

# IBM Academic Initiative



## Z/OS Sicurezza (elementi) Lezione 6/12/2007





# Funzionalità' di sicurezza

## Security Functions



Authorized programs

Authorized functions  
APF authorization  
APF libraries

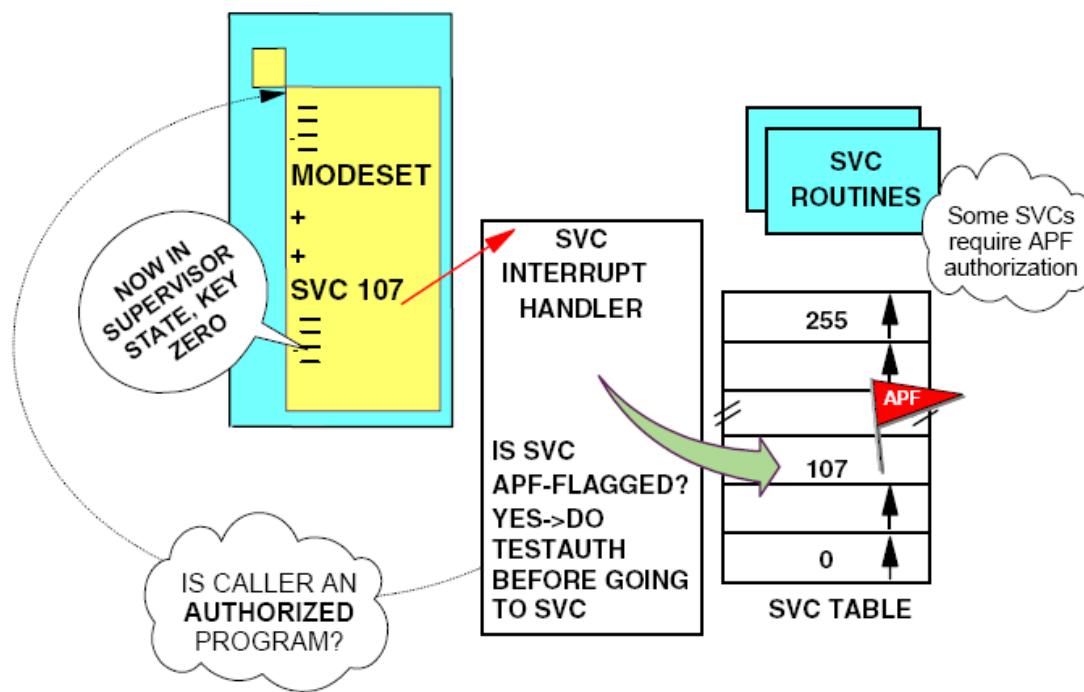
The Security Server

Network-Level Security  
System-Level Security  
Transaction-Level Security  
Cryptography  
LDAP directory



# Funzioni di sistema Autorizzate

## Authorized System Functions





## Richiamo di Architettura

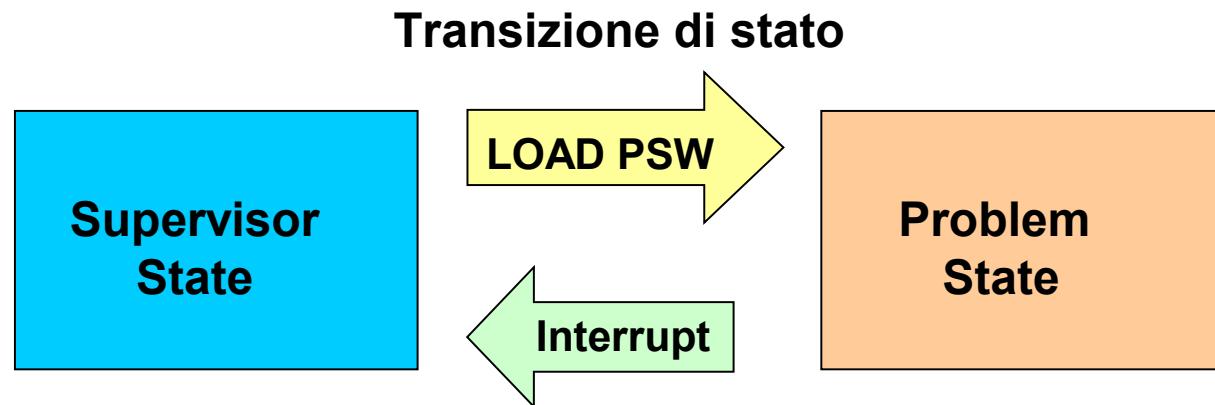
# Problem State (User Mode) e Supervisor State (Kernel Mode)

### Problem State (User Mode)

- un programma non deve eseguire istruzioni privilegiate, ovvero non puo' accedere a quelle parti dell'architettura che sono vitali per il sistema
- Non accede ai Control Registers, ai timers, alle chiavi di memoria ; accede solo alla parte non critica della PSW.

### Supervisor State (Kernel Mode)

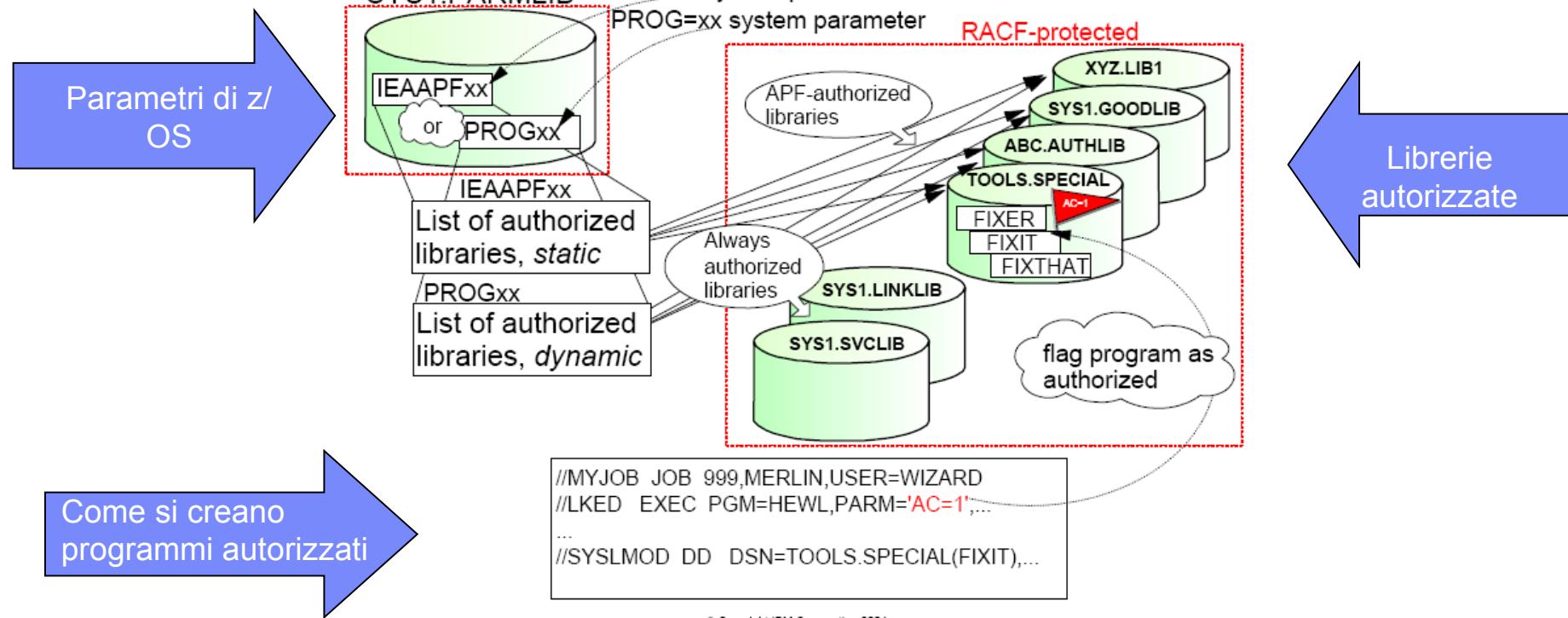
- un programma puo' esercitare tutte le potenzialità dell'architettura





# Authorized Program Facility(APF)

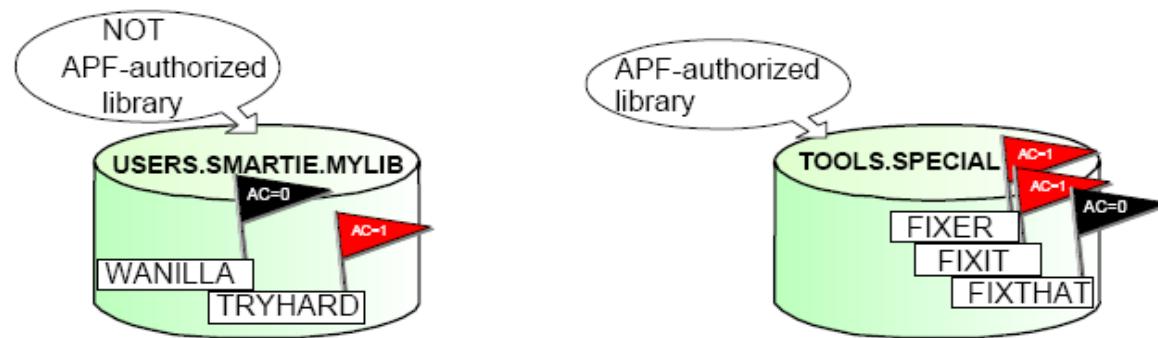
## Authorized Program Facility (APF)





# Programmi e Librerie APF

## APF Programs and APF Libraries



```
//MYJOB JOB 999,MYSELF,USER=SMARTIE  
//DOIT EXEC PGM=TRYHARD  
//STEPLIB DD DSN=USERS.SMARTIE.MYLIB,...
```

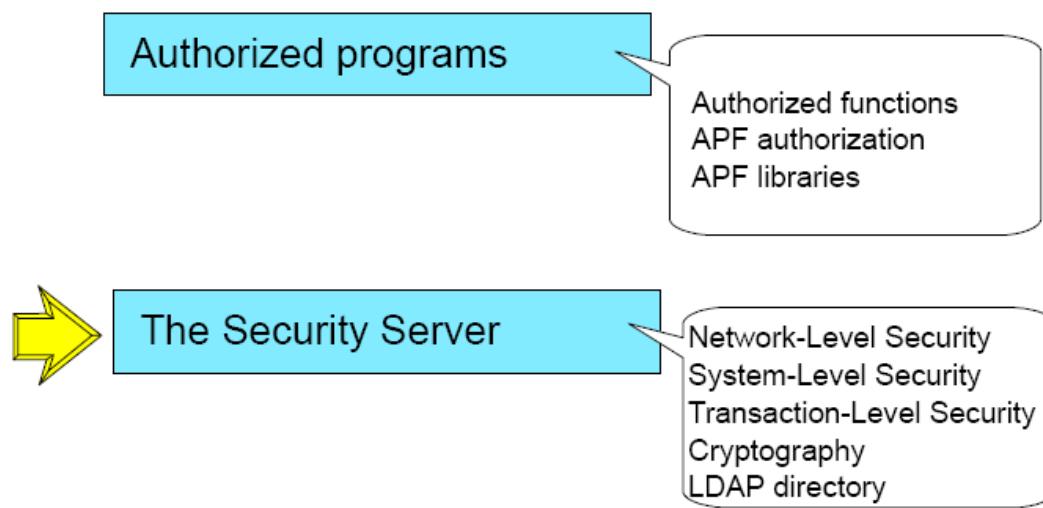
```
//MYJOB JOB 999,MERLIN,USER=WIZARD  
//DOIT EXEC PGM=FIXER  
//STEPLIB DD DSN=TOOLS.SPECIAL,...
```



# z/OS Security Server

## Security for Business

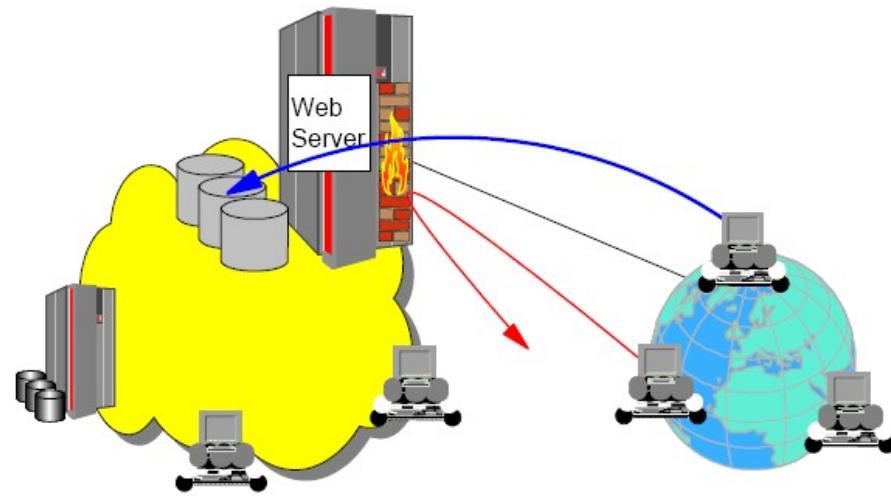
---





# Controllo della sicurezza di rete

## Network-Level Security Checking

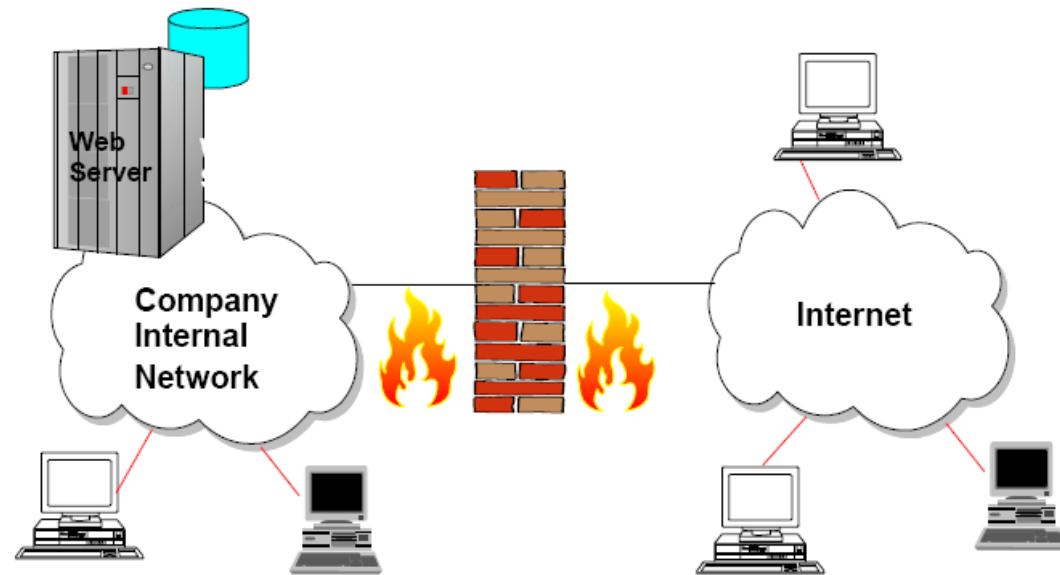


**Protezione di risorse di una rete privata connessa ad internet**



# Tecnologie di Firewall

## Firewall Technologies (1 of 2)

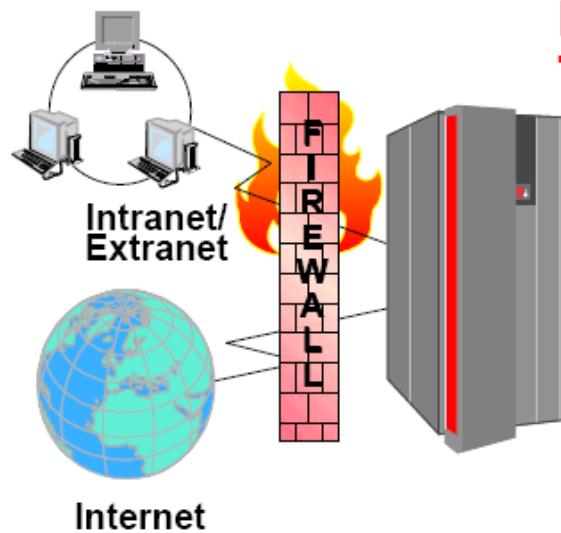




# Tecnologie di Firewall

## Firewall Technologies (2 of 2)

### Network Level



### Firewall Technologies

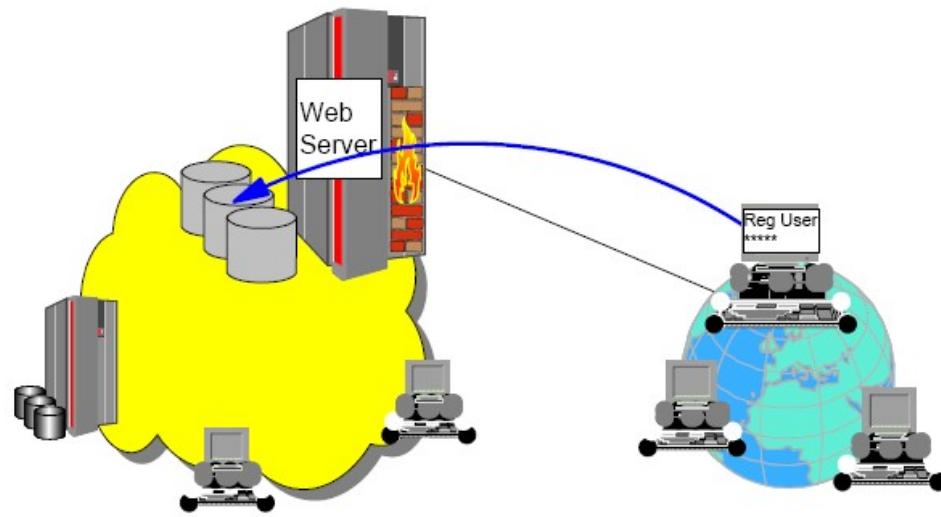
- IP Filtering
- Proxy and SOCKS Servers
- Domain Name Services
- Network Address Translation (NAT)
- Virtual Private Network (VPN)

© Copyright IBM Corporation 2004



# Controllo della sicurezza di sistema

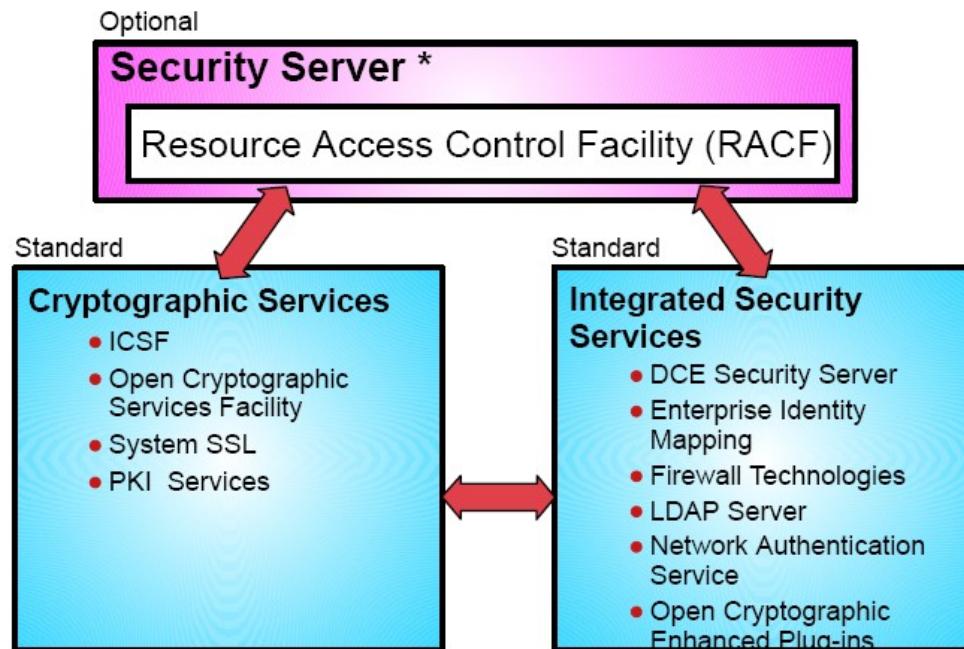
## System-Level Security Checking



Protezione di dati e applicazioni di un'azienda



## Overview of z/OS Security Services

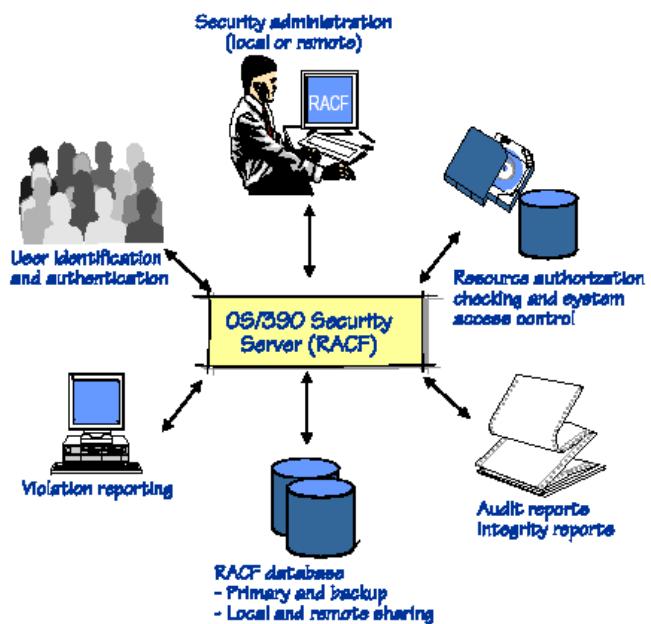


\* From OS/390 V2R9 to z/OS V1R2, component name was **SecureWay Security Server**

© Copyright IBM Corporation 2005



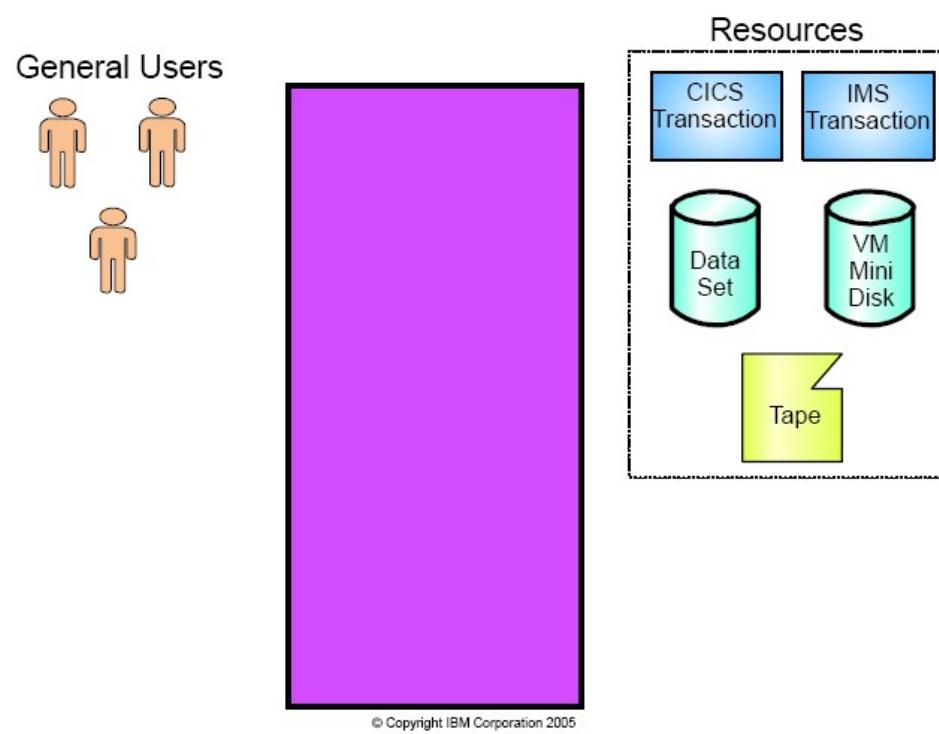
# Security Server (RACF)



- Authentication
  - Traditional or with “password alternatives”
- Authorization
  - Integration with most z/OS subsystems
- Administration
- Reporting
- Data management
- Auditing

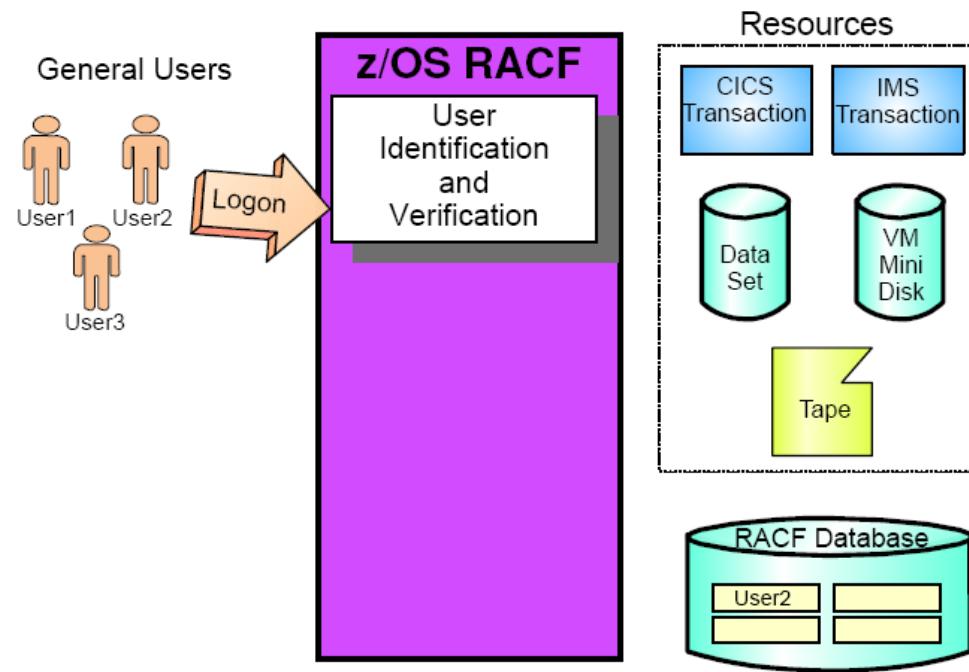


## System without RACF



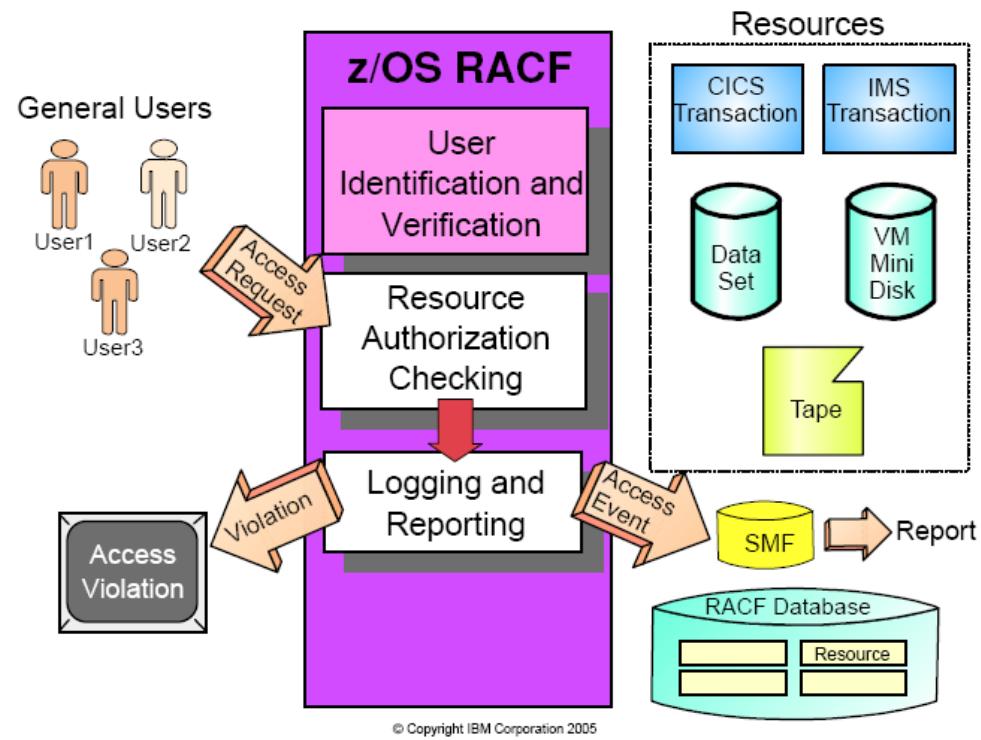


## System With RACF: User Authentication

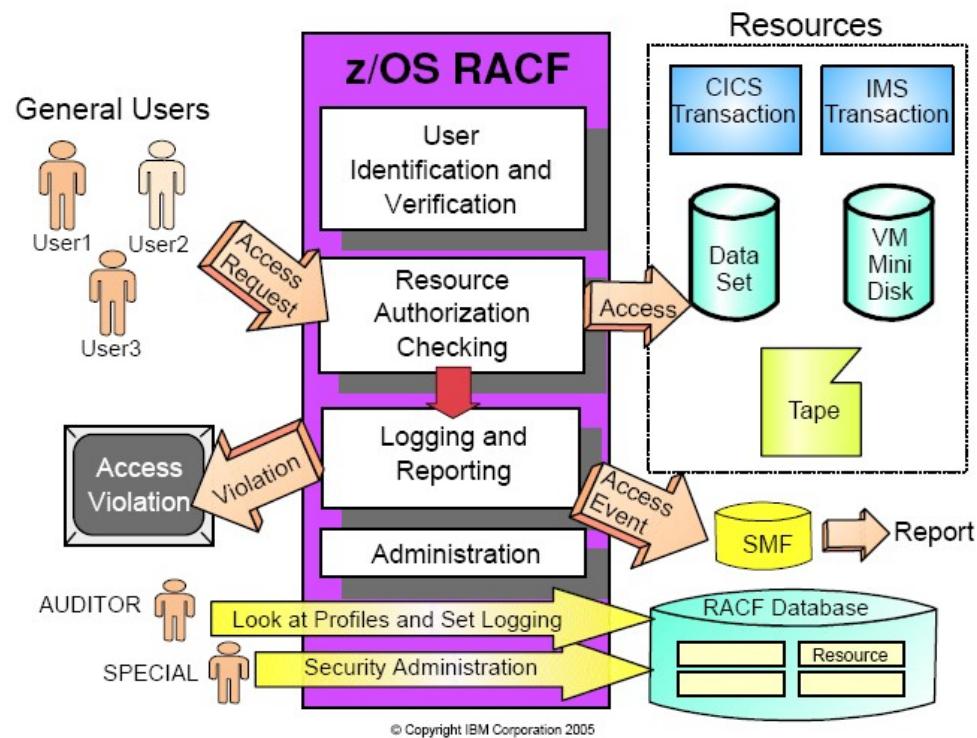


© Copyright IBM Corporation 2005

## Logging and Reporting



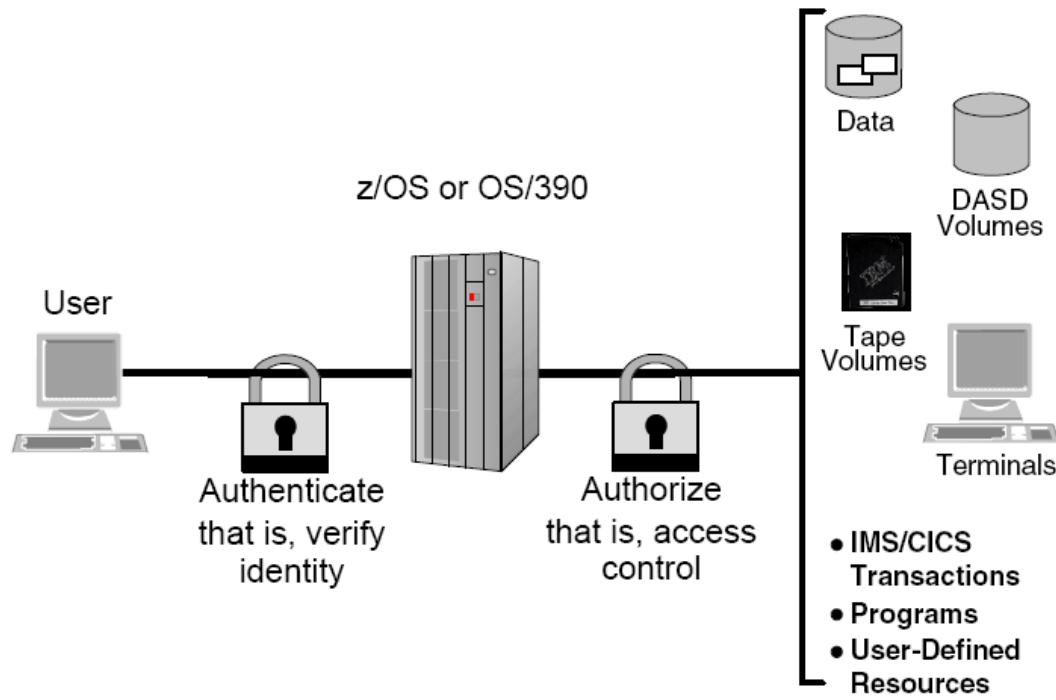
## RACF Major Function





# Protezione delle risorse di sistema

## Protecting System Resources

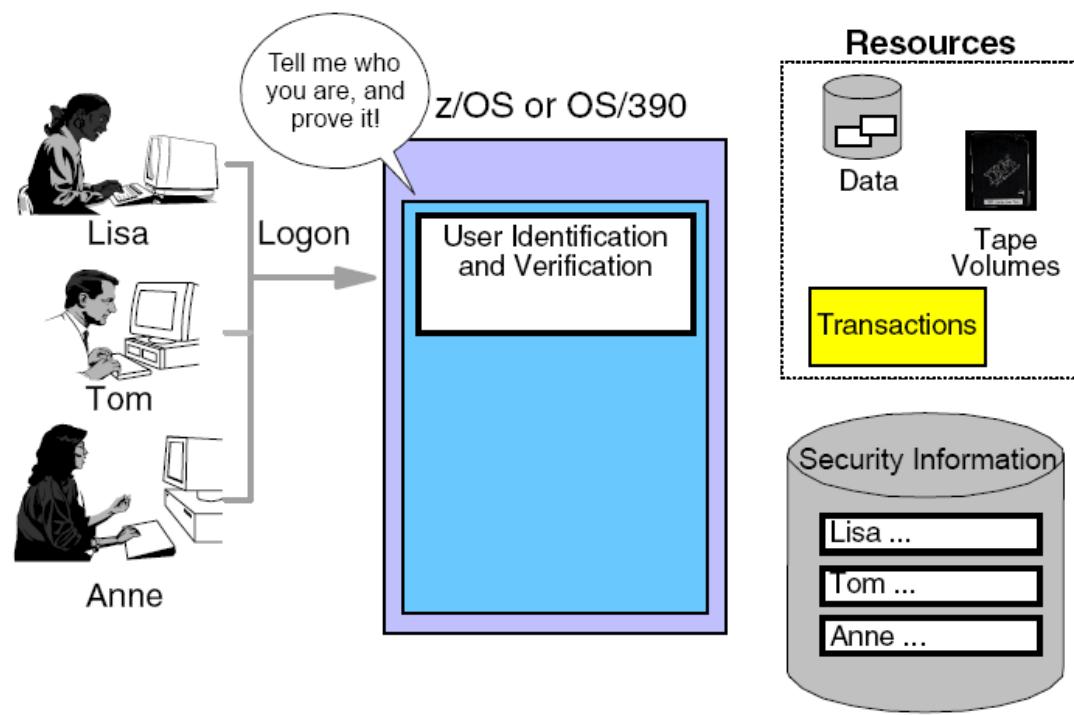


© Copyright IBM Corporation 2004



# Controllo di Autenticazione

## User Authentication





## User Profile

---

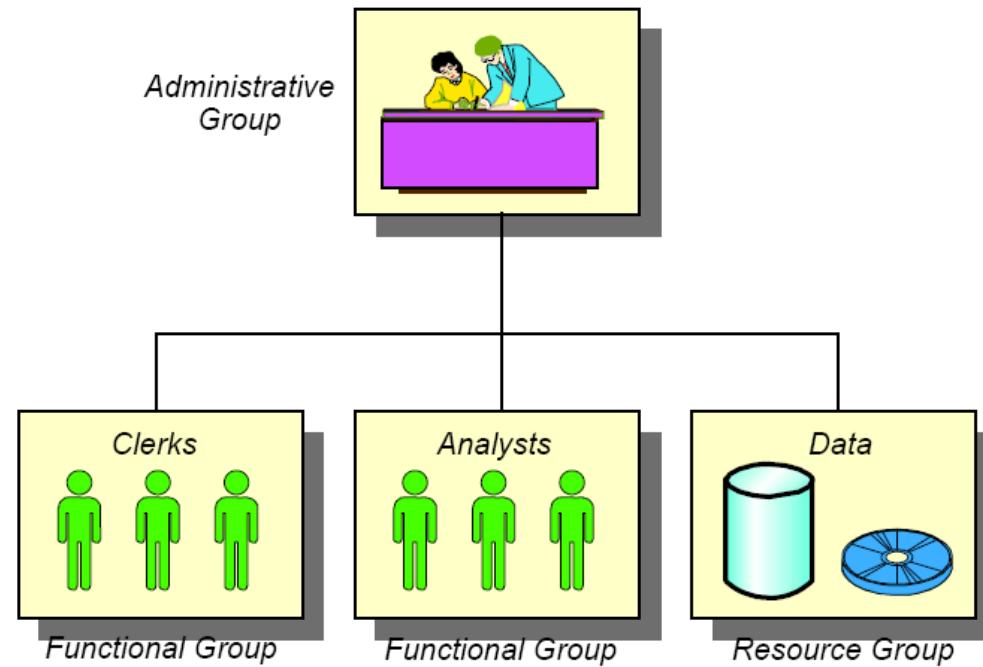


© Copyright IBM Corporation 2005



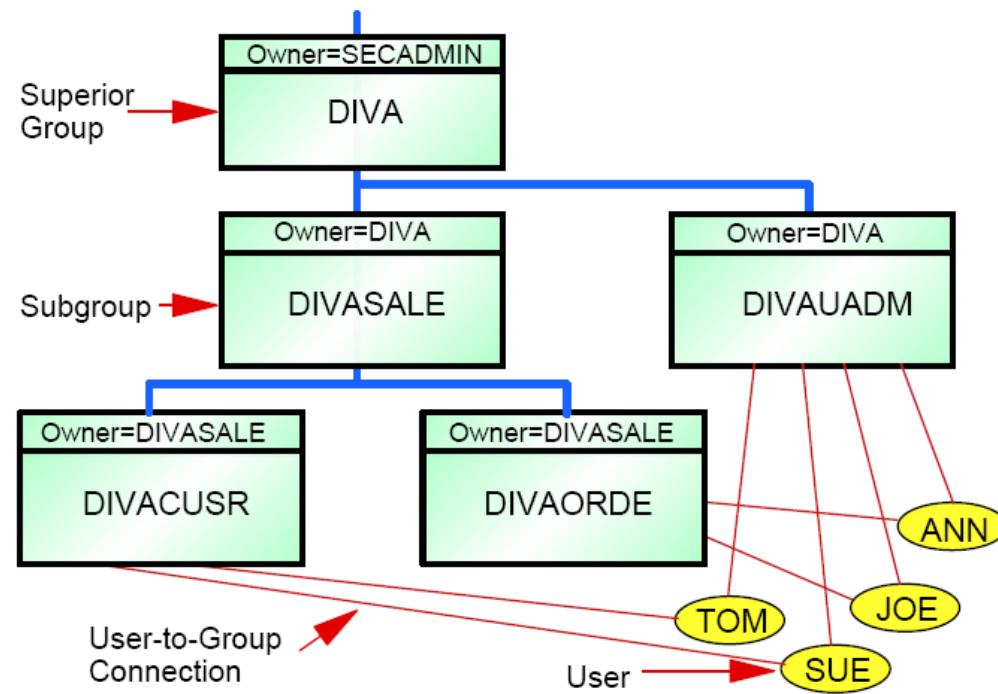
## Groups

---



© Copyright IBM Corporation 2005

## Security Server RACF Group Terminology

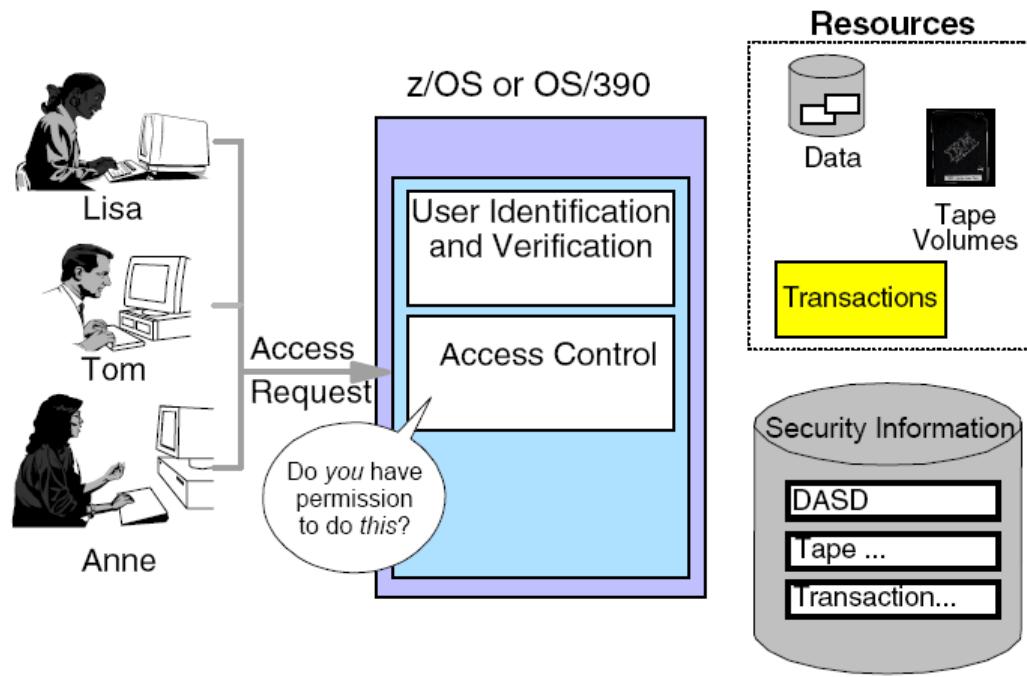


© Copyright IBM Corporation 2005



# Controllo di Autorizzazione

## Authorization Control

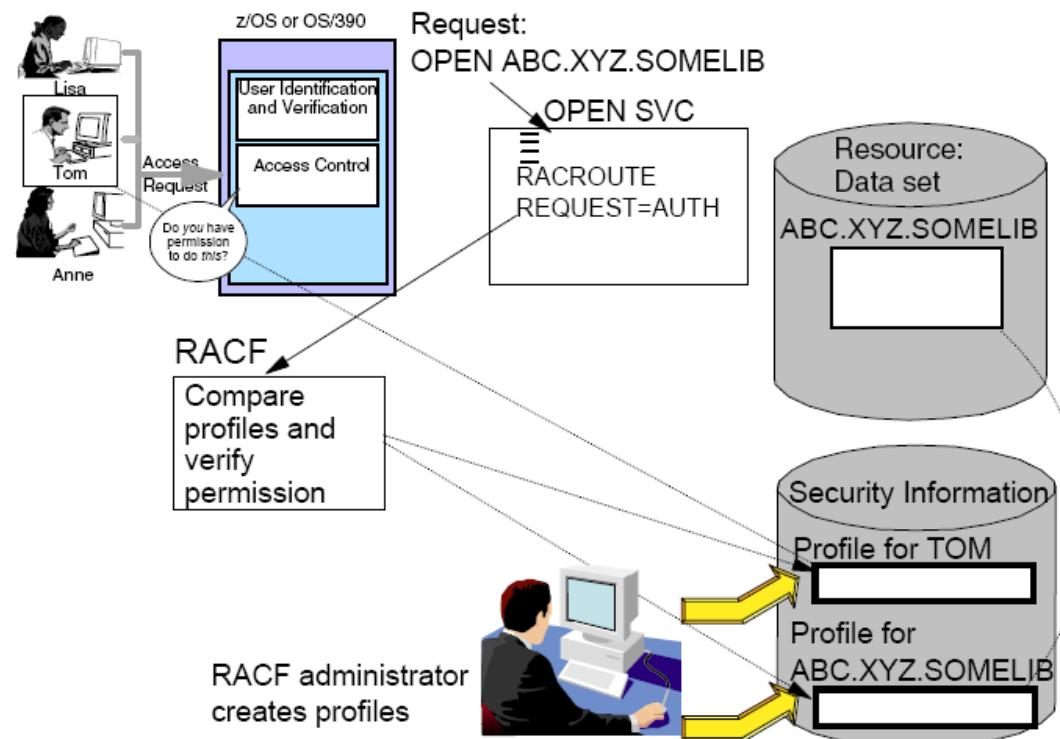


© Copyright IBM Corporation 2004

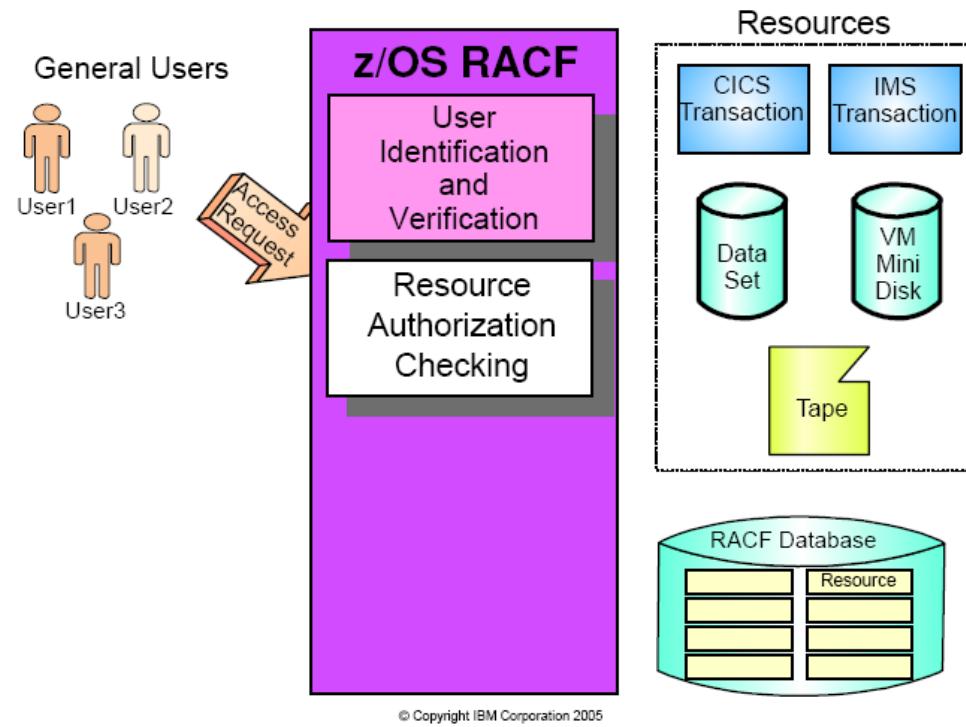


# Controllo di Accesso ai data set

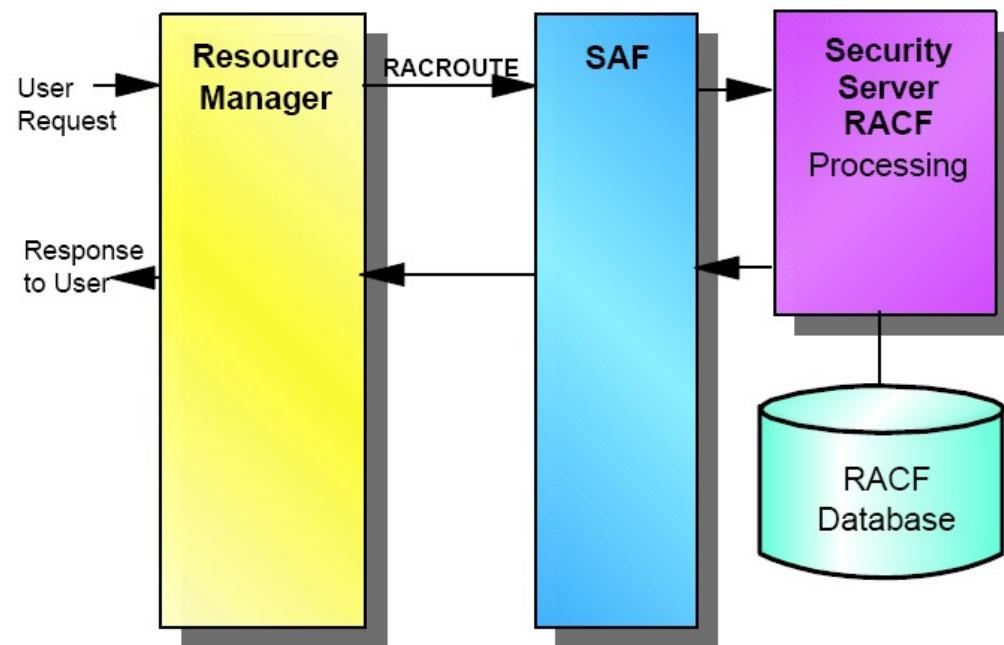
## Access Control for a Data Set



## Resource Authorization Checking



## Resource Managers and RACF



© Copyright IBM Corporation 2005



## RACF Resource Profile

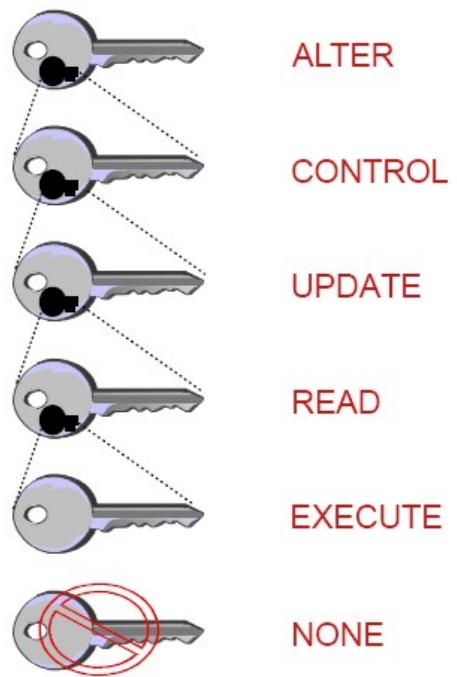
---

Profile Name	Owner	UACC	Access List	Security Classification	Auditing
--------------	-------	------	-------------	-------------------------	----------

© Copyright IBM Corporation 2005



## Access Authorities for Data Sets

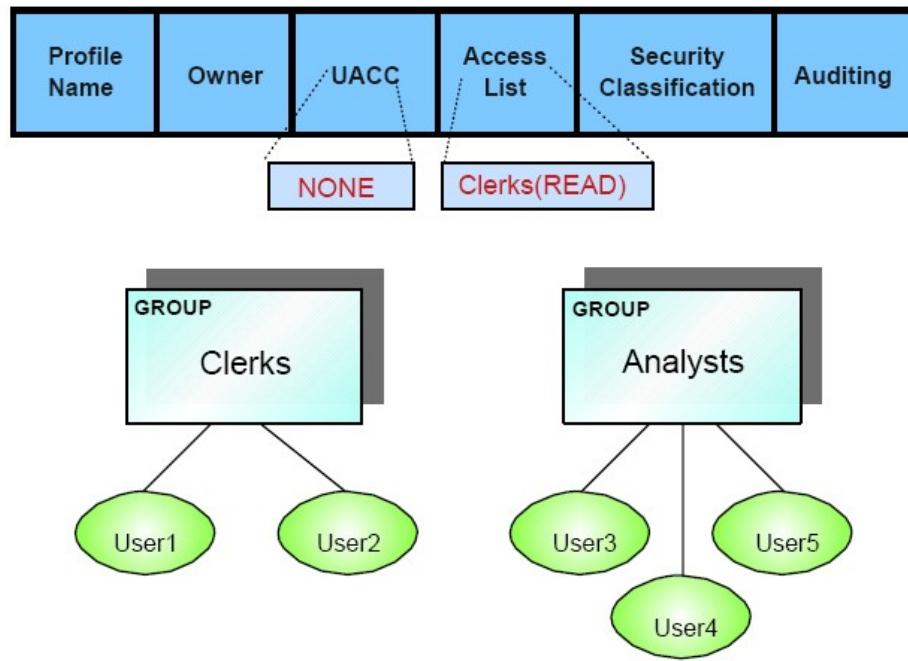


© Copyright IBM Corporation 2005



## Example - Authorization Checking

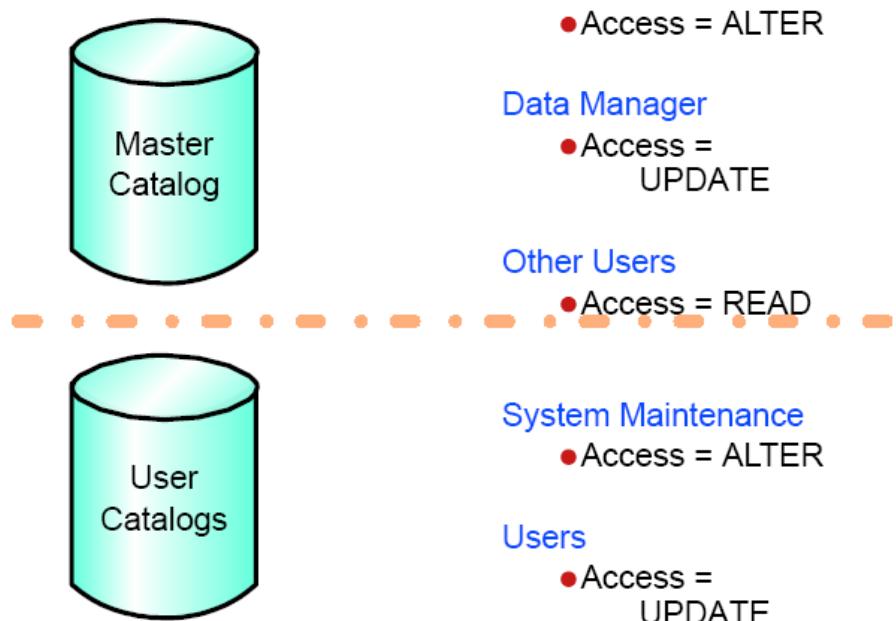
---



© Copyright IBM Corporation 2005



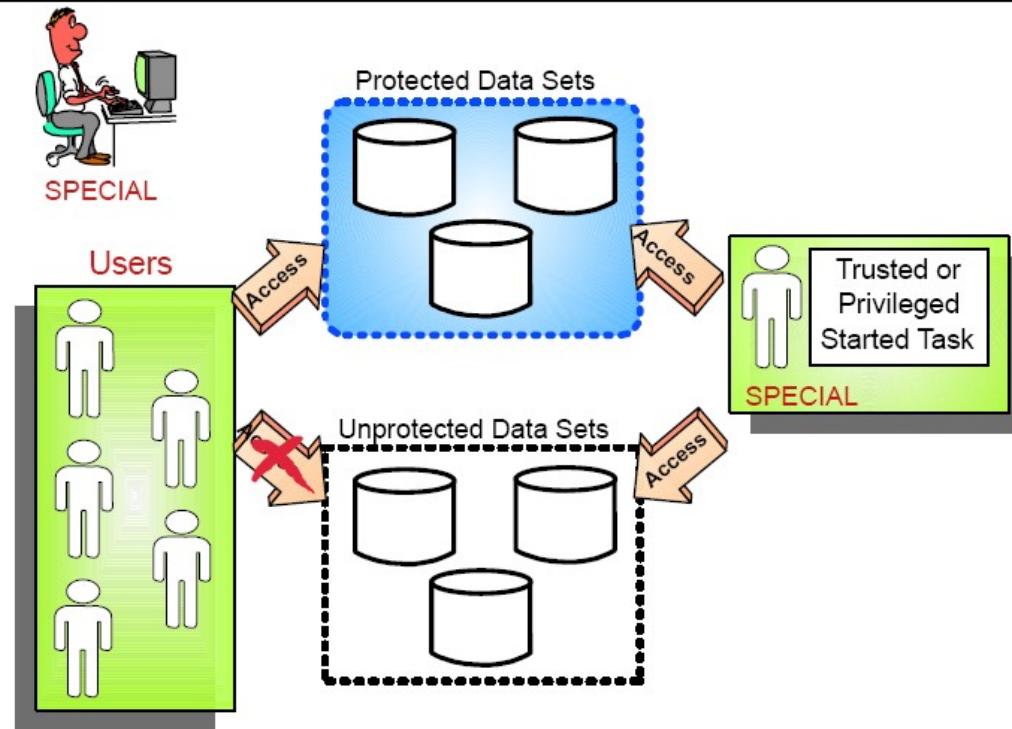
## Protecting Catalogs Example



© Copyright IBM Corporation 2005



## Protect - All



© Copyright IBM Corporation 2005



## Generic versus Discrete Profiles

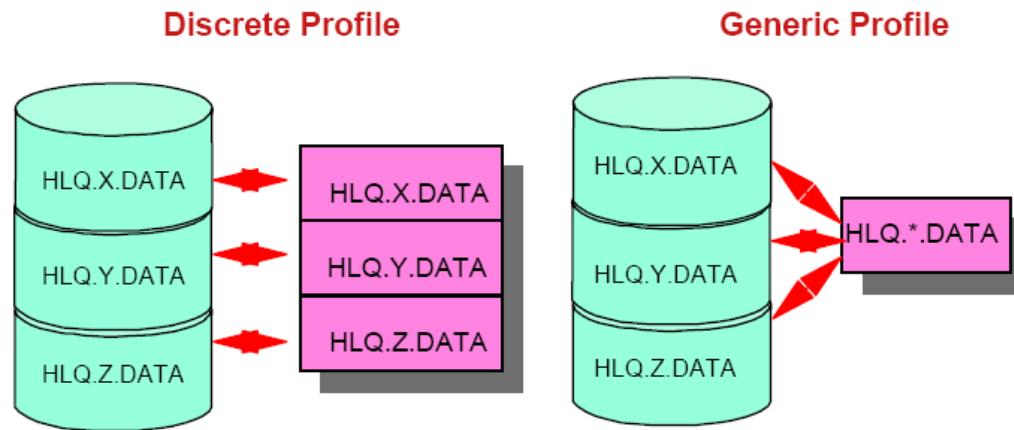
Generic	Discrete
<ul style="list-style-type: none"><li>• Many data sets can be protected with one profile</li><li>• Profile exists even if all data sets are deleted</li><li>• Covers data sets on any volume</li><li>• No RACF indicator bit on</li><li>• Easier to administer</li></ul>	<ul style="list-style-type: none"><li>• One profile for each data set</li><li>• Profile automatically deleted when data set is deleted</li><li>• Specific to a volume and unit</li><li>• RACF indicator bit set on</li></ul>

© Copyright IBM Corporation 2005



## Discrete and Generic Profiles

---

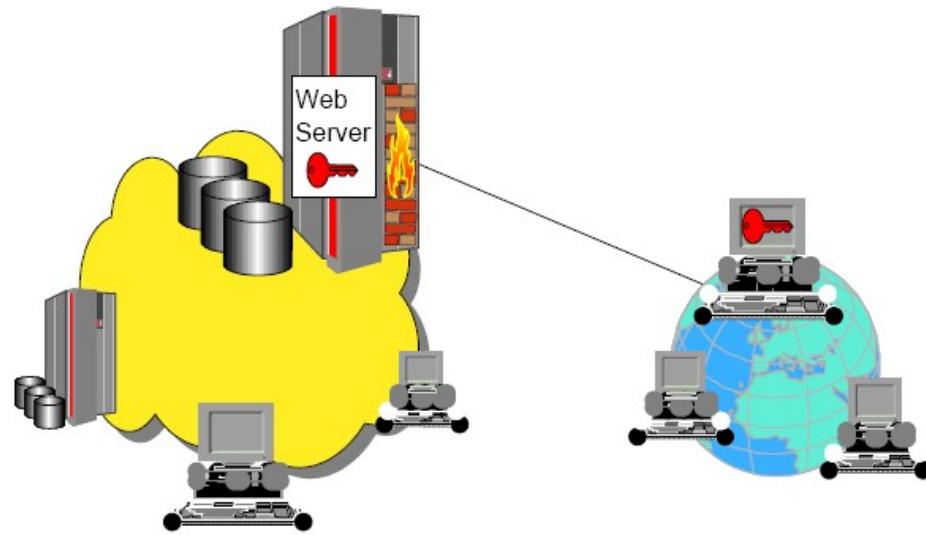


© Copyright IBM Corporation 2005



# Controllo della sicurezza di transazione

## Transaction-Level Security

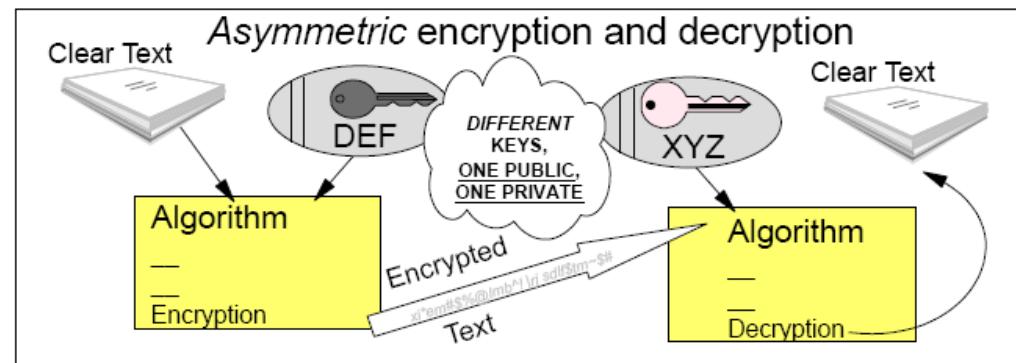
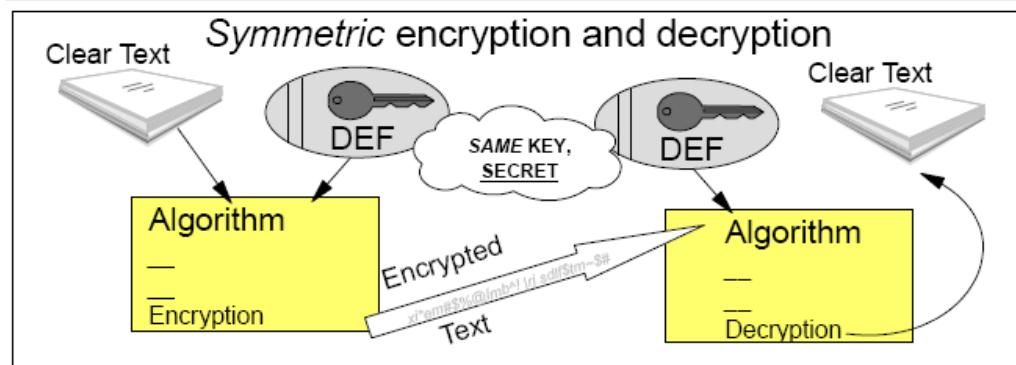


**FCapacità di due entità in Internet di condurre una transazione privata e con autenticazione**



# Crittografia – Concetti Base

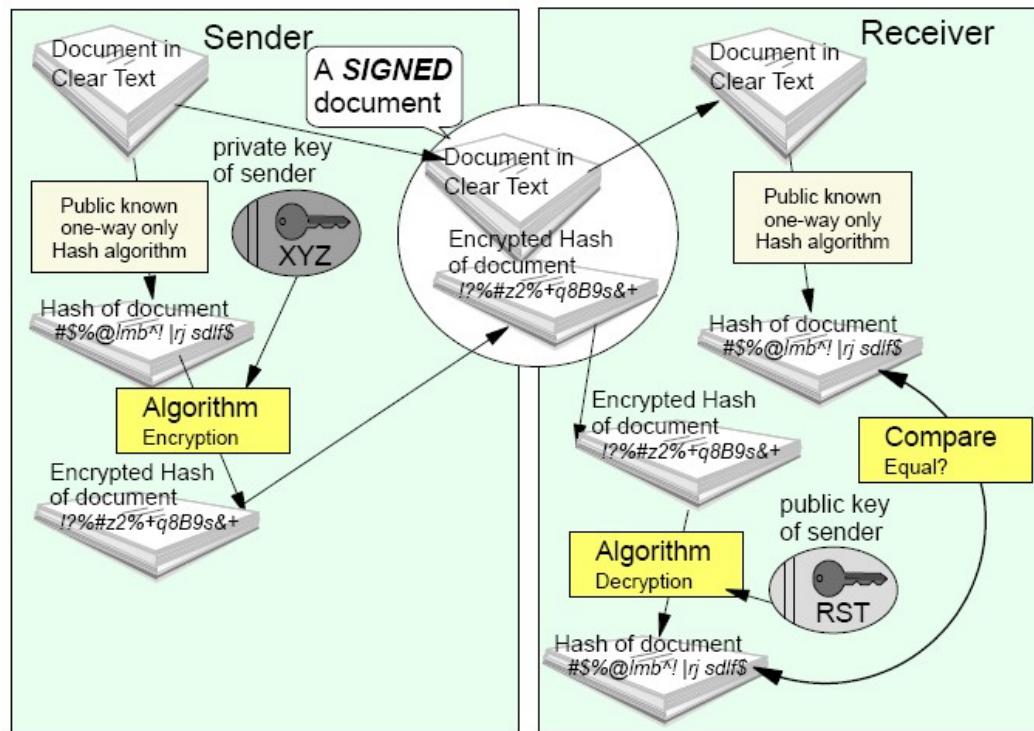
## Cryptography - Basics





# Crittografia – Firma Digitale

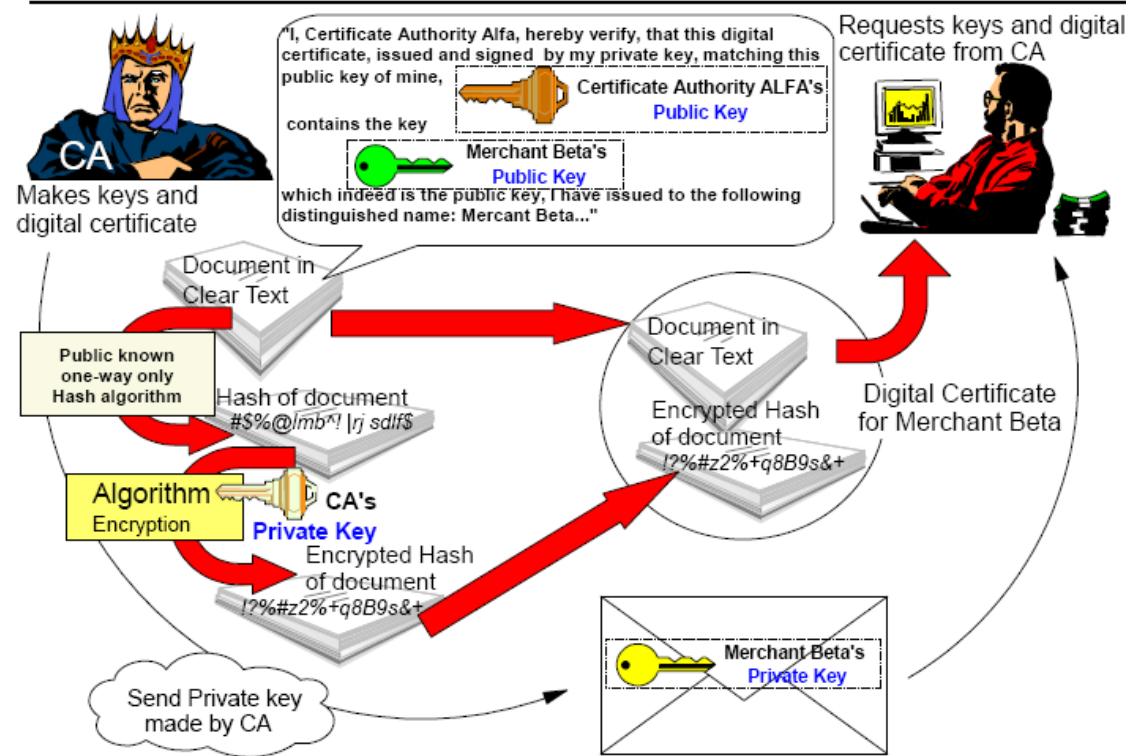
## Cryptography - Signing





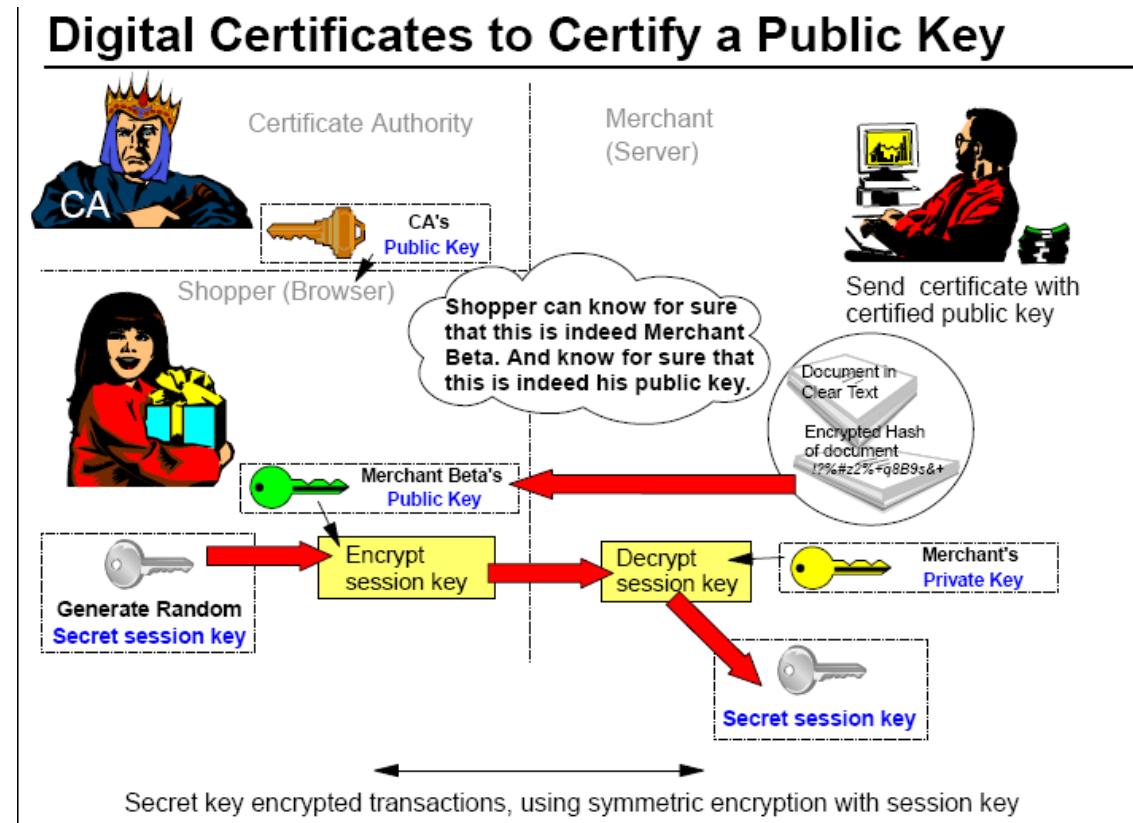
# Certificati digitali

## Certificate Authority and Digital Certificates





# Certificati digitali e chiavi pubblica

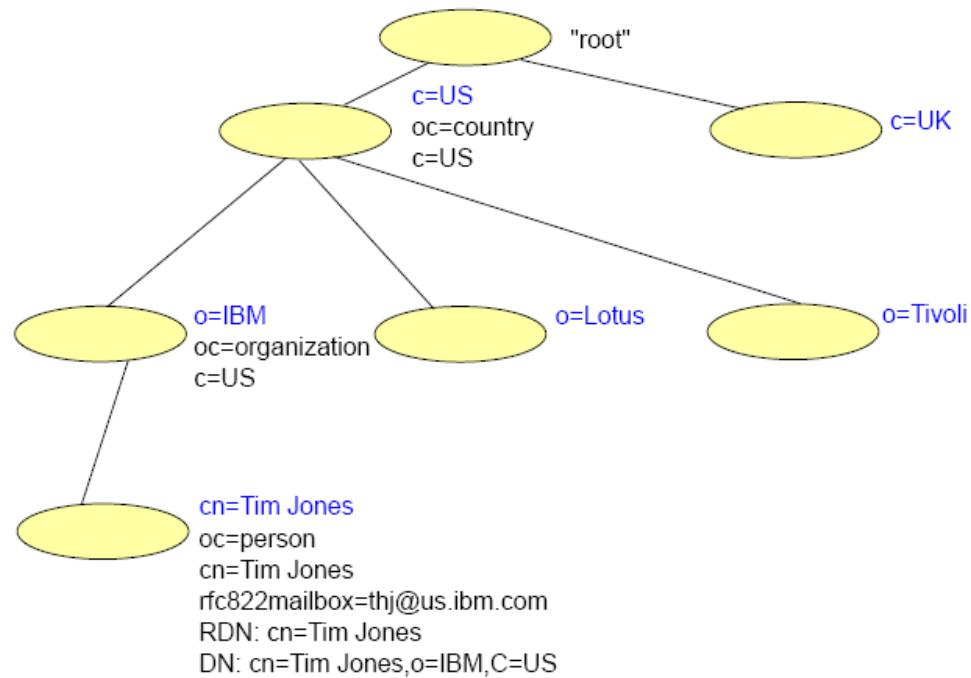




# Directory

## Directory Information and Structure

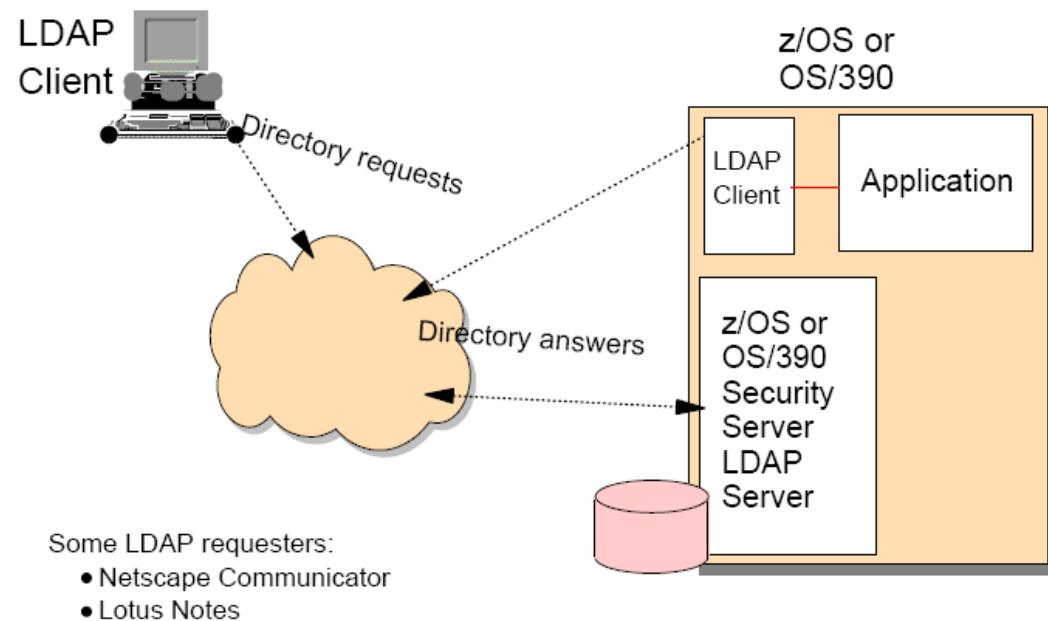
---





# LDAP Server

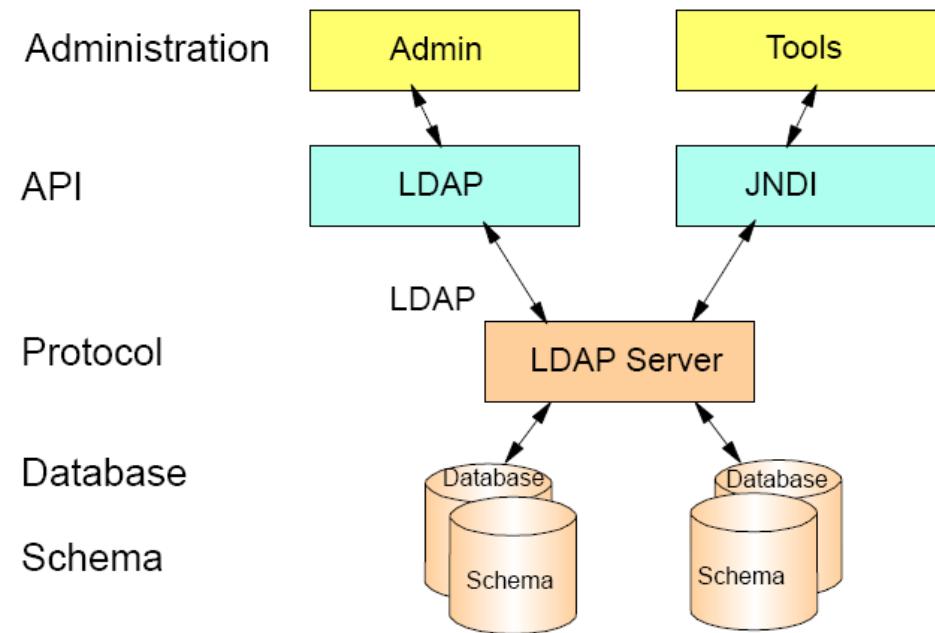
## LDAP Server





# Componenti di LDAP

## LDAP Components



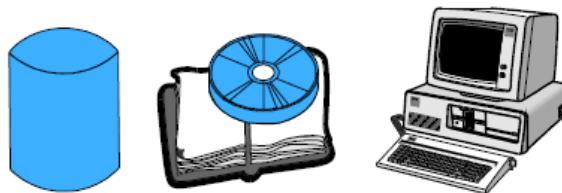
© Copyright IBM Corporation 2004



## Data Security Is

*The protection of data from unauthorized*

- Destruction
- Modification
- Disclosure
- Use

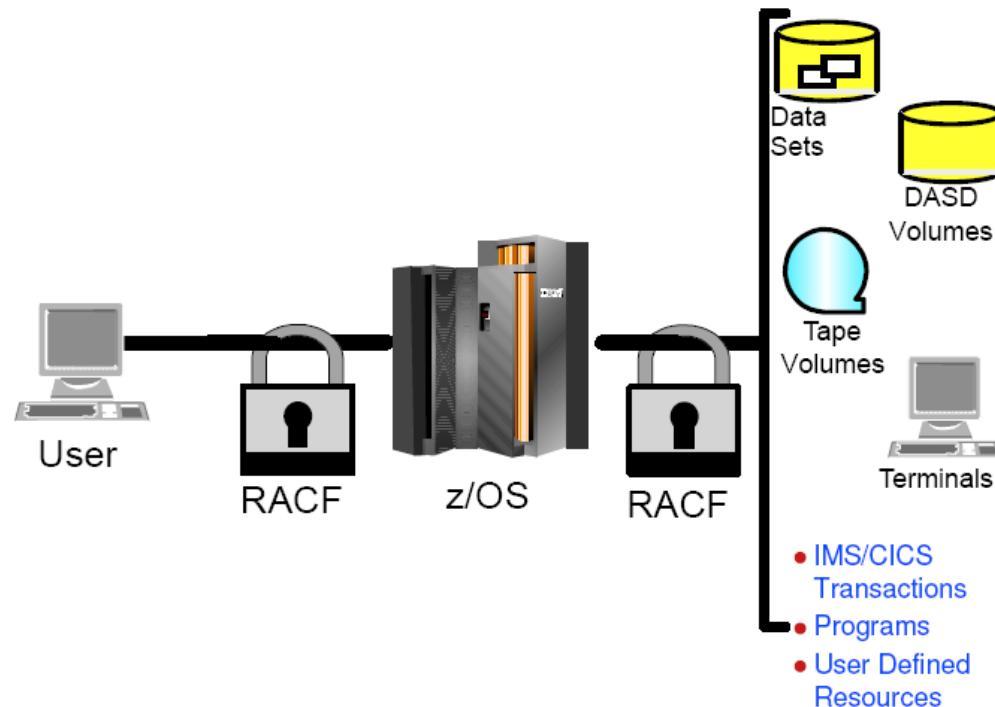


*whether accidental or intentional*

© Copyright IBM Corporation 2005



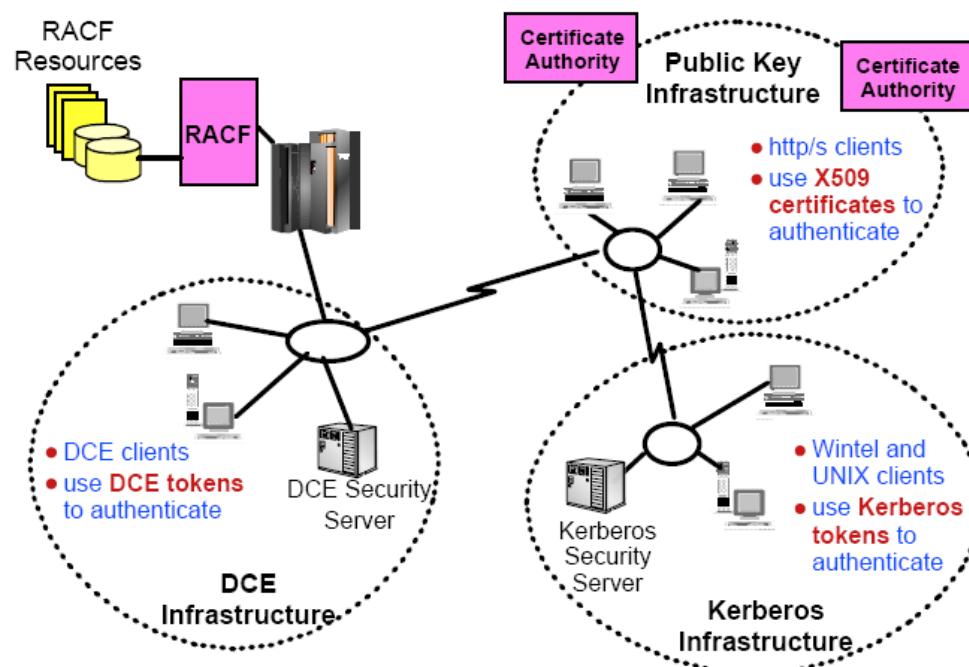
## Security Server RACF Overview



© Copyright IBM Corporation 2005



## Security in a Distributed Environment



## Distributed SignOn

