Sicurezza Documentale a.a. 2017/2018

DOCENTI: DOTT.SSA VALERIA FIONDA

DOTT. GIUSEPPE PIRRÒ

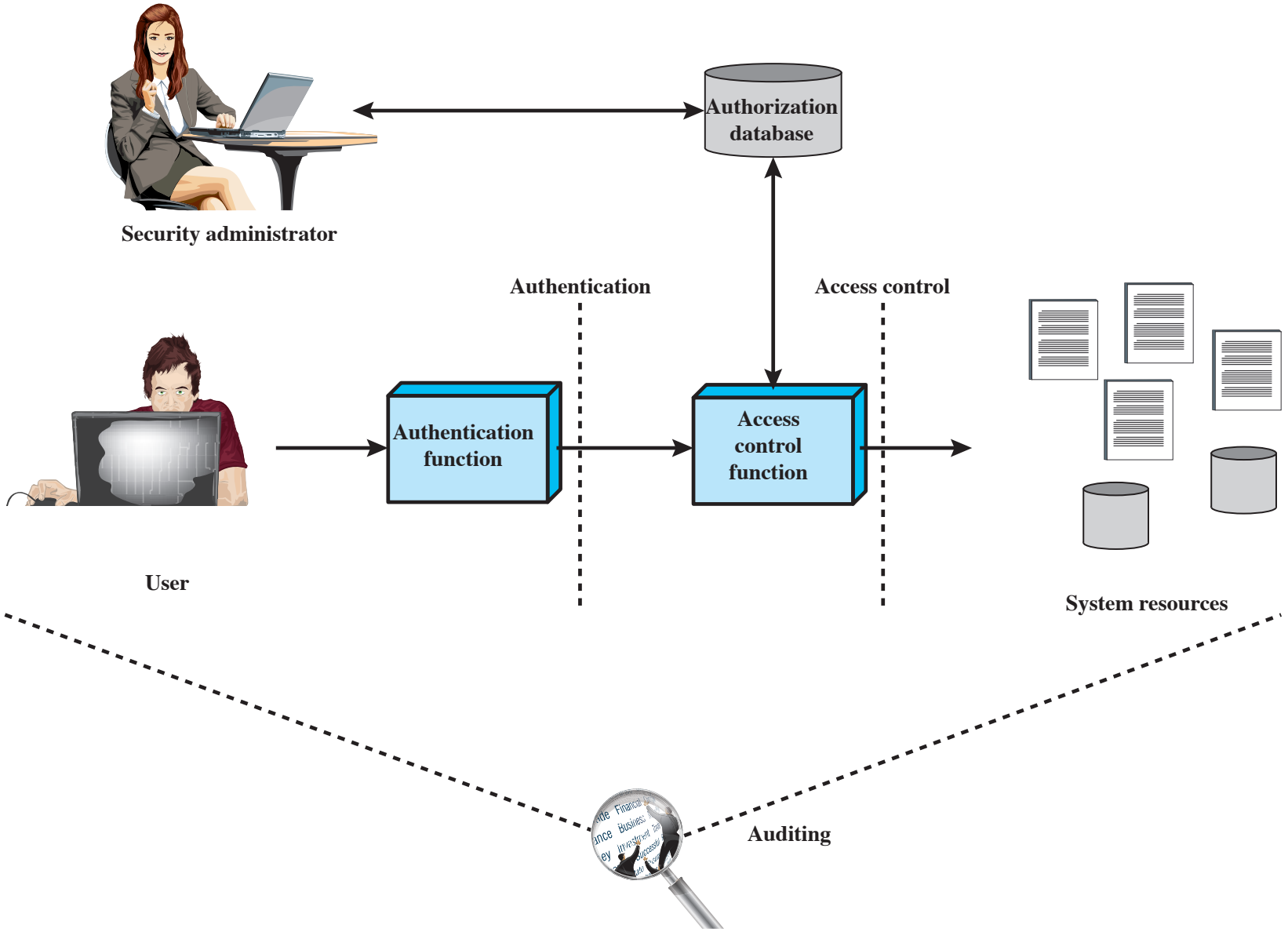
Controllo degli accessi

Gli obiettivi fondamentali

- Attraverso il controllo degli accessi si vogliono raggiungere I seguenti obiettivi:
  - Controllare l'accesso alle risorse
  - Identificare chi accede alle risorse
  - Autorizzare le operazioni che possono essere effettuate in base a chi ha effettuato l'accesso
  - Monitorare le modalità di accesso e le attività svolte

Resistenze sociali e culturali

- I sistemi protetti sono più costosi da realizzare e complessi da utilizzare
- Gli utenti devono essere introdotti alla «cultura» di protezione del sistema e delle proprie responsabilità
- Le credenziali di accesso per essere affidabili richiedono procedure non banali e/o informazioni complesse
- «Ma tanto non è mai successo niente …»


Authorization database
Security administrator
Authentication
Access control
Authentication function
Access control function
User
System resources
Auditing

Soggetti, Oggetti, e Diritti di Accesso

Soggetto

Una entita' capace di accedere agli oggetti

Tre classi
- Owner (proprietario)
- Group (gruppo)
- World (mondo)

Oggetto

Una risorsa il cui accesso e' controllato

Entita' utilizzate per contenere e/o ricevere informazione

Diritti d'Accesso

Descrivono il modo in cui un soggetto puo' accedere ad un oggetto

Includono:
- Read (lettura)
- Write (scrittura)
- Execute (esecuzione)
- Delete (cancellazione)
- Create (creazione)
- Search (ricerca)

Politiche di controlllo degli accessi

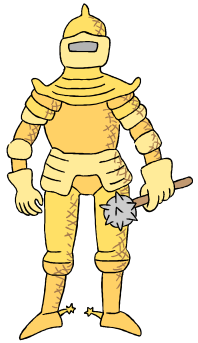
- Controllo degli accessi discrezionale (DAC)
  - Controlla l'accesso in base all'identità del richiedente e alle regole di accesso (autorizzazioni) che indicano cosa i richiedenti possono (o non possono) fare
- Controllo degli accessi obbligatorio (MAC)
  - Controlla l'accesso in base al confronto tra etichette di sicurezza e autorizzazioni di sicurezza
- Controllo degli accessi basato sui ruoli (RBAC)
  - Controlla l'accesso in base ai ruoli che gli utenti hanno all'interno del sistema e alle regole che indicano quali accessi sono consentiti agli utenti in determinati ruoli
- Controllo degli accessi basato sugli attributi (ABAC)
  - Controlla l'accesso in base agli attributi dell'utente, alla risorsa a cui si accede e alle condizioni correnti del sistema

Controllo degli accessi discrezionale (DAC)

- Schema in cui un'entità può consentire ad un'altra entità di accedere ad alcune risorse
- Spesso fornito utilizzando una matrice di accesso
  - Una dimensione rappresenta i soggetti identificati che possono tentare l'accesso alle risorse
  - L'altra dimensione rappresenta gli oggetti a cui è possibile accedere
- Ogni cella della matrice indica i diritti di accesso di un particolare soggetto per un particolare oggetto

Controllo degli accessi discrezionale (DAC)

		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



Domini di Protezione

- Insiemi di oggetti con i diritti di accesso a tali oggetti
- Maggiore flessibilità quando si associano funzionalità ai domini di protezione
- In termini di matrice di accesso, una riga definisce un dominio di protezione
- L'utente può generare processi con un sottoinsieme dei diritti di accesso dell'utente
- L'associazione tra un processo e un dominio può essere statica o dinamica
- In modalità utente, alcune aree della memoria sono protette dall'uso e alcune istruzioni potrebbero non essere eseguite
- Nella modalità kernel possono essere eseguite le istruzioni privilegiate e si può accedere alle aree protette della memoria

UNIX File Access Control

I file UNIX sono amministrati usando gli inodes (index nodes)

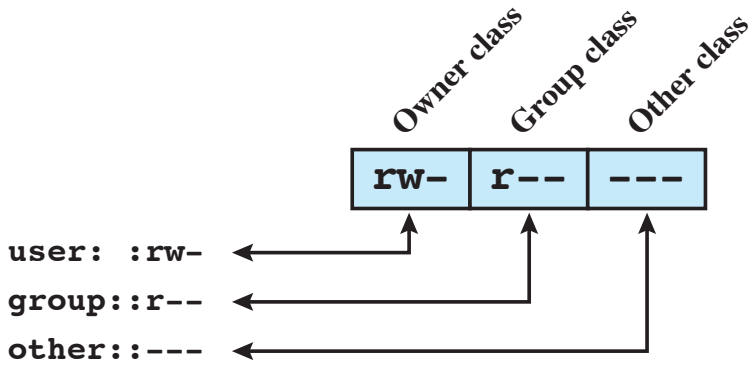
- Strutture di controllo con le informazioni chiave necessarie per un determinato file
- Diversi nomi di file possono essere associati a un singolo inode
- Un inode attivo è associato esattamente a un file
- Attributi di file, permessi e informazioni di controllo sono ordinati nell'inode
- Sul disco c'è una tabella di inode, o lista di inode, che contiene gli inode di tutti i file nel file system
- Quando un file viene aperto, il suo inode viene portato nella memoria principale e memorizzato in una tabella di inode residente in memoria

Le cartelle sono strutturate in un albero gerarchico

- Possono contenere files e/o altre cartelle
- Contengono I nomi dei files piu' i puntatori agli inodes

UNIX
File Access Control

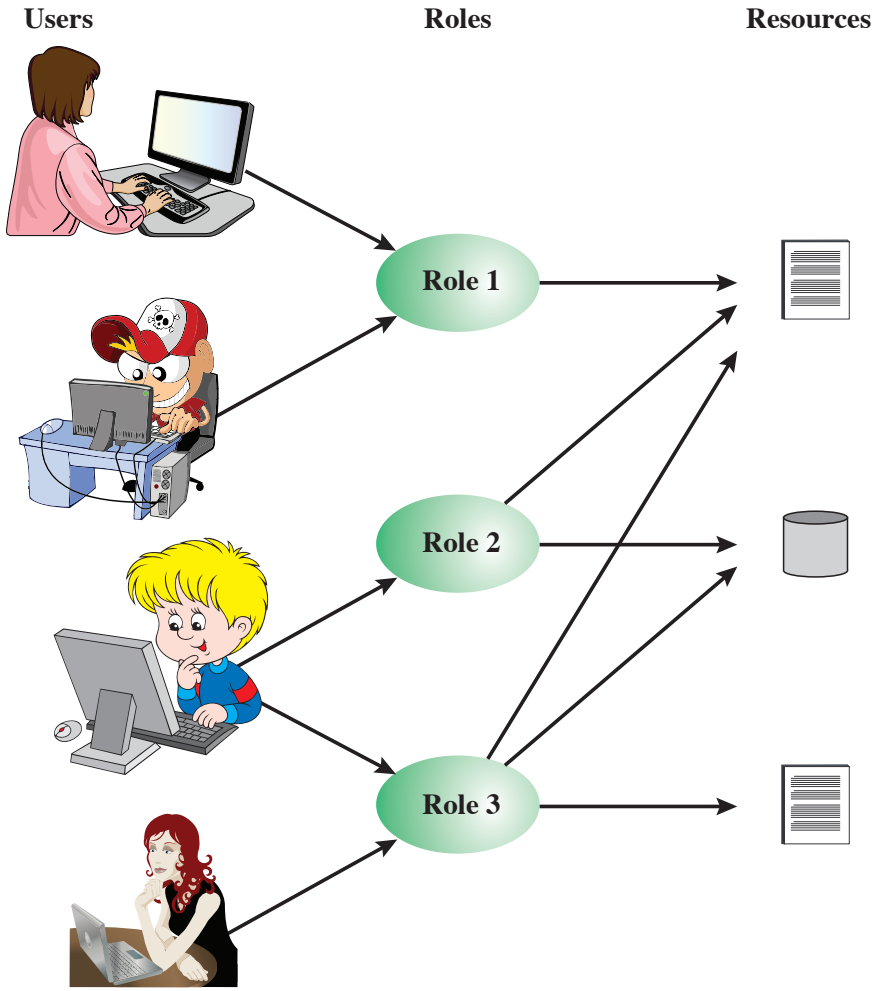
- Numero di identificazione utente unico (ID utente)
- Membro di un gruppo primario identificato da un ID di gruppo
- Appartiene ad un gruppo specifico
- 12 bit di protezione
  - Specifica permessi di lettura, scrittura ed esecuzione per il proprietario del file, i membri del gruppo e tutti gli altri utenti
- L'ID proprietario, l'ID di gruppo e i bit di protezione fanno parte dell'inode del file

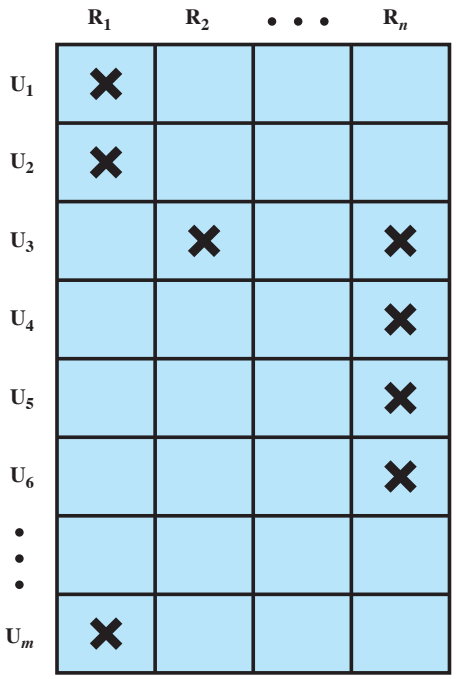


File Access Control Tradizionale UNIX

- "Set user ID"(SetUID)
- "Set group ID"(SetGID)
  - Il sistema utilizza temporaneamente i diritti del proprietario / gruppo del file in aggiunta aggiunta ai diritti dell'utente reale quando prende le decisioni sul controllo degli accessi
  - Consente ai programmi privilegiati di accedere a file / risorse generalmente non accessibili
- Sticky bit (bit 'appiccicoso')
  - Quando applicato a una directory specifica che solo il proprietario di qualsiasi file nella directory può rinominare, spostare o eliminare quel file
- Superuser
  - È esente dalle solite restrizioni di controllo degli accessi
  - Ha un accesso a livello di sistema

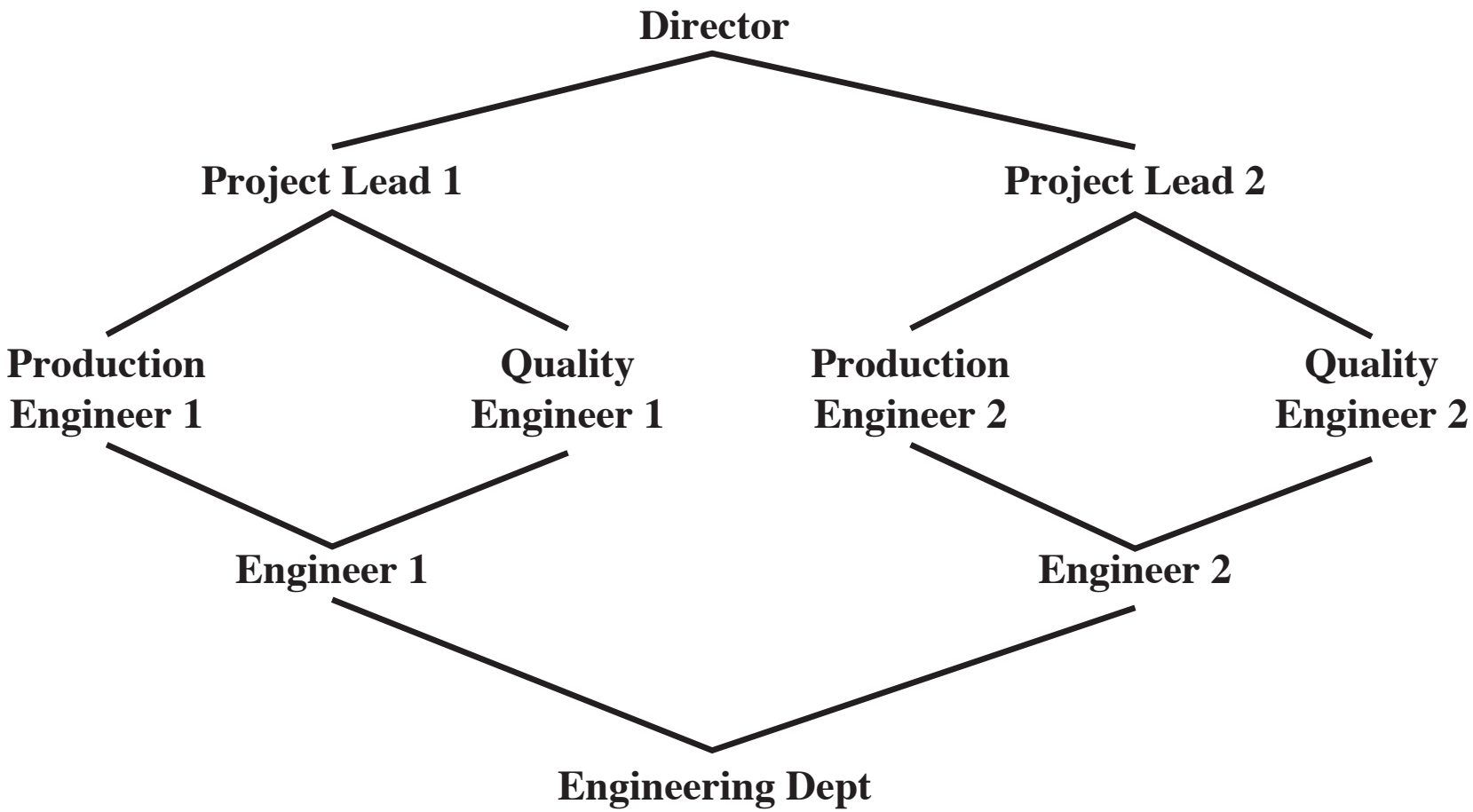
Controllo degli accessi basato sui ruoli (RBAC)





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			


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

RBAC con vincoli

Fornisce meccaqnismi per adattare RBAC alle politiche amministrative o di sicurezza specifiche di un'organizzazione

Si possono specificare delle relazioni tra I ruoli o delle condizioni che I ruoli devono soddisfare

Tipi:

Ruoli Mutuamente esclusivi

- Un utente puo' essere assegnato soltanto ad un ruolo nell'insieme (staticamente o dinamicamente)
- Ogni diritto di accesso puo' essere abilitato soltanto ad uno dei ruoli dell'insieme

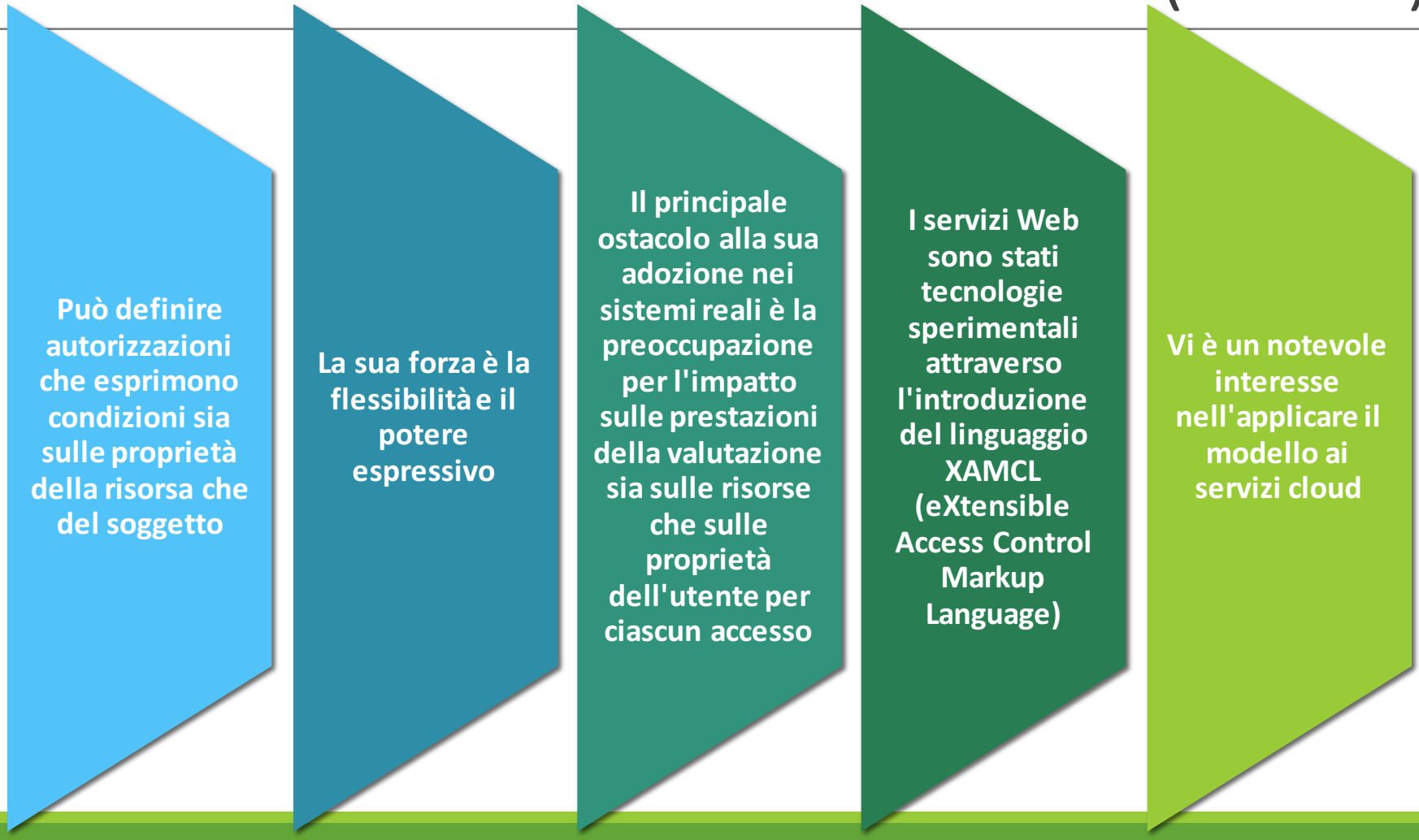
Cardinalità

- Impostare il massimo numero rispetto ad un ruolo

Ruoli prerequisiti

- Impone che un utente puo' essere assegnato ad un ruolo solo se e' gia' stato assegnato ad un altro ruolo specifico

Attribute-Based Access Control (ABAC)



ABAC Model: Attributes

Attributi del soggetto

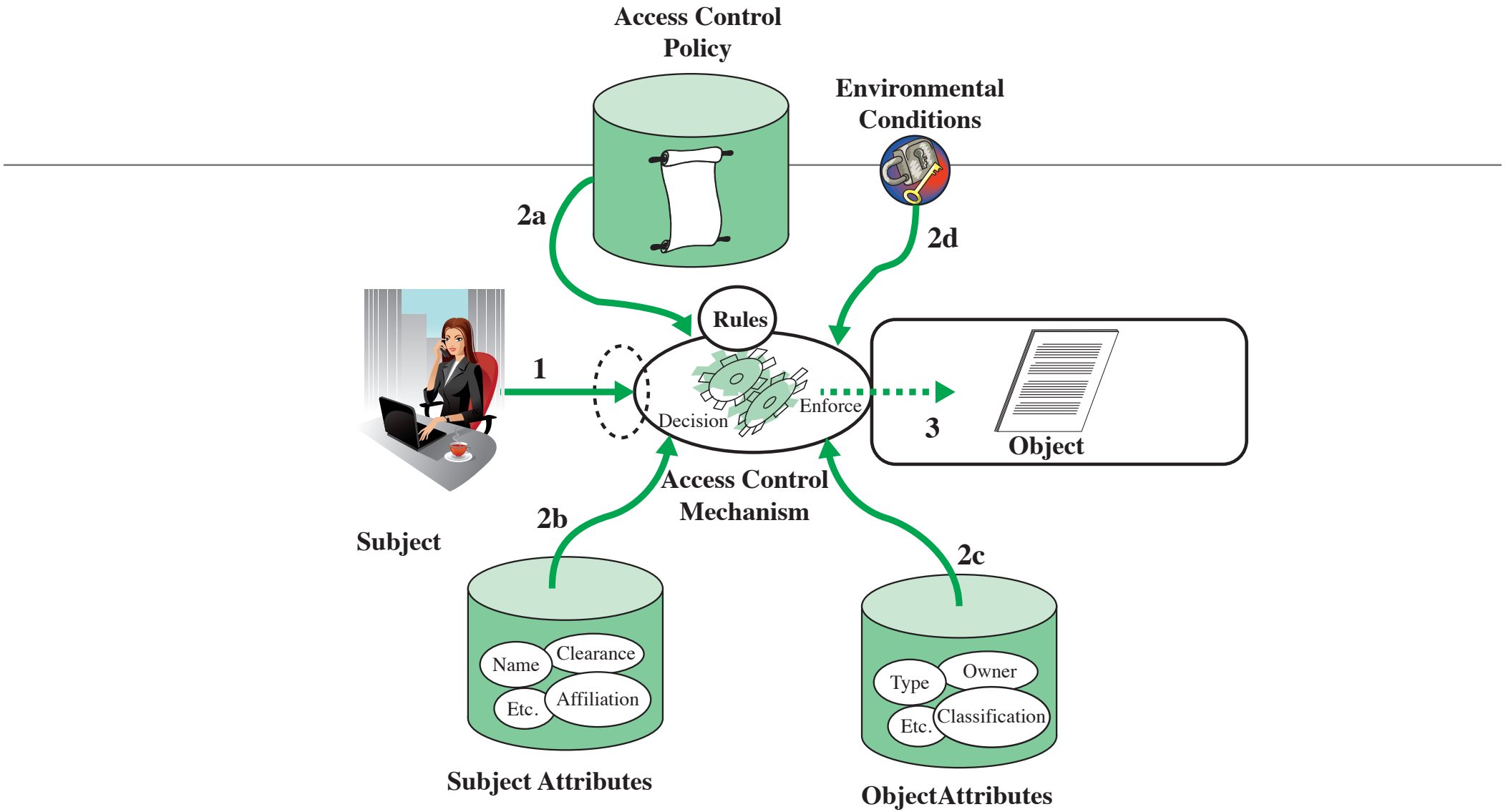
- Un soggetto è un'entità attiva che determina il trasferimento delle informazioni tra gli oggetti o modifica lo stato del sistema
- Gli attributi definiscono l'identità e le caratteristiche del soggetto

Attributi dell'oggetto

- Un oggetto (o risorsa) è un'entità passiva relativa al sistema informativo che contiene o riceve informazioni
- Gli oggetti hanno attributi che possono essere utili per prendere decisioni di controllo degli accessi

Attributi dell'ambiente

- Descrivere l'ambiente o il contesto operativo, tecnico e persino situazionale in cui si verifica l'accesso alle informazioni
- Questi attributi sono stati finora largamente ignorati nella maggior parte delle politiche di controllo degli accessi


Access Control Policy
Environmental Conditions
2a
2d
Rules
1
Decision
Enforce
3
Object
Access Control Mechanism
Subject
2b
2c
Name
Clearance
Etc.
Affiliation
Subject Attributes
Type
Owner
Etc.
Classification
ObjectAttributes