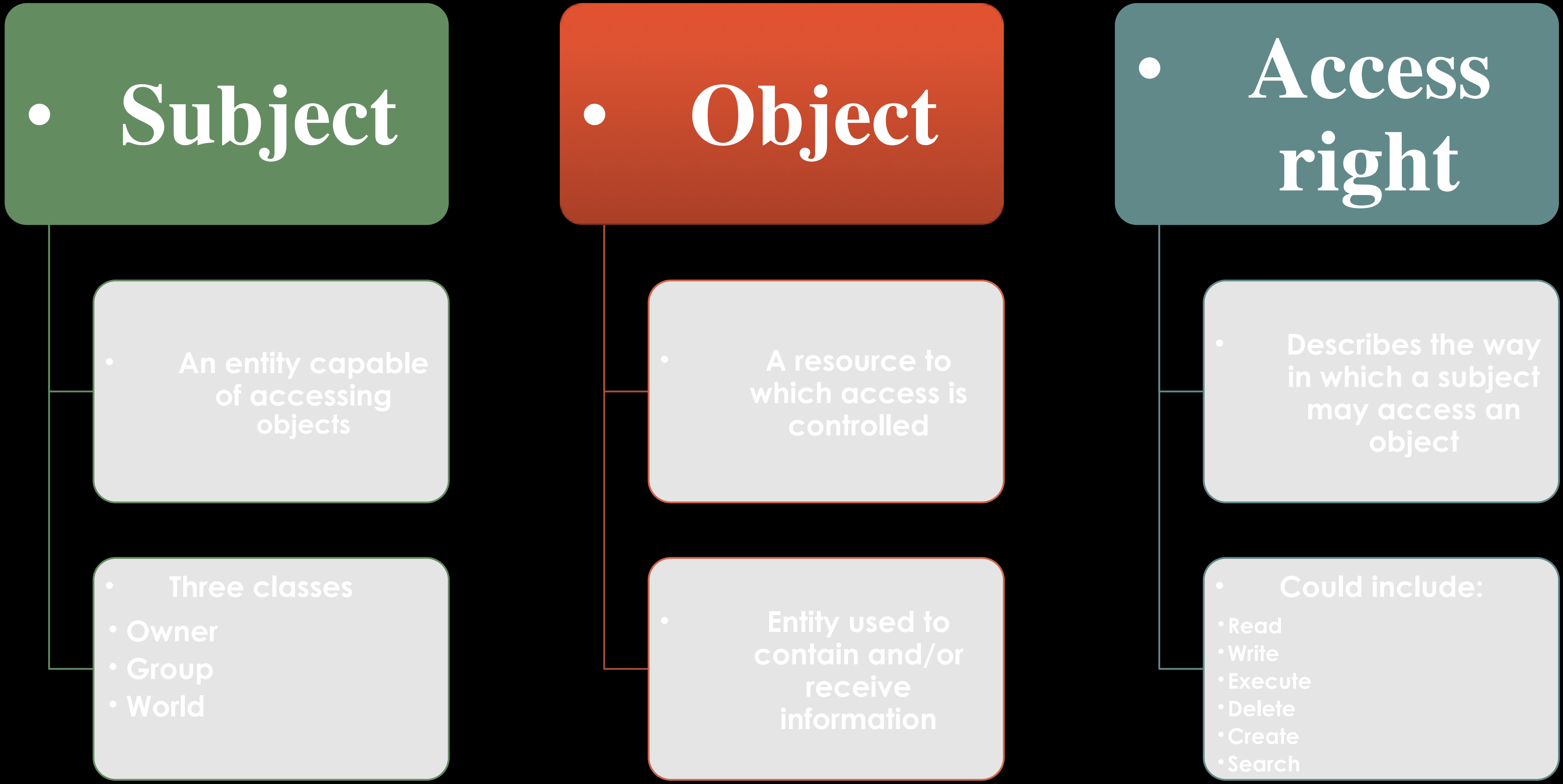
Figure 4.1 Relationship Among Access Control and Other Security Functions

Source: Based on [SAND94].

Access Control Policies

- Discretionary access control (DAC)
  - Controls access based on the identity of the requestor and on access rules (authorizations) stating what requestors are (or are not) allowed to do
- Mandatory access control (MAC)
  - Controls access based on comparing security labels with security clearances
- Role-based access control (RBAC)
  - Controls access based on the roles that users have within the system and on rules stating what accesses are allowed to users in given roles
- Attribute-based access control (ABAC)
  - Controls access based on attributes of the user, the resource to be accessed, and current environmental conditions

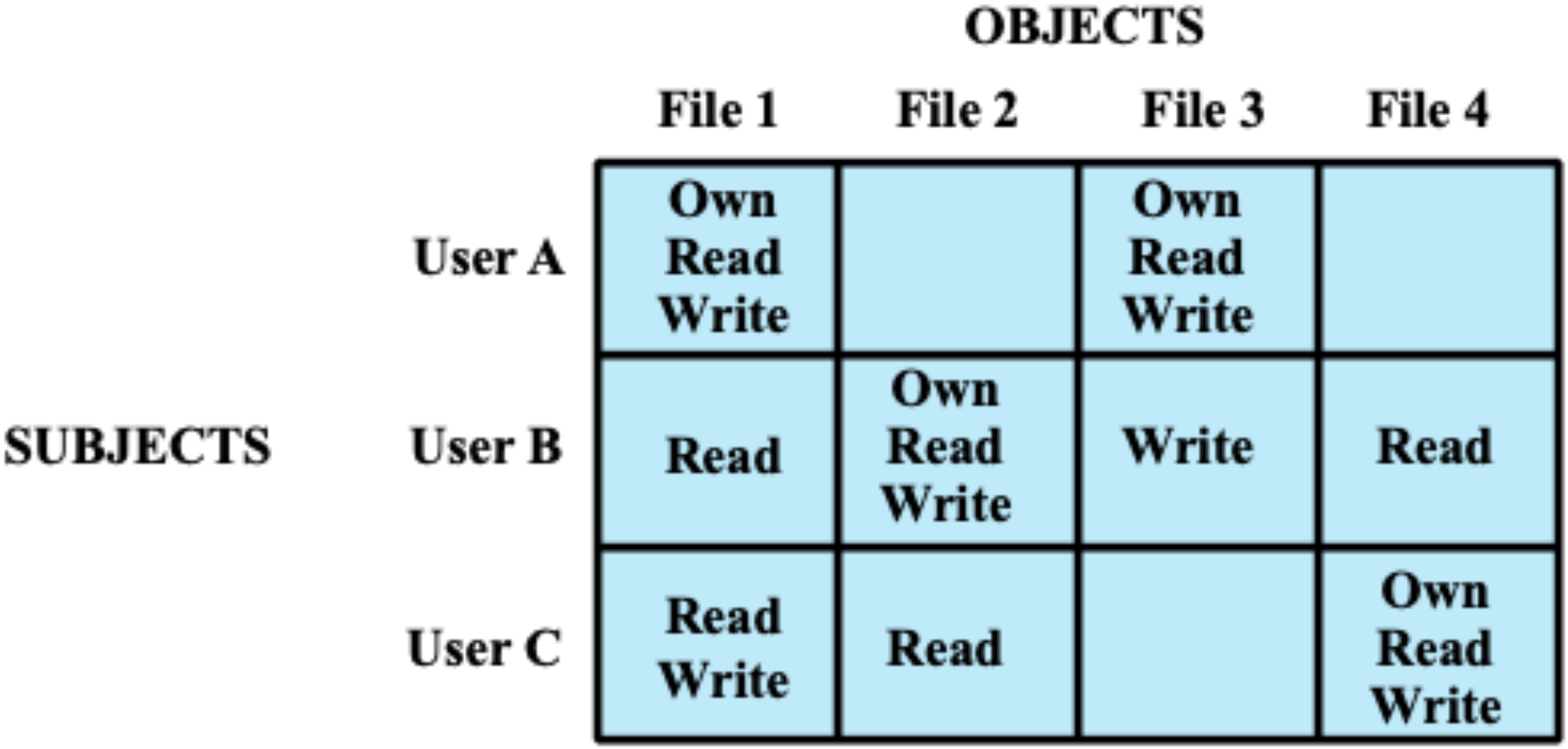
Subjects, Objects, and Access Rights



- Subject
  - An entity capable of accessing objects
  - Three classes
    - Owner
    - Group
    - World
- Object
  - A resource to which access is controlled
  - Entity used to contain and/or receive information
- Access right
  - Describes the way in which a subject may access an object
  - Could include:
    - Read
    - Write
    - Execute
    - Delete
    - Create
    - Search

Discretionary Access Control (DAC)

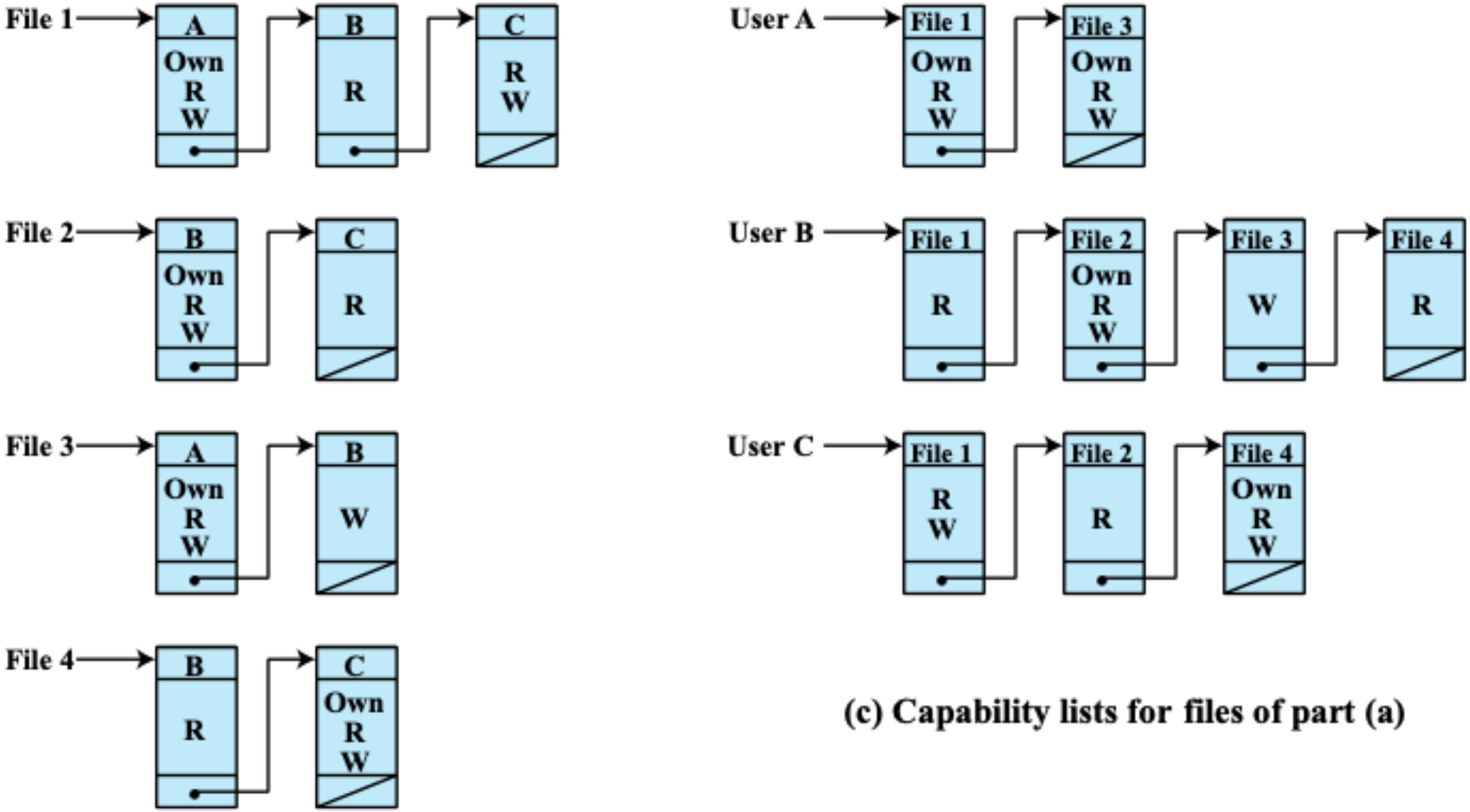
- Scheme in which an entity may be granted access rights that permit the entity, by its own violation, to enable another entity to access some resource
- Often provided using an access matrix
  - One dimension consists of identified subjects that may attempt data access to the resources
  - The other dimension lists the objects that may be accessed
- Each entry in the matrix indicates the access rights of a particular subject for a particular object



		OBJECTS			
		File 1	File 2	File 3	File 4
SUBJECTS	User A	Own Read Write		Own Read Write	
	User B	Read	Own Read Write	Write	Read
	User C	Read Write	Read		Own Read Write

(a) Access matrix

Figure 4.2 Example of Access Control Structures



(b) Access control lists for files of part (a)

(c) Capability lists for files of part (a)

Figure 4.2 Example of Access Control Structures

Table 4.2

Authorization Table for Files in Figure 4.2

Subject	Access Mode	Object
A	Own	File 1
A	Read	File 1
A	Write	File 1
A	Own	File 3
A	Read	File 3
A	Write	File 3
B	Read	File 1
B	Own	File 2
B	Read	File 2
B	Write	File 2
B	Write	File 3
B	Read	File 4
C	Read	File 1
C	Write	File 1
C	Read	File 2
C	Own	File 4
C	Read	File 4
C	Write	File 4

(Table is on page 113 in the textbook)

		OBJECTS								
			subjects		files		processes		disk drives	
		S_1	S_2	S_3	F_1	F_2	P_1	P_2	D_1	D_2
SUBJECTS	S_1	control	owner	owner control	read *	read owner	wakeup	wakeup	seek	owner
	S_2		control		write *	execute			owner	seek *
	S_3			control		write	stop			

* - copy flag set

Figure 4.3 Extended Access Control Matrix

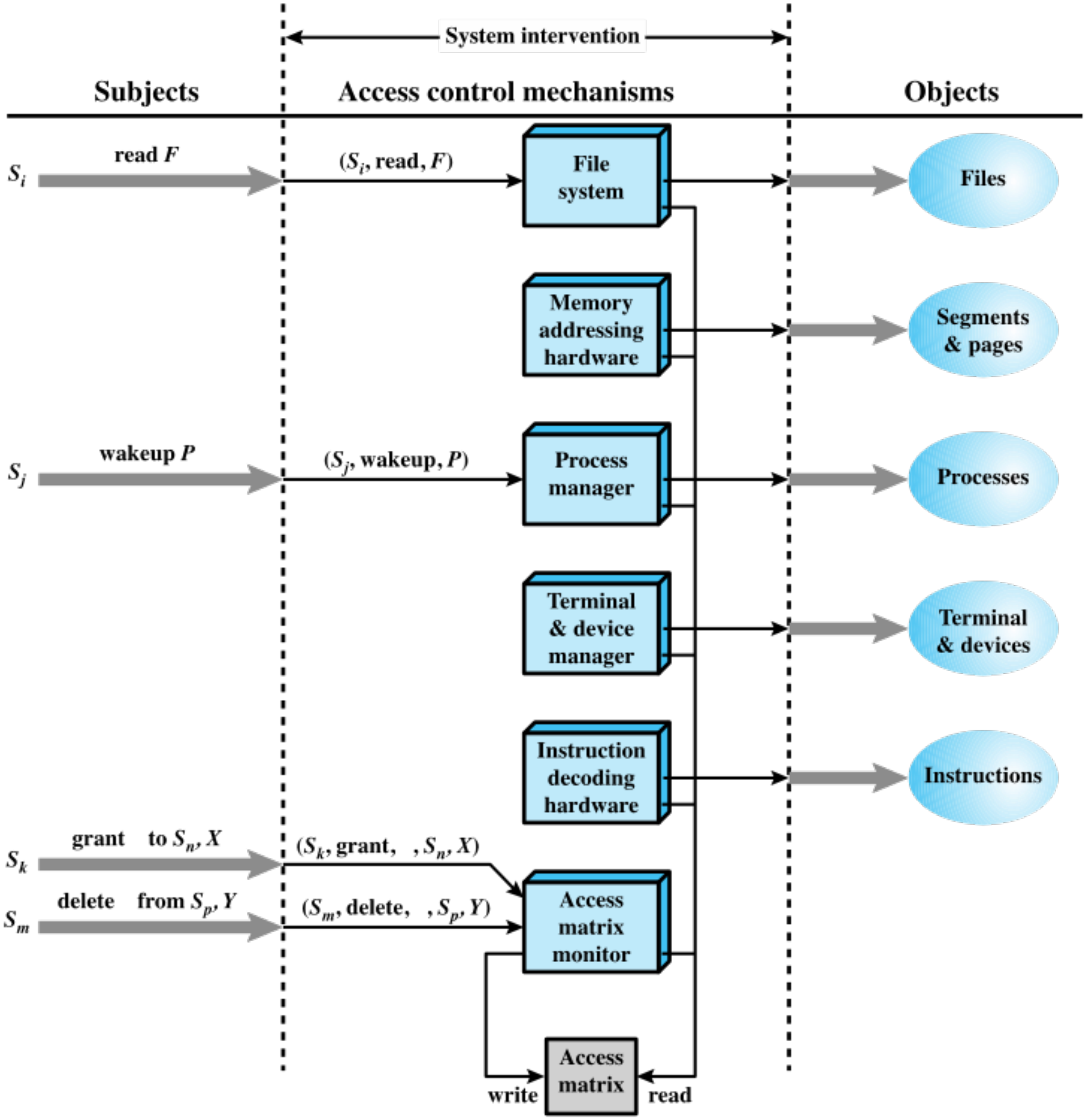
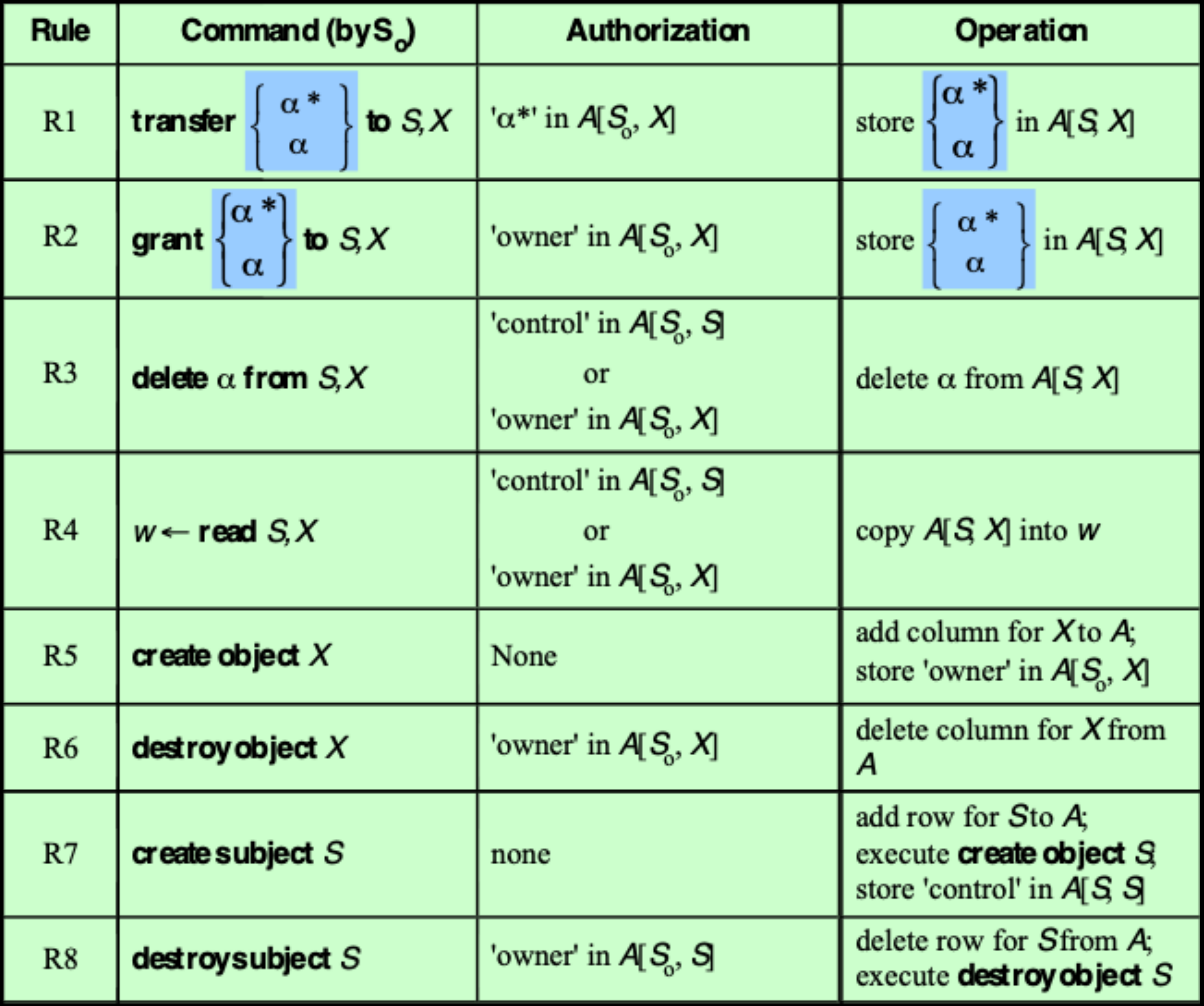


Figure 4.4 An Organization of the Access Control Function



Rule	Command (by S_o)	Authorization	Operation
R1	**transfer** $\begin{Bmatrix}\alpha^*\\ \alpha\end{Bmatrix}$ **to** S, X	'α*' in $A[S_o, X]$	store $\begin{Bmatrix}\alpha^*\\ \alpha\end{Bmatrix}$ in $A[S, X]$
R2	**grant** $\begin{Bmatrix}\alpha^*\\ \alpha\end{Bmatrix}$ **to** S, X	'owner' in $A[S_o, X]$	store $\begin{Bmatrix}\alpha^*\\ \alpha\end{Bmatrix}$ in $A[S, X]$
R3	**delete** α **from** S, X	'control' in $A[S_o, S]$ or 'owner' in $A[S_o, X]$	delete α from $A[S, X]$
R4	$w \leftarrow$ **read** S, X	'control' in $A[S_o, S]$ or 'owner' in $A[S_o, X]$	copy $A[S, X]$ into w
R5	**create object** X	None	add column for X to A; store 'owner' in $A[S_o, X]$
R6	**destroy object** X	'owner' in $A[S_o, X]$	delete column for X from A
R7	**create subject** S	none	add row for S to A; execute **create object** S; store 'control' in $A[S, S]$
R8	**destroy subject** S	'owner' in $A[S_o, S]$	delete row for S from A; execute **destroy object** S

Table 4.3

Access Control System Commands

(Table is on page 116 in the textbook)

Protection Domains

- Set of objects together with access rights to those objects
- More flexibility when associating capabilities with protection domains
- In terms of the access matrix, a row defines a protection domain
- User can spawn processes with a subset of the access rights of the user
- Association between a process and a domain can be static or dynamic
- In user mode certain areas of memory are protected from use and certain instructions may not be executed
- In kernel mode privileged instructions may be executed and protected areas of memory may be accessed

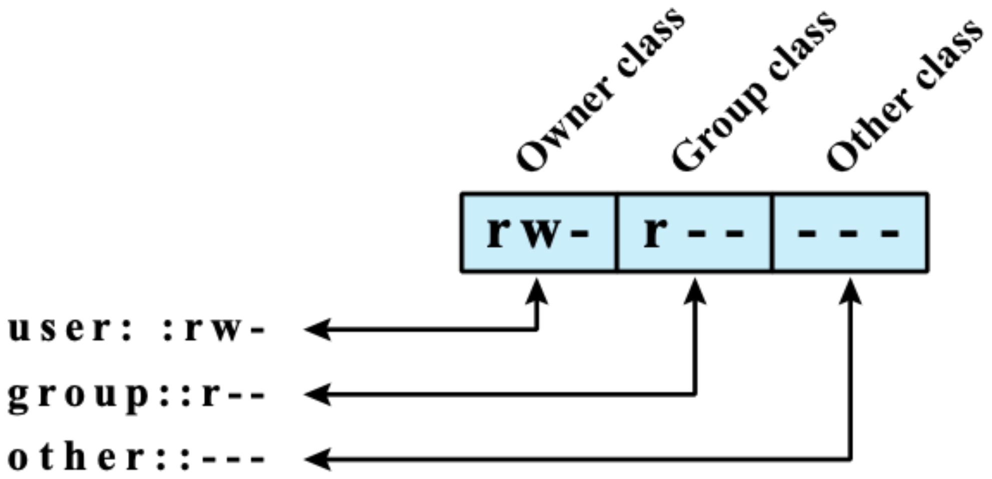
UNIX File Access Control

- UNIX files are administered using inodes (index nodes)
  - Control structures with key information needed for a particular file
  - Several file names may be associated with a single inode
  - An active inode is associated with exactly one file
  - File attributes, permissions and control information are sorted in the inode
  - On the disk there is an inode table, or inode list, that contains the inodes of all the files in the file system
  - When a file is opened its inode is brought into main memory and stored in a memory resident inode table

- **Directories are structured in a hierarchical tree**
  - May contain files and/or other directories
  - Contains file names plus pointers to associated inodes

UNIX
File Access Control

- Unique user identification number (user ID)
- Member of a primary group identified by a group ID
- Belongs to a specific group
- 12 protection bits
  - Specify read, write, and execute permission for the owner of the file, members of the group and all other users
- The owner ID, group ID, and protection bits are part of the file's inode



(a) Traditional UNIX approach (minimal access control list)

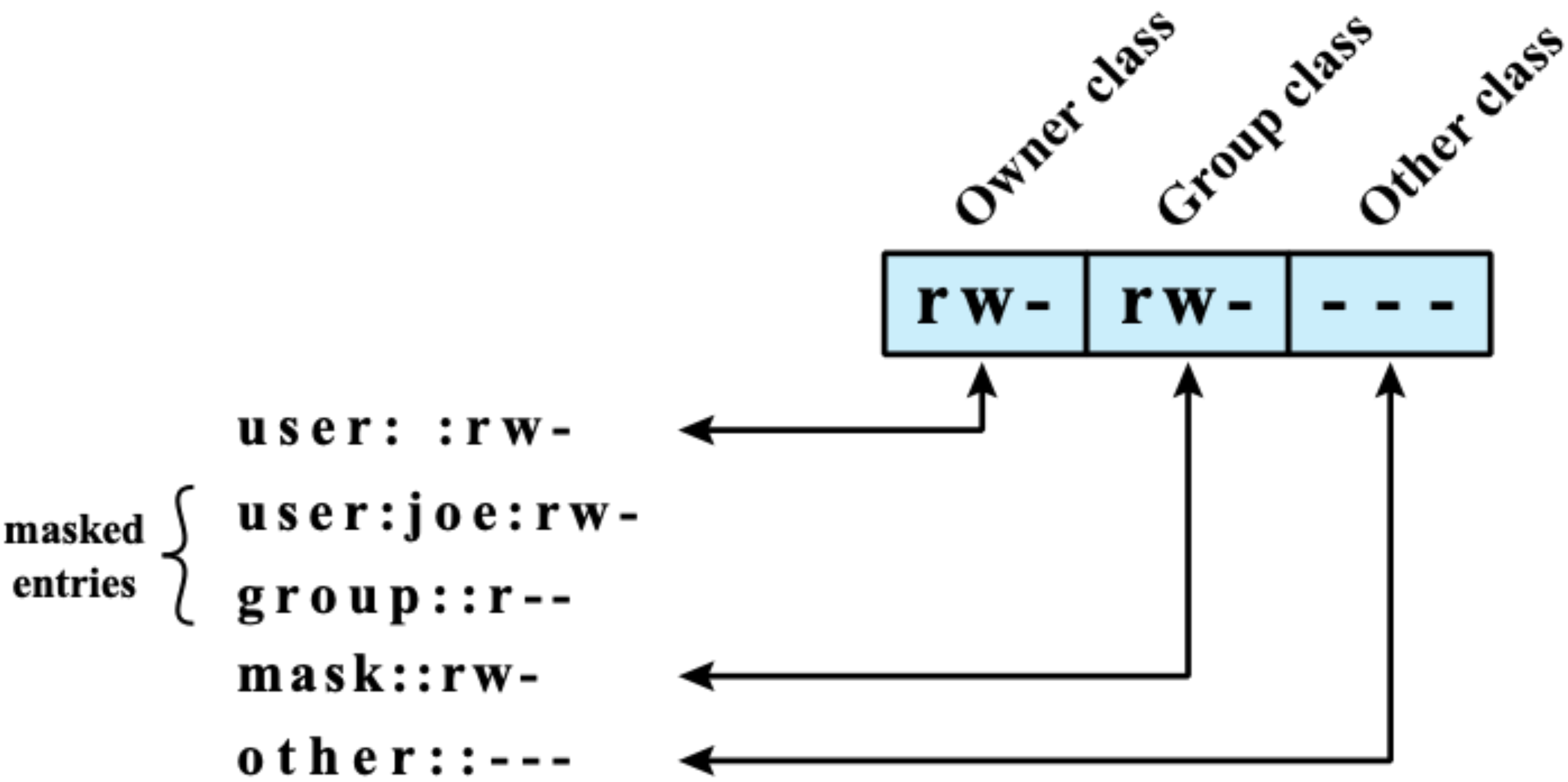
Figure 4.5 UNIX File Access Control

Traditional UNIX File Access Control

- “Set user ID”(SetUID)
- “Set group ID”(SetGID)
  - System temporarily uses rights of the file owner/group in addition to the real user’s rights when making access control decisions
  - Enables privileged programs to access files/resources not generally accessible
- Sticky bit
  - When applied to a directory it specifies that only the owner of any file in the directory can rename, move, or delete that file
- Superuser
  - Is exempt from usual access control restrictions
  - Has system-wide access

Access Control Lists (ACLs) in UNIX

- **Modern UNIX systems support ACLs**
  - FreeBSD, OpenBSD, Linux, Solaris
- **FreeBSD**
  - Setfacl command assigns a list of UNIX user IDs and groups
  - Any number of users and groups can be associated with a file
  - Read, write, execute protection bits
  - A file does not need to have an ACL
  - Includes an additional protection bit that indicates whether the file has an extended ACL
- **When a process requests access to a file system object two steps are performed:**
  - Step 1 selects the most appropriate ACL
  - Step 2 checks if the matching entry contains sufficient permissions



Owner class

Group class

Other class

```
rw-  rw-  ---
```

```
user::rw-
user:joe:rw-
group::r--
mask::rw-
other::---
```

masked entries

(b) Extended access control list

Figure 4.5 UNIX File Access Control

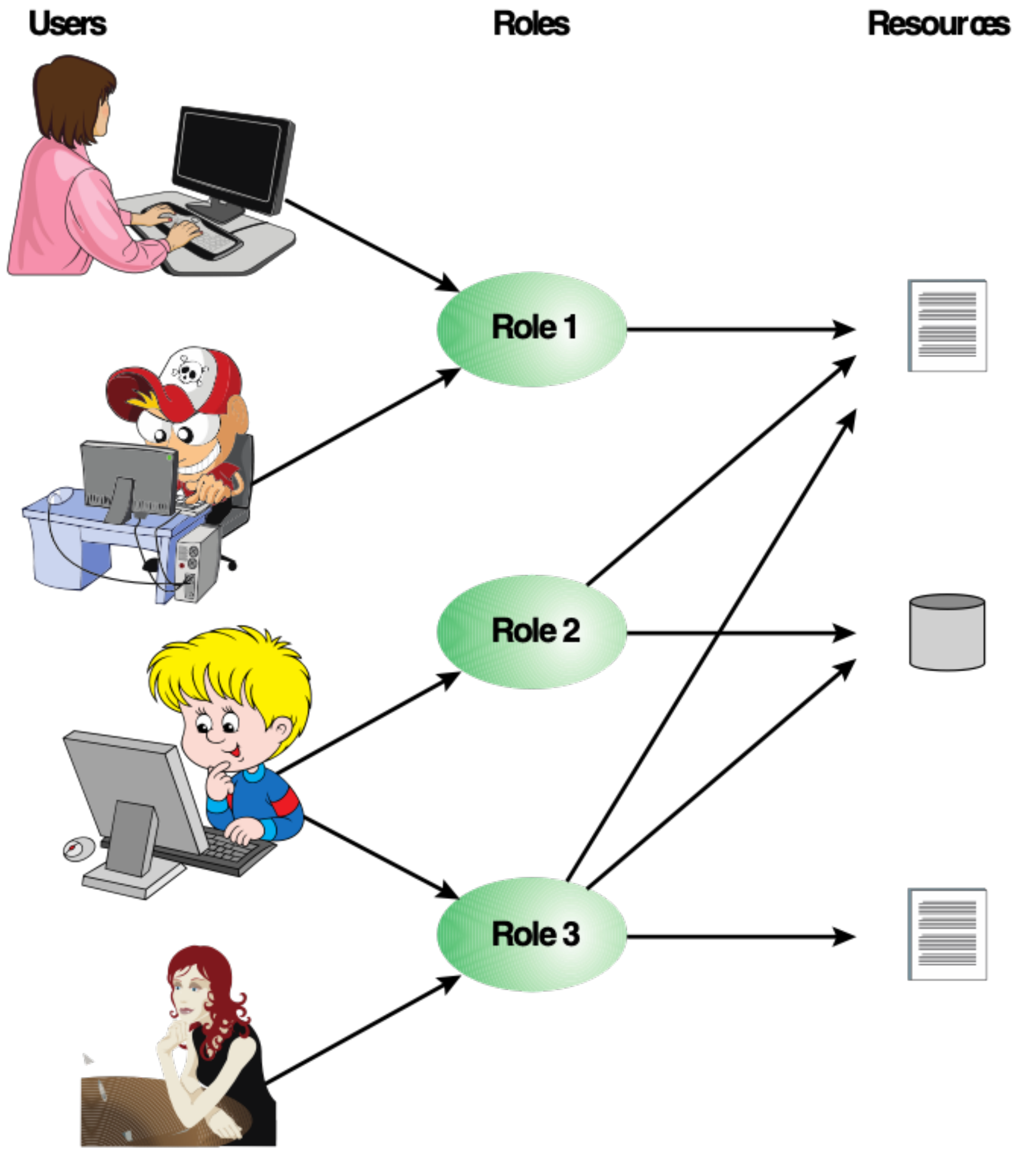
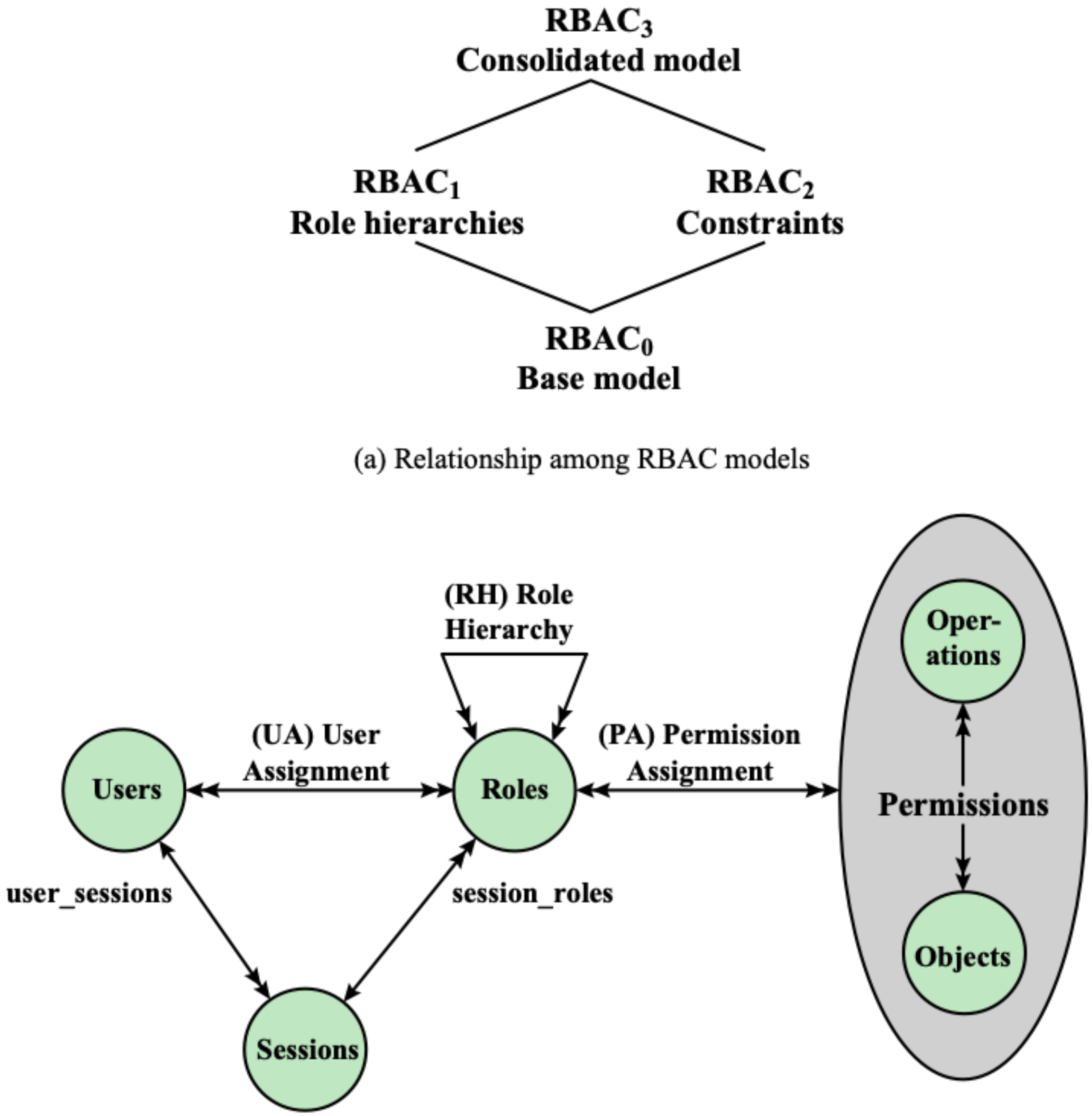


Figure 4.6 Users, Roles, and Resources

	R_1	R_2	• • •	R_n
U_1	✖			
U_2	✖			
U_3		✖		✖
U_4				✖
U_5				✖
U_6				✖
• • •				
U_m	✖			

	OBJECTS								
ROLES	R_1	R_2	R_n	F_1	F_1	P_1	P_2	D_1	D_2
R_1	control	owner	owner control	read *	read owner	wakeup	wakeup	seek	owner
R_2		control		write *	execute			owner	seek *
• • •									
R_n			control		write	stop			

Figure 4.7 Access Control Matrix Representation of RBAC

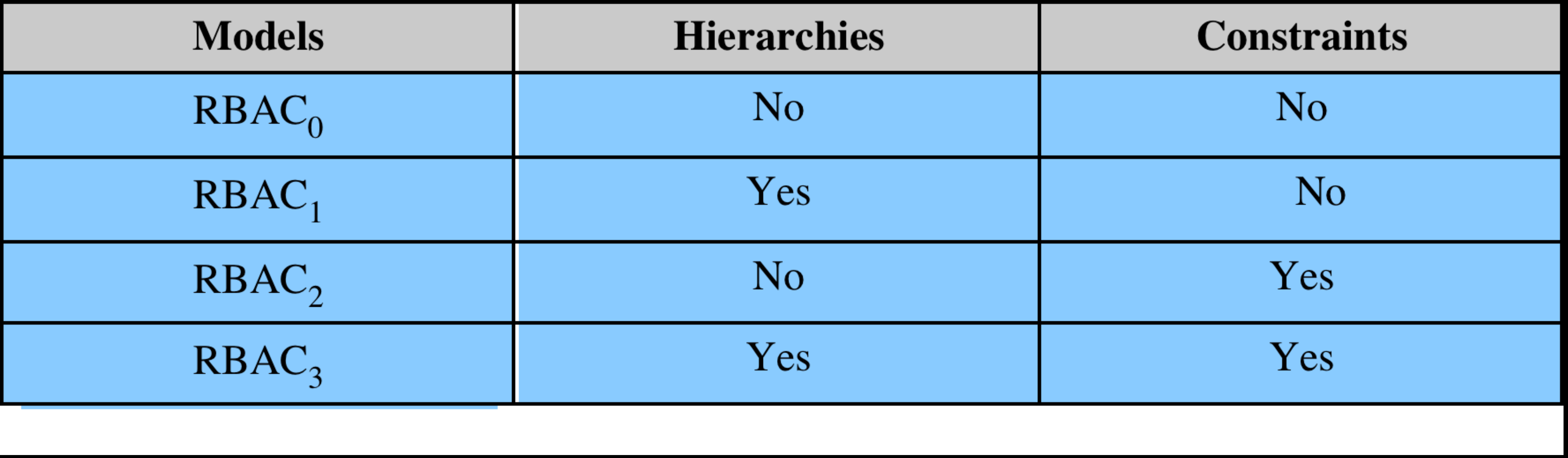


(a) Relationship among RBAC models

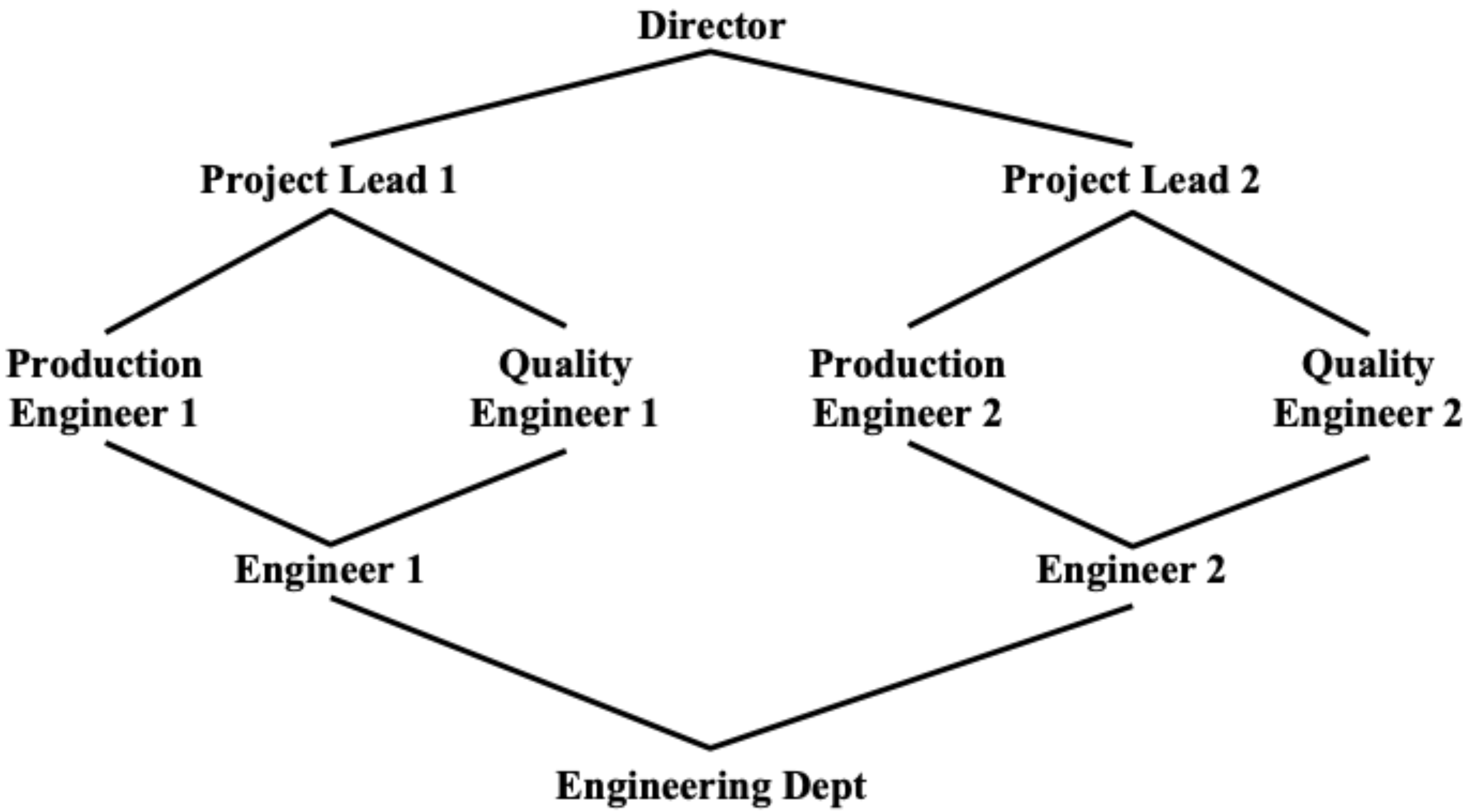
(b) RBAC models

Figure 4.8 A Family of Role-Based Access Control Models.

Table 4.4
Scope RBAC Models



Models	Hierarchies	Constraints
$RBAC_0$	No	No
$RBAC_1$	Yes	No
$RBAC_2$	No	Yes
$RBAC_3$	Yes	Yes



Director

Project Lead 1

Project Lead 2

Production Engineer 1

Quality Engineer 1

Production Engineer 2

Quality Engineer 2

Engineer 1

Engineer 2

Engineering Dept

Figure 4.9 Example of Role Hierarchy

Constraints - RBAC

- Provide a means of adapting RBAC to the specifics of administrative and security policies of an organization
- A defined relationship among roles or a condition related to roles
- Types:

Mutually exclusive roles

- A user can only be assigned to one role in the set (either during a session or statically)
- Any permission (access right) can be granted to only one role in the set

Cardinality

- Setting a maximum number with respect to roles

Prerequisite roles

- Dictates that a user can only be assigned to a particular role if it is already assigned to some other specified role

Attribute-Based Access Control (ABAC)

- Can define authorizations that express conditions on properties of both the resource and the subject
- Strength is its flexibility and expressive power
- Main obstacle to its adoption in real systems has been concern about the performance impact of evaluating predicates on both resource and user properties for each access
- Web services have been pioneering technologies through the introduction of the eXtensible Access Control Markup Language (XAMCL)
- There is considerable interest in applying the model to cloud services

ABAC Model: Attributes

• Subject attributes

- A subject is an active entity that causes information to flow among objects or changes the system state
- Attributes define the identity and characteristics of the subject

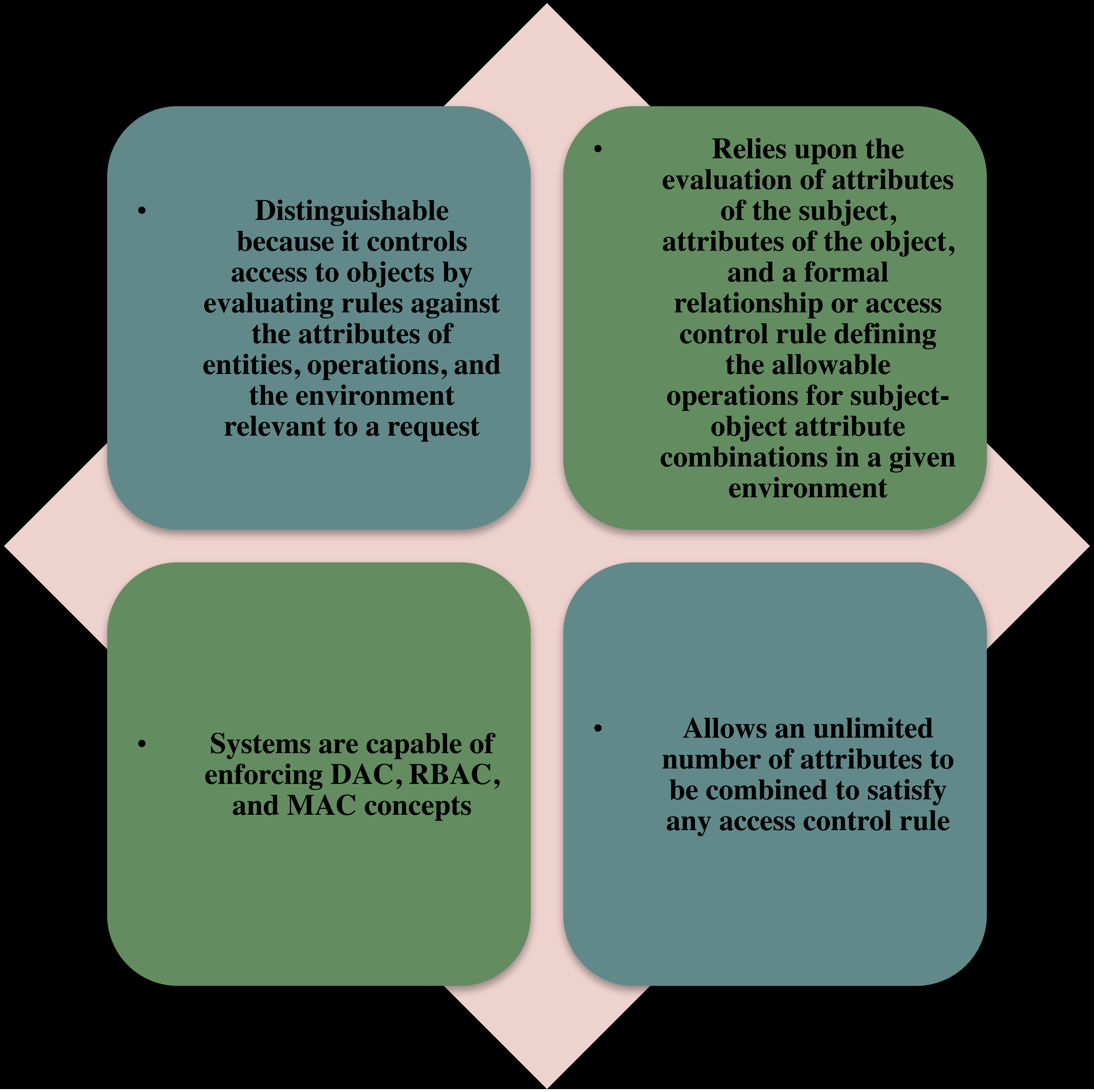
• Object attributes

- An object (or resource) is a passive information system-related entity containing or receiving information
- Objects have attributes that can be leverages to make access control decisions

• Environment attributes

- Describe the operational, technical, and even situational environment or context in which the information access occurs
- These attributes have so far been largely ignored in most access control policies

ABAC



- Distinguishable because it controls access to objects by evaluating rules against the attributes of entities, operations, and the environment relevant to a request

- Relies upon the evaluation of attributes of the subject, attributes of the object, and a formal relationship or access control rule defining the allowable operations for subject-object attribute combinations in a given environment

- Systems are capable of enforcing DAC, RBAC, and MAC concepts

- Allows an unlimited number of attributes to be combined to satisfy any access control rule

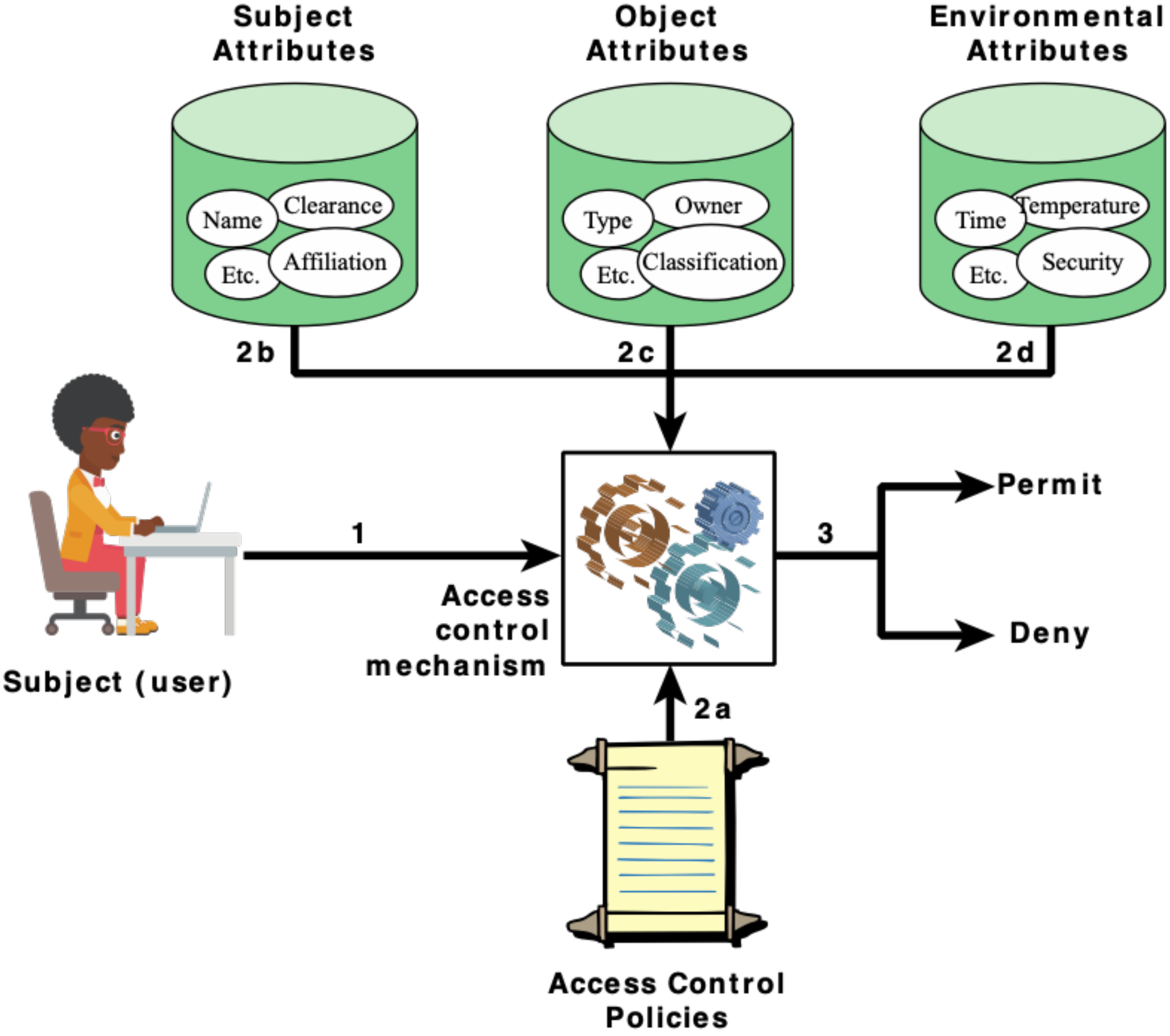
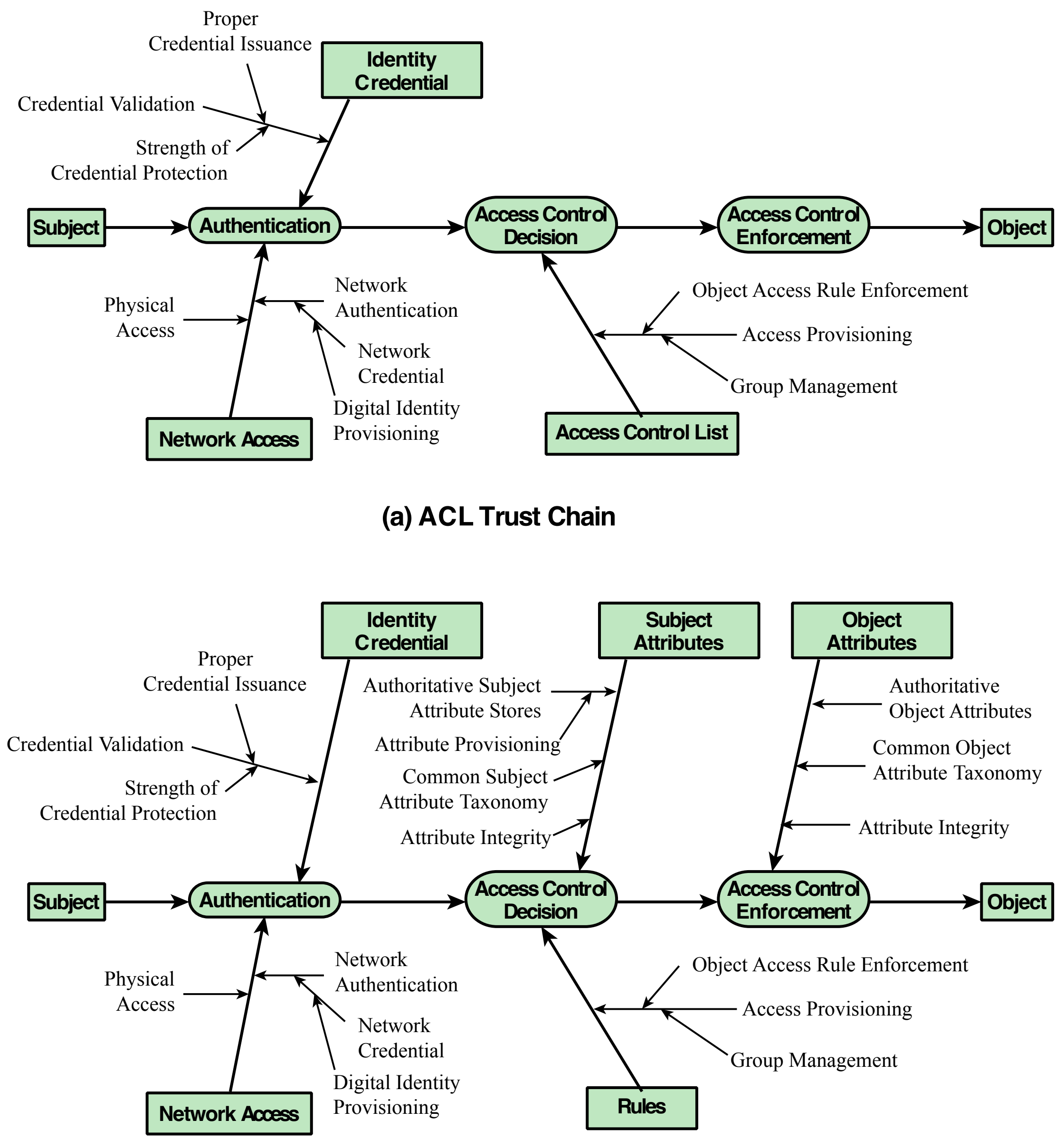


Figure 4.10 ABAC Scenario



(a) ACL Trust Chain

(b) ABAC Trust Chain

Figure 4.11 ACL and ABAC Trust Relationships

ABAC Policies

- A policy is a set of rules and relationships that govern allowable behavior within an organization, based on the privileges of subjects and how resources or objects are to be protected under which environment conditions

Typically written from the perspective of the object that needs protecting and the privileges available to subjects

- Privileges represent the authorized behavior of a subject and are defined by an authority and embodied in a policy

- Other terms commonly used instead of privileges are: rights, authorizations, and entitlements

Identity, Credential, and Access Management (ICAM)

- A comprehensive approach to managing and implementing digital identities, credentials, and access control
- Developed by the U.S. government
- Designed to:
  - Create trusted digital identity representations of individuals and nonperson entities (NPEs)
  - Bind those identities to credentials that may serve as a proxy for the individual of NPE in access transactions
    - A credential is an object or data structure that authoritatively binds an identity to a token possessed and controlled by a subscriber
  - Use the credentials to provide authorized access to an agency's resources

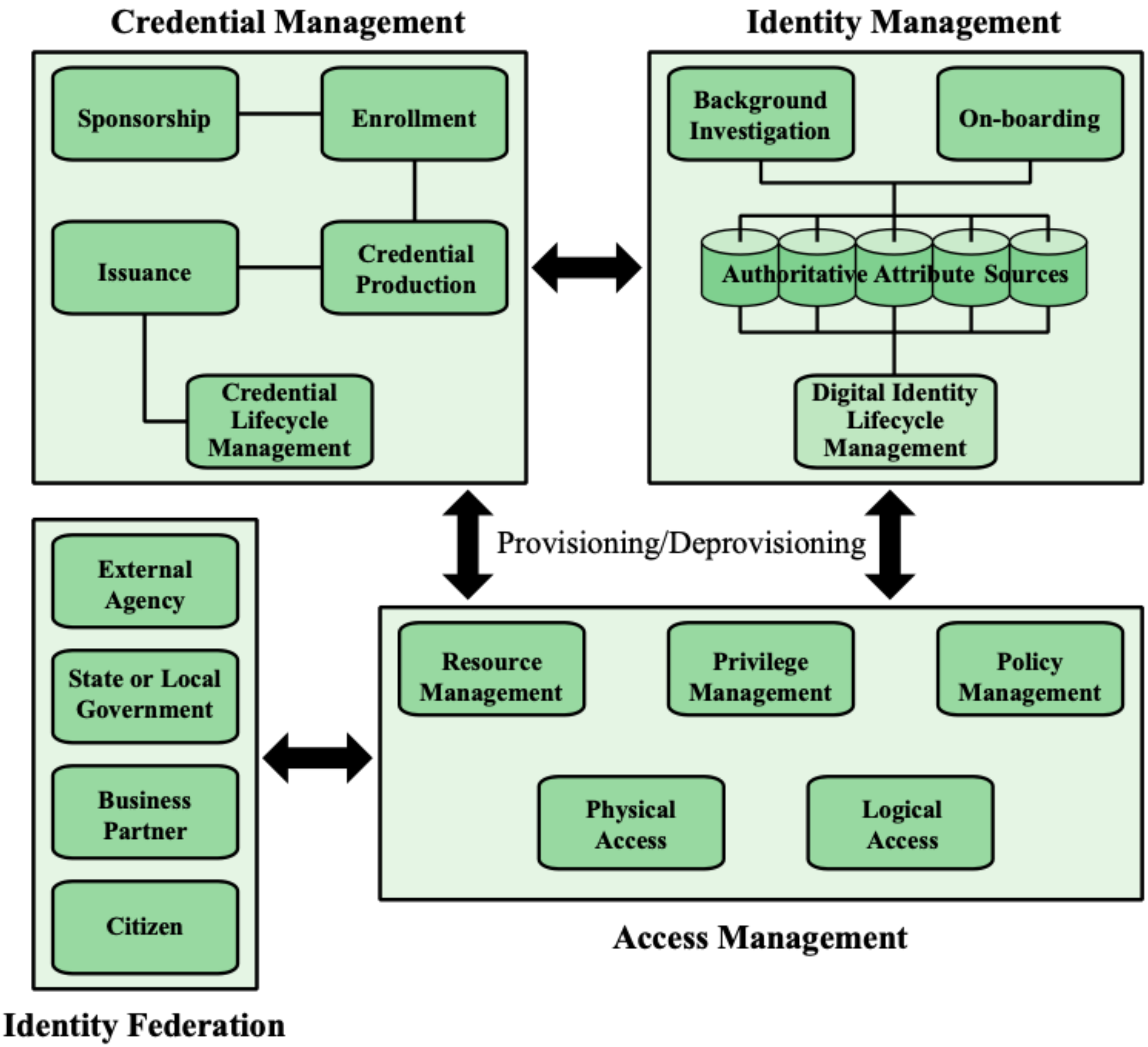
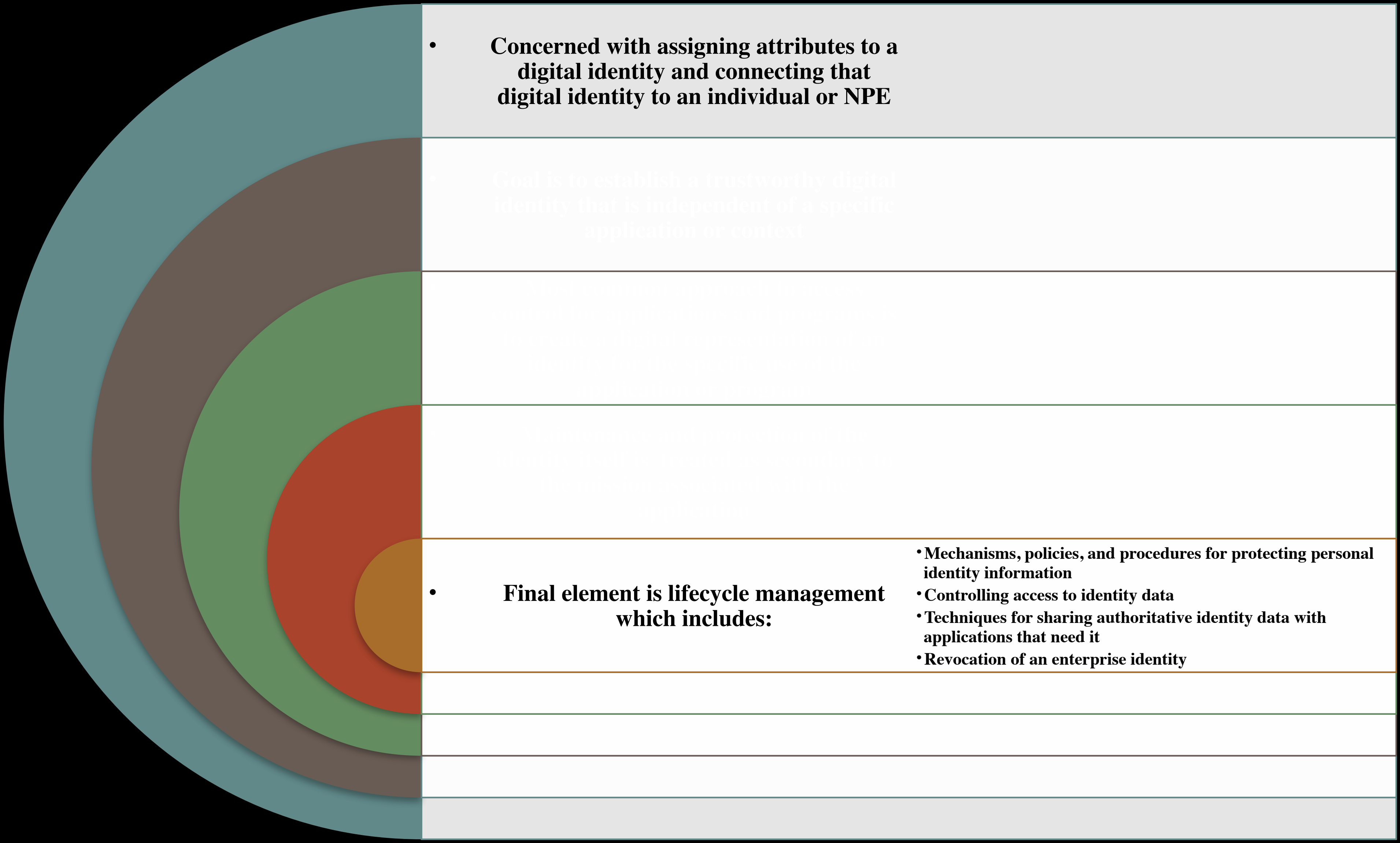


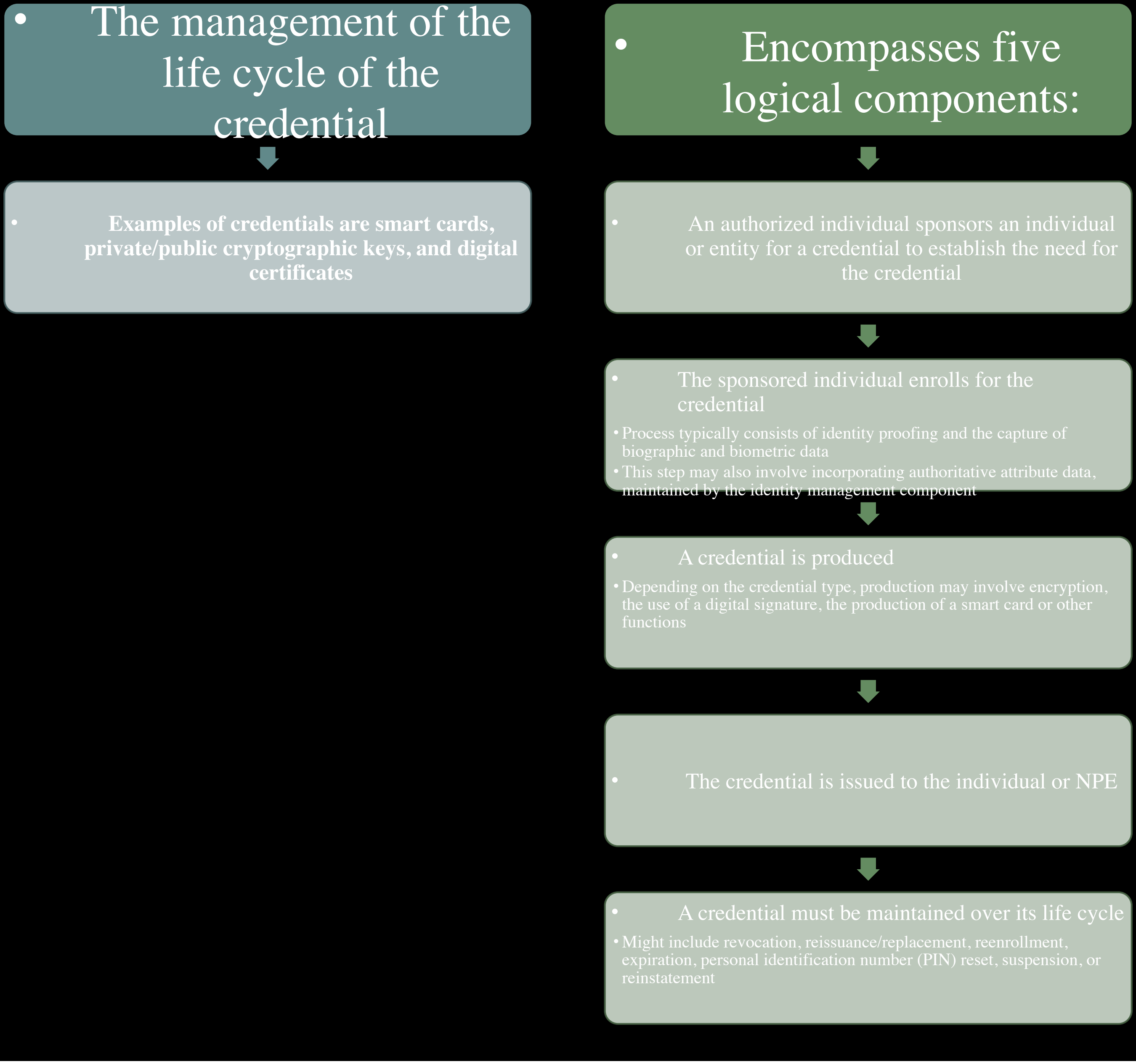
Figure 4.12 Identity, Credential, and Access Management (ICAM)

Identity Management



- Concerned with assigning attributes to a digital identity and connecting that digital identity to an individual or NPE
- Goal is to establish a trustworthy digital identity that is independent of a specific application or context
- Most common approach to access control for applications and programs is to create a digital representation of an identity for the specific use of the application or program
- Maintenance and protection of the identity itself is treated as secondary to the mission associated with the application
- Final element is lifecycle management which includes:
  - Mechanisms, policies, and procedures for protecting personal identity information
  - Controlling access to identity data
  - Techniques for sharing authoritative identity data with applications that need it
  - Revocation of an enterprise identity

Credential Management



- The management of the life cycle of the credential
  - Examples of credentials are smart cards, private/public cryptographic keys, and digital certificates

- Encompasses five logical components:
  - An authorized individual sponsors an individual or entity for a credential to establish the need for the credential
  - The sponsored individual enrolls for the credential
    - Process typically consists of identity proofing and the capture of biographic and biometric data
    - This step may also involve incorporating authoritative attribute data, maintained by the identity management component
  - A credential is produced
    - Depending on the credential type, production may involve encryption, the use of a digital signature, the production of a smart card or other functions
  - The credential is issued to the individual or NPE
  - A credential must be maintained over its life cycle
    - Might include revocation, reissuance/replacement, reenrollment, expiration, personal identification number (PIN) reset, suspension, or reinstatement

Access Management

- Deals with the management and control of the ways entities are granted access to resources

- Covers both logical and physical access

- May be internal to a system or an external element

- Purpose is to ensure that the proper identity verification is made when an individual attempts to access a security sensitive building, computer systems, or data

- Three support elements are needed for an enterprise-wide access control facility:
  - Resource management
  - Privilege management
  - Policy management

Three support elements are needed for an enterprise-wide access control facility:

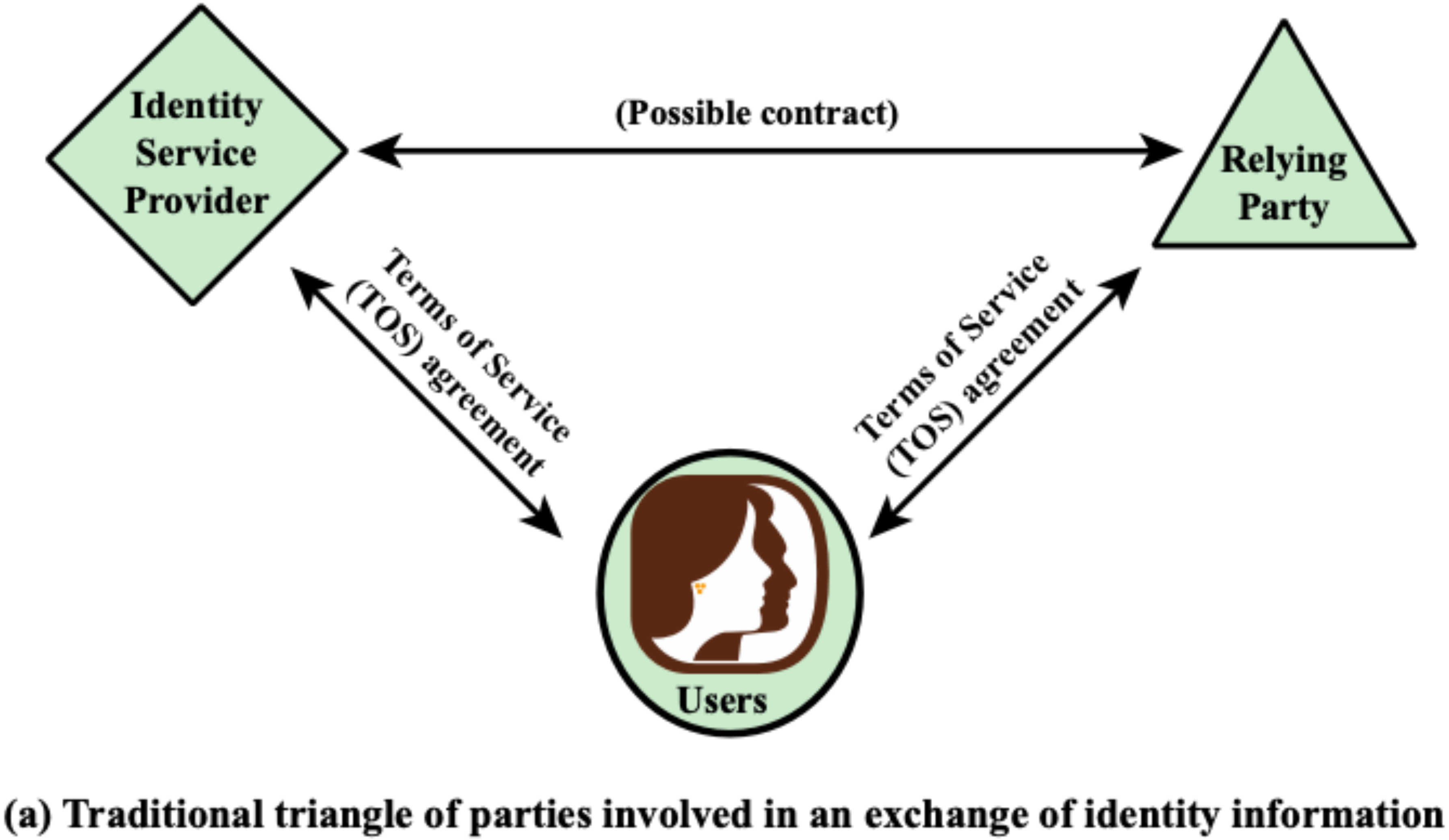
- Resource management
  - Concerned with defining rules for a resource that requires access control
  - Rules would include credential requirements and what user attributes, resource attributes, and environmental conditions are required for access of a given resource for a given function

- Privilege management
  - Concerned with establishing and maintaining the entitlement or privilege attributes that comprise an individual’s access profile
  - These attributes represent features of an individual that can be used as the basis for determining access decisions to both physical and logical resources
  - Privileges are considered attributes that can be linked to a digital identity

- Policy management
  - Governs what is allowable and unallowable in an access transaction

Identity Federation

- Term used to describe the technology, standards, policies, and processes that allow an organization to trust digital identities, identity attributes, and credentials created and issued by another organization
- Addresses two questions:
  - How do you trust identities of individuals from external organizations who need access to your systems
  - How do you vouch for identities of individuals in your organization when they need to collaborate with external organizations


Identity Service Provider
(Possible contract)
Relying Party
Terms of Service (TOS) agreement
Terms of Service (TOS) agreement
Users

(a) Traditional triangle of parties involved in an exchange of identity information

Figure 4.13 Identity Information Exchange Approaches

Open Identity Trust Framework

- **OpenID**
  - **An open standard that allows users to be authenticated by certain cooperating sites using a third party service**

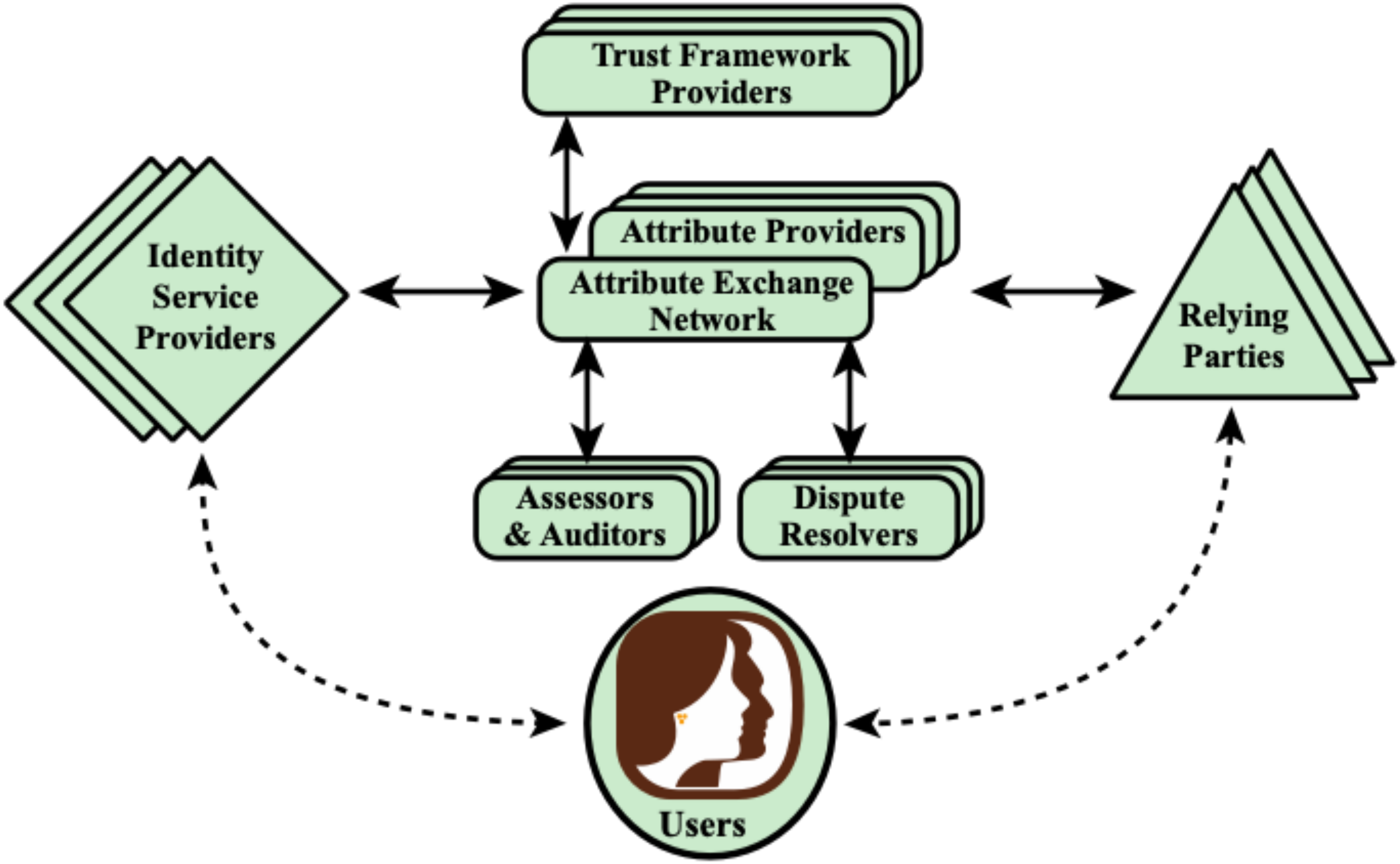
- **OIDF**
  - **OpenID Foundation is an international nonprofit organization of individuals and companies committed to enabling, promoting, and protecting OpenID technologies**

- **ICF**
  - **Information Card Foundation is a nonprofit community of companies and individuals working together to evolve the Information Card ecosystem**

- **OITF**
  - **Open Identity Trust Framework is a standardized, open specification of a trust framework for identity and attribute exchange, developed jointly by OIDF and ICF**

- **OIX**
  - **Open Identity Exchange Corporation is an independent, neutral, international provider of certification trust frameworks conforming to the OITF model**

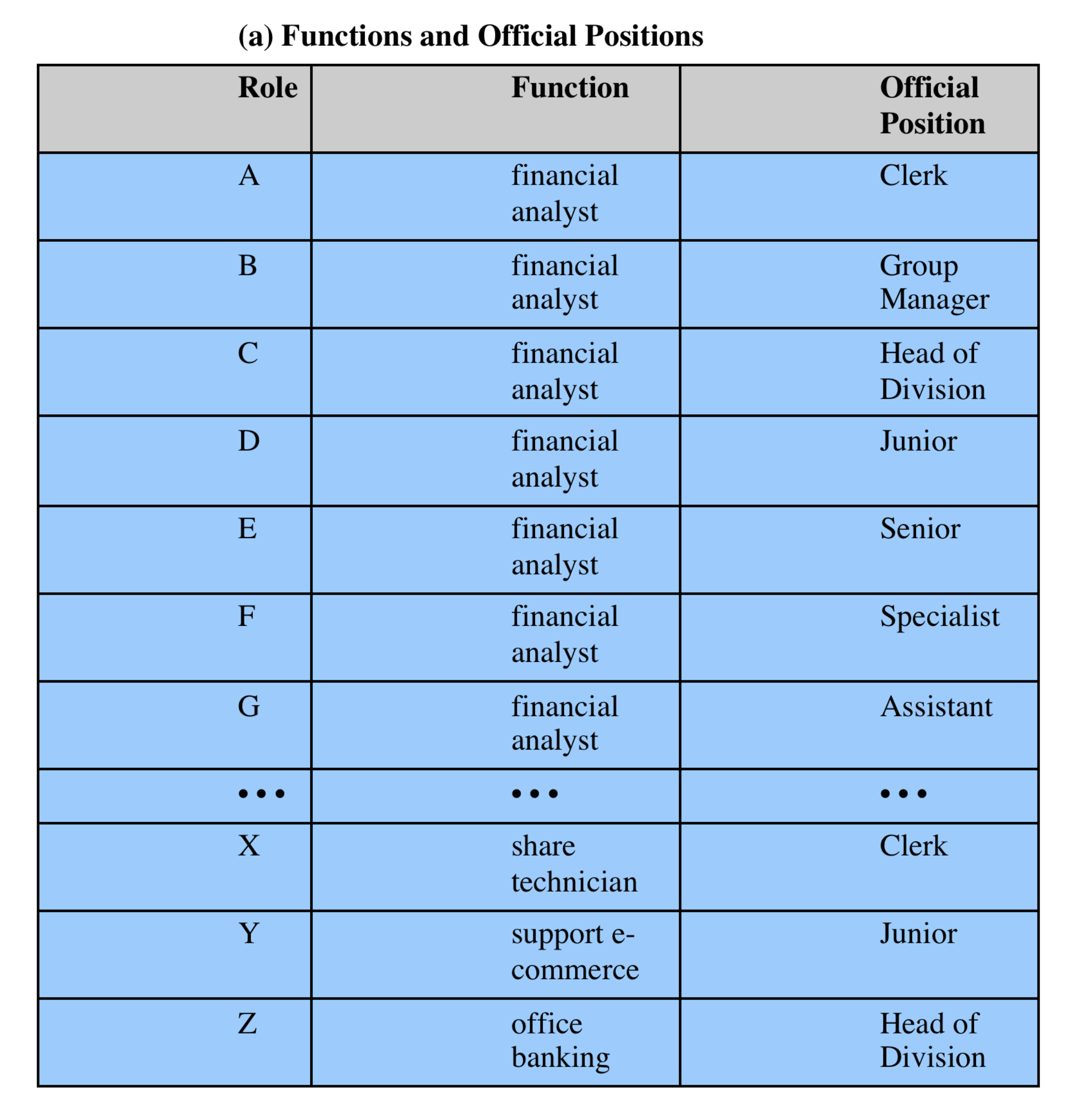
- **AXN**
  - **Attribute Exchange Network is an online Internet-scale gateway for identity service providers and relying parties to efficiently access user asserted, permissioned, and verified online identity attributes in high volumes at affordable costs**


Trust Framework Providers
Identity Service Providers
Attribute Providers
Attribute Exchange Network
Relying Parties
Assessors & Auditors
Dispute Resolvers
Users

(B) Identity attribute exchange elements

Figure 4.13 Identity Information Exchange Approaches

Table 4.5
Functions and Roles for Banking Example



(a) Functions and Official Positions

Role	Function	Official Position
A	financial analyst	Clerk
B	financial analyst	Group Manager
C	financial analyst	Head of Division
D	financial analyst	Junior
E	financial analyst	Senior
F	financial analyst	Specialist
G	financial analyst	Assistant
• • •	• • •	• • •
X	share technician	Clerk
Y	support e-commerce	Junior
Z	office banking	Head of Division

Table 4.5
Functions and Roles for Banking Example

(b) Permission Assignments

Role	Application	Access Right
A	money market instruments	1, 2, 3, 4
	derivatives trading	1, 2, 3, 7, 10, 12
	interest instruments	1, 4, 8, 12, 14, 16
B	money market instruments	1, 2, 3, 4, 7
	derivatives trading	1, 2, 3, 7, 10, 12, 14
	interest instruments	1, 4, 8, 12, 14, 16
	private consumer instruments	1, 2, 4, 7
• • •	• • •	• • •

(c) PA with Inheritance

Role	Application	Access Right
A	money market instruments	1, 2, 3, 4
	derivatives trading	1, 2, 3, 7, 10, 12
	interest instruments	1, 4, 8, 12, 14, 16
B	money market instruments	7
	derivatives trading	14
	private consumer instruments	1, 2, 4, 7
• • •	• • •	• • •

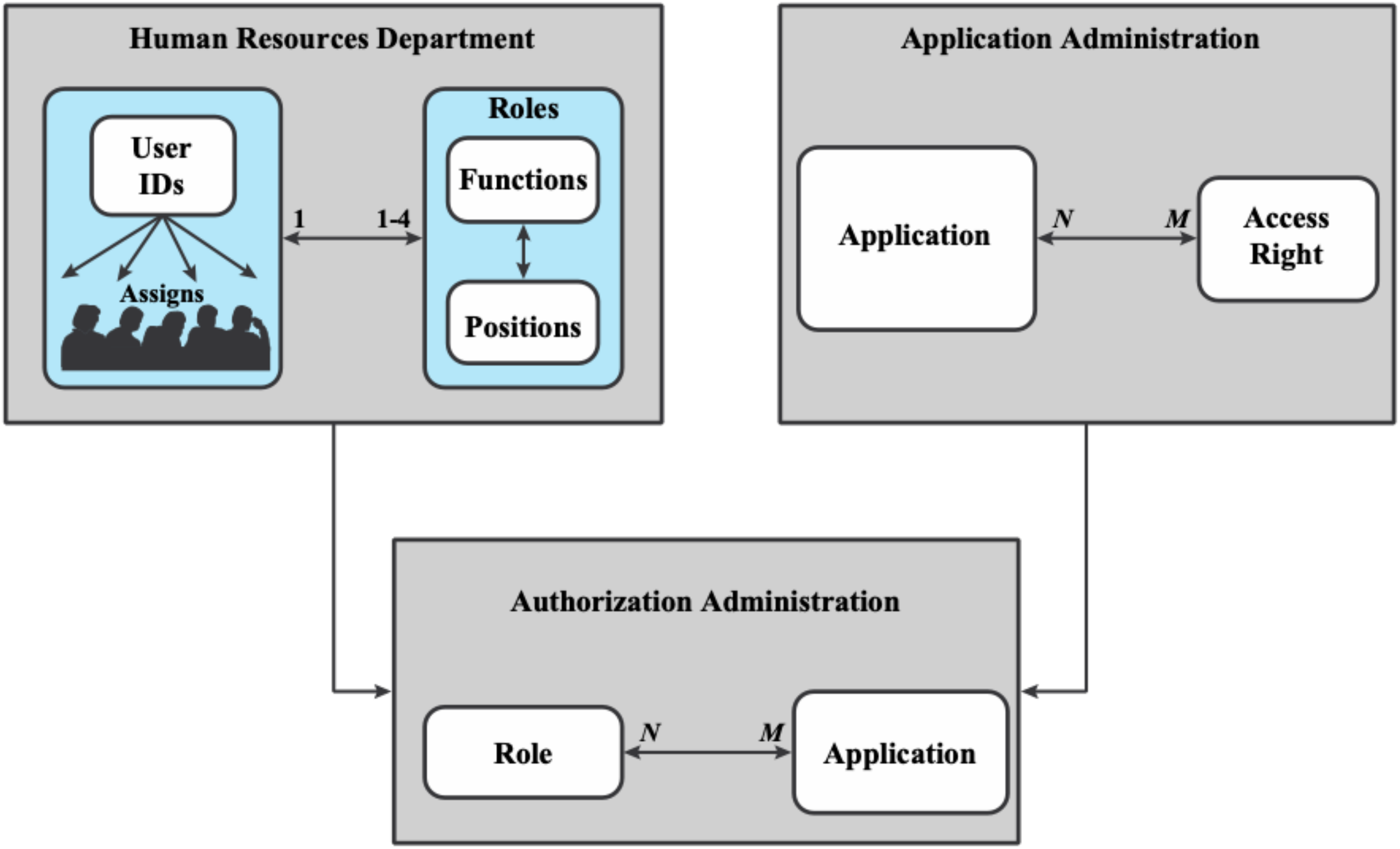


Figure 4.14 Example of Access Control Administration

Summary

- Access control principles
  - Access control context
  - Access control policies
- Subjects, objects, and access rights
- Discretionary access control
  - Access control model
  - Protection domains
- UNIX file access control
  - Traditional UNIX file access control
  - Access control lists in UNIX
- Role-based access control
  - RBAC reference models
- Attribute-based access control
  - Attributes
  - ABAC logical architecture
  - ABAC policies
- Identity, credential, and access management
  - Identity management
  - Credential management
  - Access management
  - Identity federation
- Trust frameworks
  - Traditional identity exchange approach
  - Open identity trust framework
- Bank RBAC system