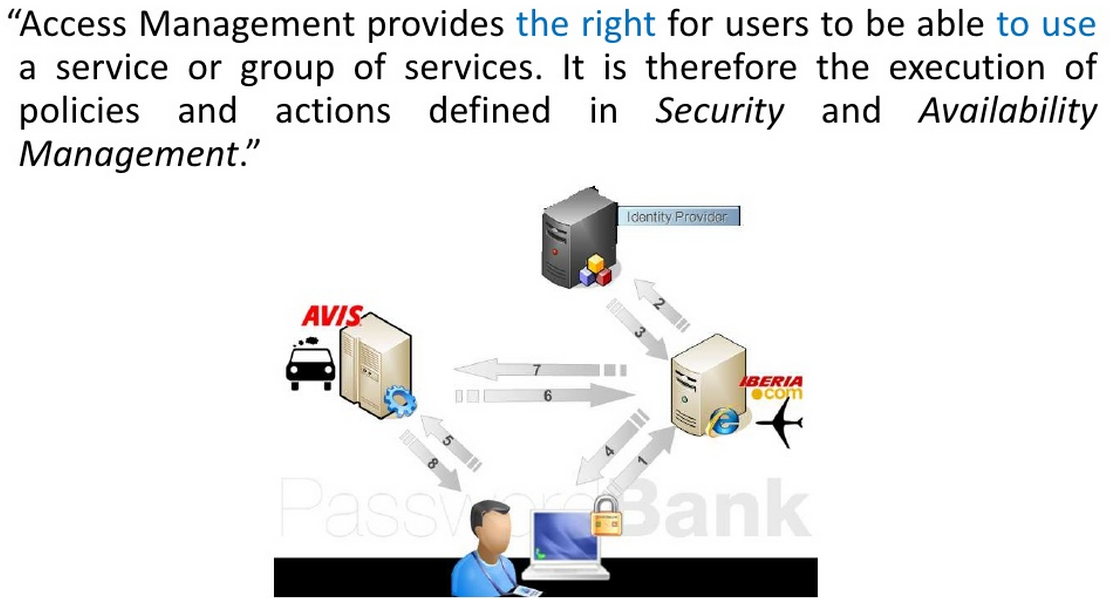
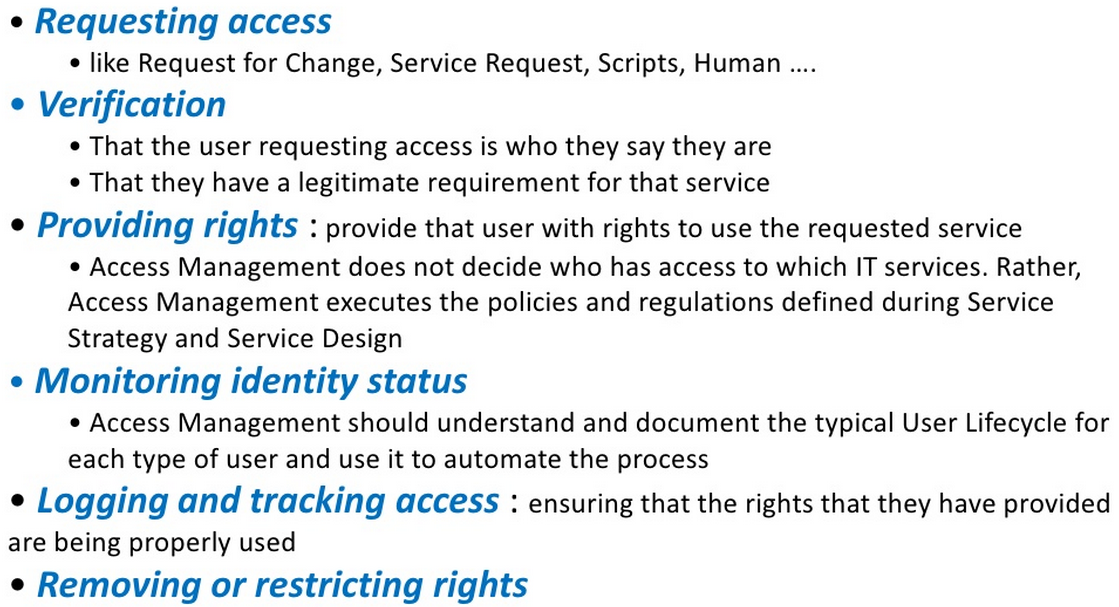
**Access Management**



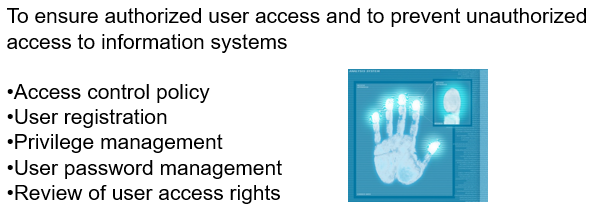
**Access Management: Objectives**



**Access Management: Process**



**Access Management: Control Access**



**Additional Measurements: User Responsibilities**

To prevent unauthorized user access and compromise or theft of information and information processing facilities

* Password use
* Unattended user equipment
* Clear desk and clear screen policy

**Additional Measurements: Network Control**

To prevent unauthorized access to networked services

* Policy on the use of network services
* User authentication for external connections
* Equipment identification in networks
* Remote diagnostic and configuration port protection
* Segregation in networks
* Network connection control
* Network routing control
* …

**Additional Measurements: Operating System**

To prevent unauthorized access to operating systems

* Secure log-on procedures
* User identification and authentication
* Password management system
* Use of system utilities
* Session time-out
* Limitation of connection time
* …

**Additional Measurements: Applications**

To prevent unauthorized access to information held in application systems

* Information access restriction
* Sensitive system isolation
* …

**Additional Thoughts:**

* Where is Window OS file access management?
* Where is Linux OS file access management?
* Examples of Access Managements:
* I forget my passwords.
* I am log-out of access to the system, because I try too many time.
* How can IT help users to remember his/her passwords?
* …
* We have we strict IT rules. But we have client demanding a piece of critical info. Any work-around suggestions? An example:
  + FTP transfer to a depot of specific info.
  + FTP data has 10-day expiration date.
  + Data transfer to the FTP server, by who?
  + …