CISSP® 2015

Domain 5: Identity & Access Management

V1

Domain 5: Identity & Access Management

A. Control Physical & Logical access to assets

- Information & System
  - More on intangible, more controls on logical access, say username password, access right, e-cert, token, biometric etc.
- Devices & Facilities
  - More on tangible, more physical access control, say cable lock, door, windows, entry lock, security guard, straight line of sight, server room controls etc.

Access Control Administration

- **Administration:** involve implementing, monitoring, modifying, testing and terminating user accesses
- **Who is decision maker of access right?**
  - **Centralized Access Control Administration**
    - One entity (dept or individual) is responsible for overseeing access to all resources.
    - **More consistent and reliable, but may be slow**
  - **Decentralized Access Control Administration**
    - decentralize the control access to the people closer and have better understanding to the resources, such as functional manager
    - **Advantage**: change could be faster
    - **Disadvantage**: Not consistent, not fairness across the organization

B. Manage identification & authentication of people and devices

- **Access Controls Overview**
  - Control how users and systems access with other systems and resources
  - Define the relationship of **Subjects** and **Objects**
  - **Subject**: can be user, program or process
  - **Object**: can be DB, file, directory, field, computer, program….
  - Authorized and Unauthorized access
  - Extremely important, 1st line defense

4 Steps in Access Control

1. **Identification**: define who you are, ie user ID
2. **Authentication**: verify who you are, ie pwd, token
3. **Authorization**: what you can access
4. **Accountability**: accountable for your actions

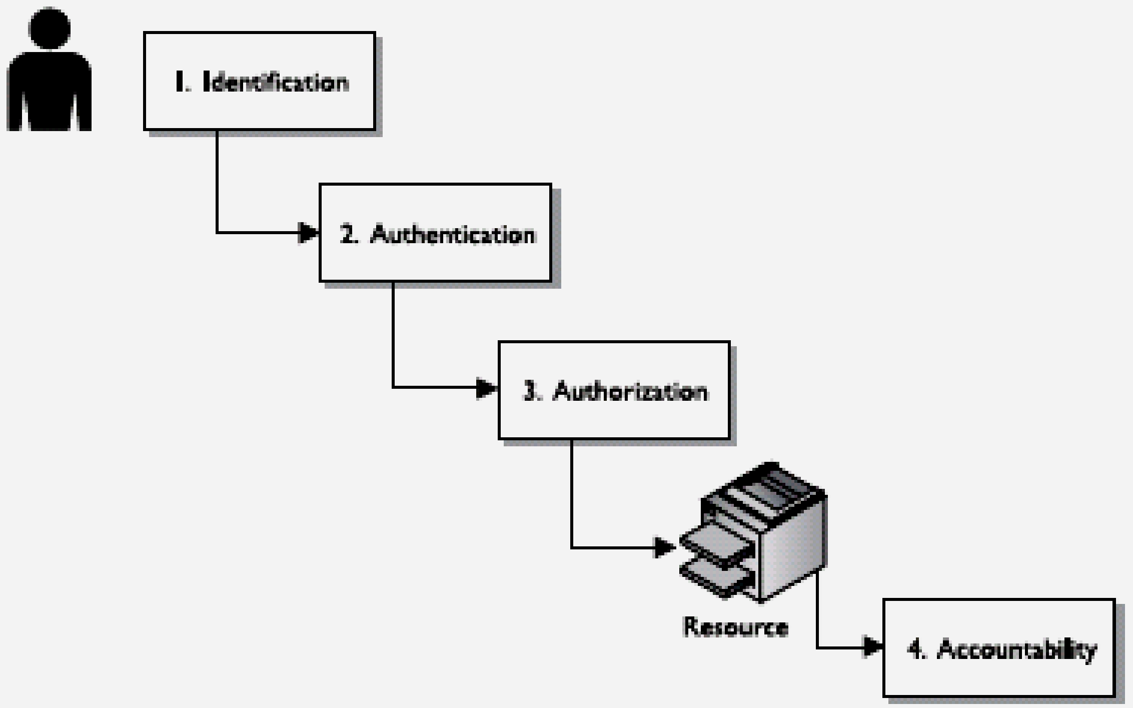


Figure 4-2 Four steps must happen for a subject to access an object: identification, authentication, authorization, and accountability.

B1. Identity Management Implementation

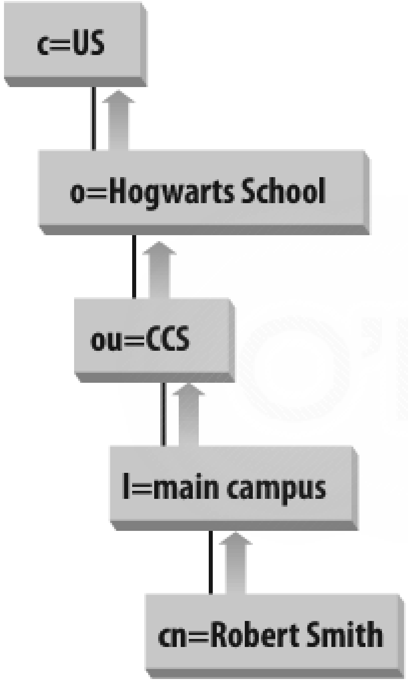
- **Identification key aspects:**
  - **Uniqueness**: unique ID for accountability. Eq fingerprint
  - **Nondescriptive**: do not indicate the purpose of account. Eg Backup_operator
  - **Issuance**: by another authority eg. ID card
  - Can be public
  - **Methods:** Username, Employee number, Account number, Radio Frequency Identification (RFID), E-Mail Address, IP, MAC address
  - **RFID**: Convenience, but eavesdropping, Traffic Analysis, Spoofing, DoS (use signal), Reader integrity (install fake reader), Privacy

B1. Identity Management Implementation

- **Implementation includes:**
  - **Password Management**: example, self-password reset, self password generation, password policy etc.
  - **Account Management:** Creation, modifying and decommissioning of account, limitation in centralizing over multiple applications, OS, DB, mainframes
  - **Profile Management**: Profile=collection of information of identify. Example, name, phone #, home address, email, date of birth etc.
  - **Directory Management**
  - **Single Sign-On**

Directory Management:
Lightweight Directory Access Protocol (LDAP)

- **LDAP** is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed **Directory Services** over an Internet Protocol (IP) network.
- **Directory Services** play an important role intranet and Internet applications and SSO
- **Examples**, directory services may provide any organized set of records, often with a hierarchical structure, such as a person name, location, operation unit, organization, country etc.



Legacy Single Sign-On

- Legacy means non-web based SSO
- SSO vs Password Synchronization
  - Operational: Pwd Syn still require multi-login with single pwd value
  - Similar vulnerability: attacker uncovers one, means uncover all
- SSO ideally requires redundancy or failover in place
- For legacy systems, either login differently or using batch script
- 2 Benefits:
  - Convenient to user and administrator for large number of applications, systems, DB etc.
  - can have stronger password and to prevent user to write down
- drawback: one password is hacked, means hacked all. The risk will be higher, if systems are managed by different providers or different trust levels.

Kerberos

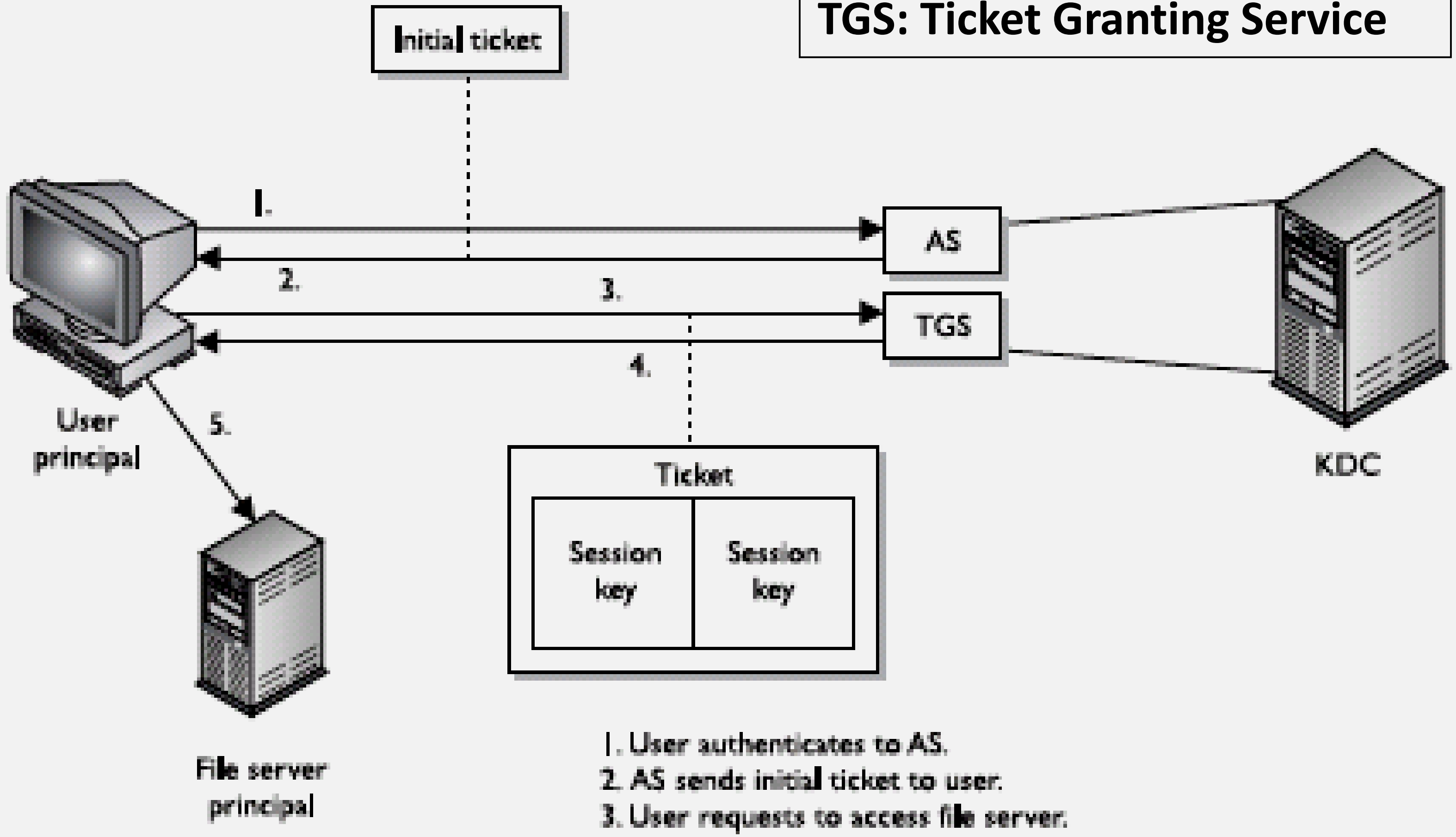
- **Kerberos**
  - three-headed dog in Greek
  - invented by MIT
  - example of single sign-on
- **Main Components in Kerberos**
  - Key Distribution Center (KDC): hold all secret keys,
  - Principle: KDC provides security service to principle eg. User, application…
  - Ticket is generated by ticket granting service (TGS) and contain session key
  - Authentication Service (AS) is inside KDC
- **Weaknesses of Kerberos**
  - single point of failure of KDC
  - temp store secret key in workstation
  - vulnerable to password guessing

Kerberos

AS: Authentication Service

KDC: Key Distribution Center

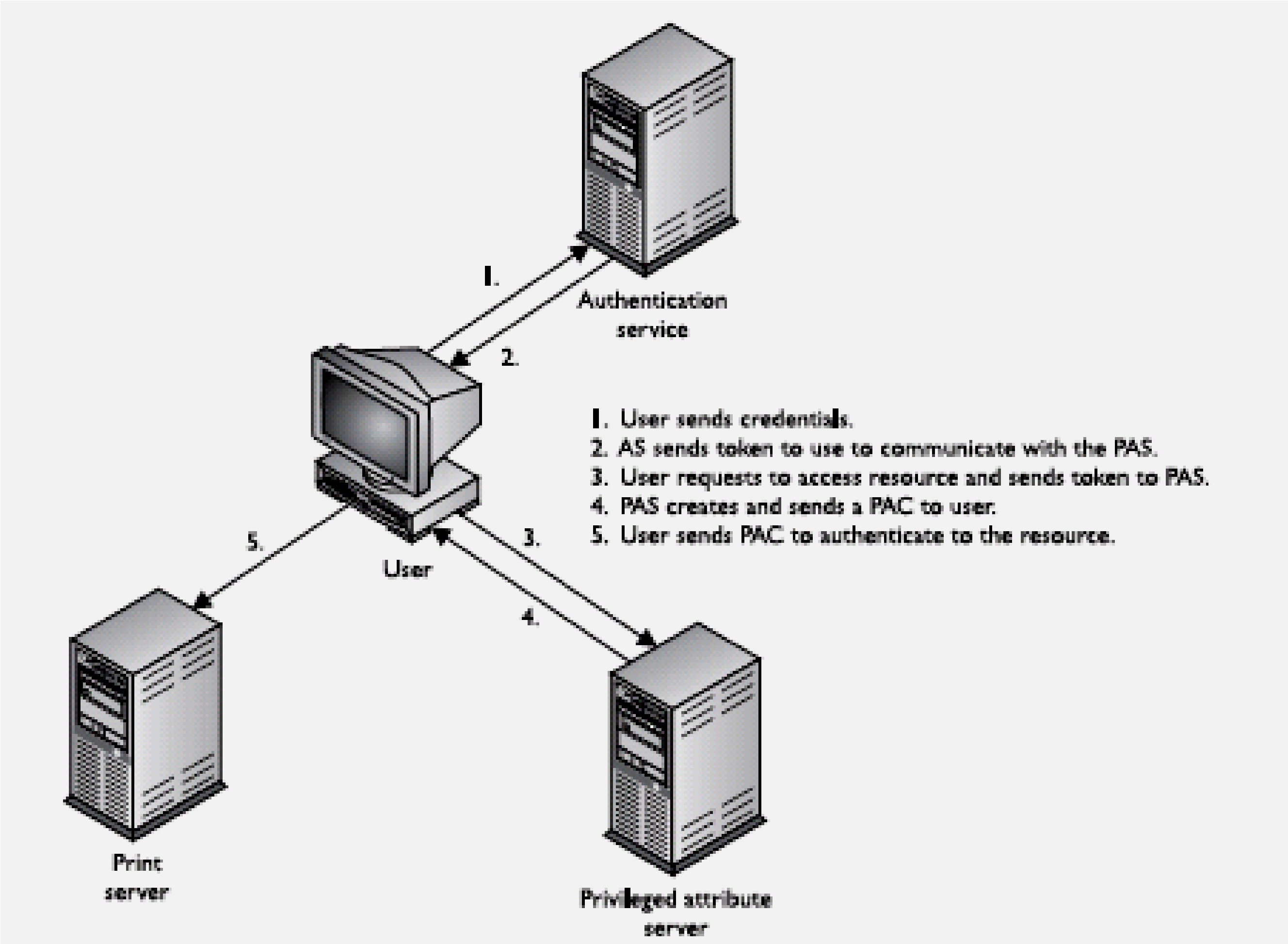
TGS: Ticket Granting Service



1. User authenticates to AS.
2. AS sends initial ticket to user.
3. User requests to access file server.
4. TGS creates new ticket with session keys.
5. User extracts one session key and sends ticket to file server.

Figure 4-10 The user must receive a ticket from the KDC before being able to use the requested resource.

SESAME



1. User sends credentials.
2. AS sends token to use to communicate with the PAS.
3. User requests to access resource and sends token to PAS.
4. PAS creates and sends a PAC to user.
5. User sends PAC to authenticate to the resource.

Figure 4-11 SESAME is very similar to Kerberos.

- **SESAME**
  - Secure European System for Application in a Multi-vendor Environment
  - SSO and extend Kerberos functionality and improve weakness
  - PAS: Privileged Attribute Server; PAC: Privileged Attribute Certificates

Federated Identity Management

- a **trend** to federate identities among organizations, eg. Automobile manufacturer and Parts suppliers
- **Technologies**: interface, standardization, cross-certification trust model, SAML
- **Administration**: Policy, Standard and Procedure among organizations

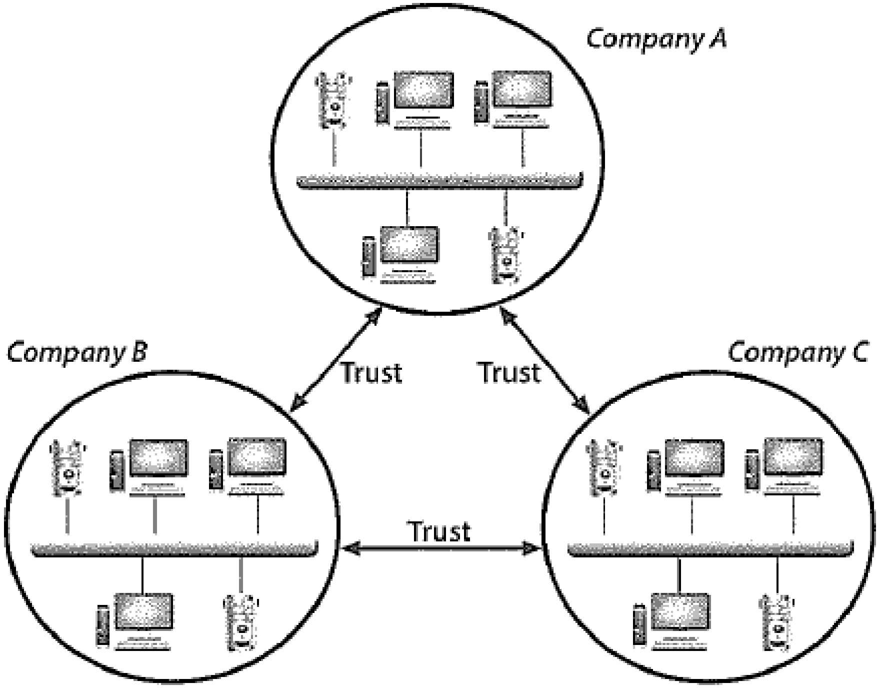


Figure 5.3 - **The Cross-Certification Trust model**

Security Assertion Markup Language (SAML)

- Standard for exchanging authentication and authorization data between security domains
- **XML (Extensible Markup Language) and XML Schema:** Compatibility, data inclusion
- **XML Signature**: Digital signatures for authentication and message integrity
- **XML Encryption**: Particularly authentication and authorization information
- **Hypertext transfer protocol (HTTP**): as communication protocol
- **SOAP (Simple Object Access Protocol)** allows programs that run on OS (such as Windows and Linux) to communicate using Hypertext Transfer Protocol (HTTP) and its Extensible Markup Language (XML).

B2. Single/Multi-Factor Authentication

- **Authentication factors:**
  - **Factor 1**: something you know (authentication by knowledge)
  - **Factor 2**: something you have (authentication by ownership)
  - **Factor 3**: something you are (authentication by characteristic)
- **Must be private and keep secret**
- **Methods:** password, token, digital signature, biometric …
- From Factor 1 to 3: more tighten in security level and more expense
- **Strong Authentication (two-factor authentication)** contains two out of three factors

Static Password

- **Passwords:** most common authentication way, usually static and reusable password
- **Password Management**
  - Scope covered: pwd generated, updated and kept secret
  - If too complicated, defeat the purpose
  - Attacking Technique to get pwd: Electronic Monitoring (network traffic), Access the pwd file, Brute force attacks, Dictionary Attack (use Rainbow table), Social engineering
  - Last successful /unsuccessful login date/time

Static Password

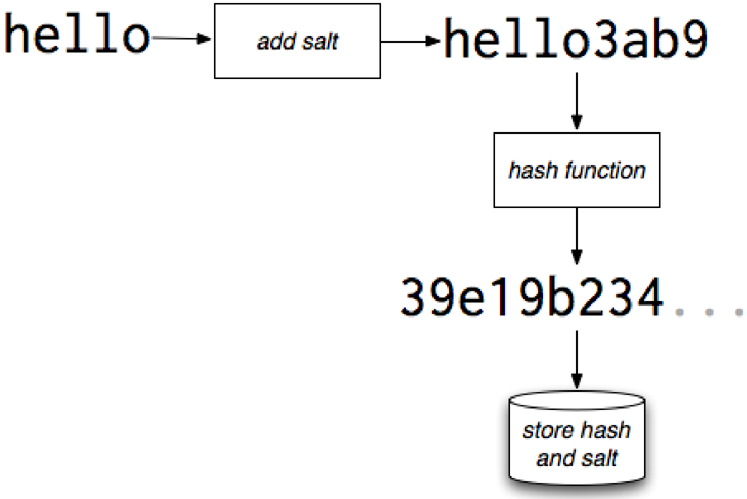
- **Password Hashing and Encryption**
  - Most systems hash or encrypt the user password and store in system file
  - Hashing enjoys the characteristic of “**Onewayness**”
  - Prevent attacker sniffs the password from the network

Static Password

- **Password Checkers (or Cracker)**
  - a tool to detect the weak password by the organization, not using regular login interface
  - **Dictionary**: reverse hashing based on Dictionary (rainbow table)
  - **Brute force**: reverse hashing with all combinations
  - The tool can tell Auditor how many easily guessable password in your organization.
  - Have to get management approve first.
  - Usually the same tool used hacker, but called password cracker.

Salting

- A salt is random data (or a constant) that is used as an additional input to a one-way function that hashes a password or passphrase.
- The primary function of salts is to defend against **dictionary attacks** versus a list of password hashes and against pre-computed rainbow table attacks.

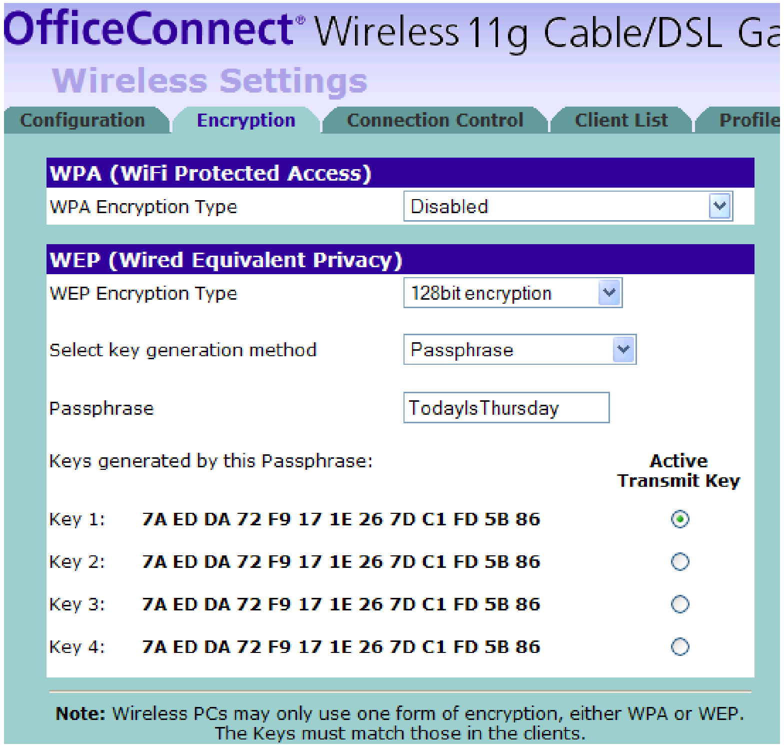


Static Password

- **Password Aging**
  - Forcing users to change pwd at regular intervals
  - Minimum and Maximum age. Why minimum?
- **Password History**
  - not allow user revert back to previously or recently used passwords
- **Limit Logon Attempts**
  - allow only a certain number of unsuccessful logon attempts
  - will lock a period of time or indefinitely
- **Cognitive Password**
  - Fact- or opinion-based information to verify identification
  - Capture at enrolment and use in “forget password”
  - For example, first school, mother maiden name….
- **Graphical Password**
  - Detect mouse movement or select pictures
  - Prevent keystroke logger attack

Static Password

- **Passphrase**
  - is longer than pwd, eg StickWithMeKidAndYouWillWearDiamonds
  - Example: wireless router passphrase
  - it will convert to virtual password
  - Virtual password is more secure than password, not easy guessable



WPA (WiFi Protected Access)

WPA Encryption Type: Disabled

WEP (Wired Equivalent Privacy)

WEP Encryption Type: 128bit encryption

Select key generation method: Passphrase

Passphrase: TodayIsThursday

Keys generated by this Passphrase:		Active Transmit Key
Key 1:	7A ED DA 72 F9 17 1E 26 7D C1 FD 5B 86	●
Key 2:	7A ED DA 72 F9 17 1E 26 7D C1 FD 5B 86	○
Key 3:	7A ED DA 72 F9 17 1E 26 7D C1 FD 5B 86	○
Key 4:	7A ED DA 72 F9 17 1E 26 7D C1 FD 5B 86	○

Note: Wireless PCs may only use one form of encryption, either WPA or WEP. The Keys must match those in the clients.

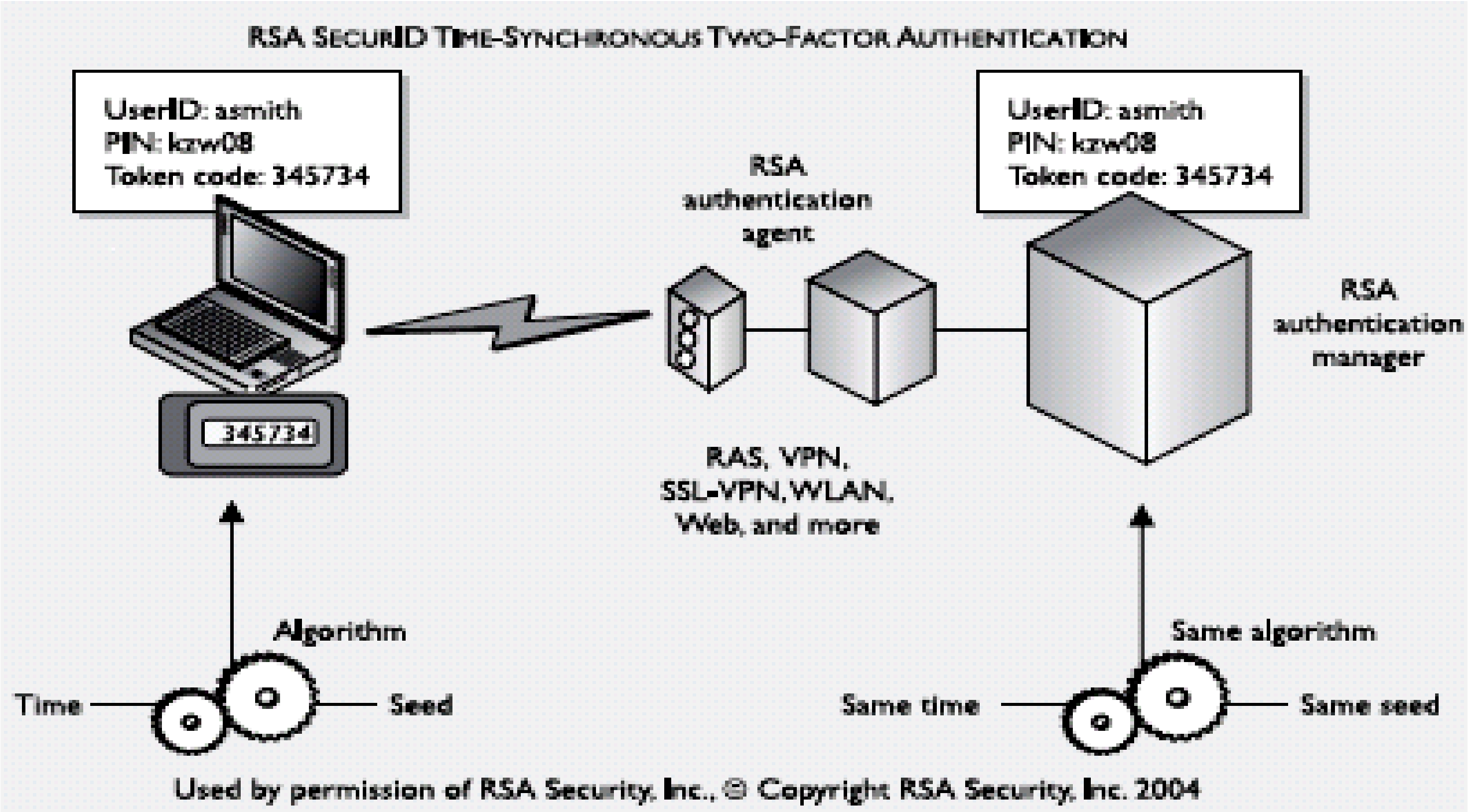
Dynamic Password

- **One-time password (or dynamic password)**
  - is only good for once
  - more secure than static password
  - Normally work with device

Token

(1) Hard Token

- time-based: use time + seed
- counter-based: next counter + seed



Used by permission of RSA Security, Inc., © Copyright RSA Security, Inc. 2004

Token

- **(2) Soft Token**
  - **Software-based** security token that generates a single-use login PIN.
  - **Advantage**: low cost, easy-to-remember location, single device
  - **Disadvantage**: inherently less secure, greatly depends on security of OS and client software.
- **Token concerns**
  - **Private keys** must be non-exportable
  - **Never** store keys in plaintext
  - **Distributing** the seed record and initial passphrases requires **confidential** channel
  - User authentication is required every time activation of soft token
  - Token time limit less than 2 minutes
  - **Hard token**: physical security
  - Use available **Trusted Platform Modules** (TPM)
  - **Audit**

Cards

Customer Service : ☎ 91-44-2851 9484, 2851 9470
2
1
AUTHORISED SIGNATURE - NOT VALID UNLESS SIGNED
Not valid for payments in Foreign Exchange in Nepal and Bhutan.
NOT TRANSFERABLE
This card can be used for ABB services at IOB branches. Use of this card is governed by the conditions of use. This card should be signed immediately by the authorised user and will remain a property of Indian Overseas Bank. If found, please return to any branch of IOB or
INDIAN OVERSEAS BANK
ATM / DEBIT CARD DIVISION
Central Office : 763, Anna Salai, Chennai - 600 002. INDIA
visit us at : www.iob.com
E-mail : atmcard@iobnet.co.in

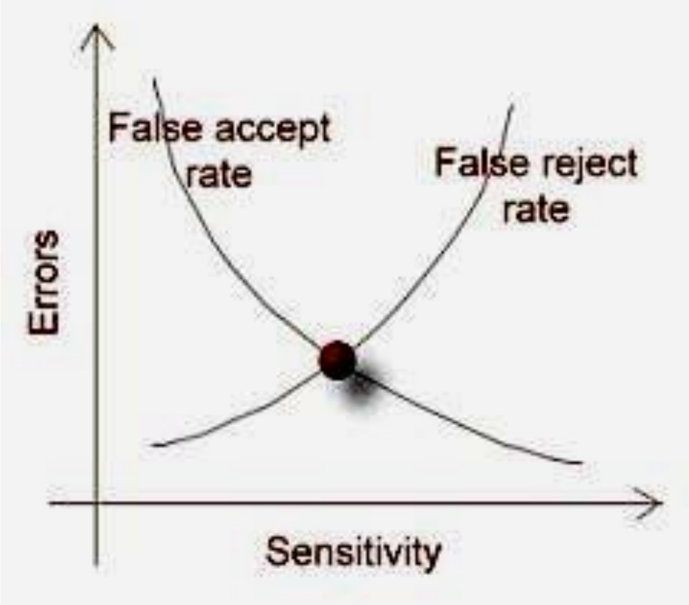
- **Memory Cards**
  - memory card cannot process information
  - holds user’s authentication information
  - User need to enter PIN, that is two-factor authentication
  - Eg. ATM card
- **Smart Card**
  - can process with microprocessor
  - two type contact and contactless
  - the information on card is not readable until the authentication done

Biometrics

- verify an individual’s identity by analyzing unique personal attribute (fingerprint) or behavior (signature)
- sophisticated and accurate technology, but expense and complex
- Two categories:
  - **Physiological**: physical attributes unique, eg. Fingerprint, “what you are”
  - **Behavioral**: characteristic eg. Signature, “what you do”

Biometrics

- Two type of error:
  - **Type I error**: false rejection rate
  - **Type II error**: false acceptance rate (more dangerous)



- **Crossover error rate (CER):** tune the sensitivity of device to a point that false rejection rate is equal to false acceptance rate. CER of 3 is more accurate than CER of 4.
- CER is indication of accuracy and for buying selection. But the final configuration of device are organization specific (say Military)

Biometrics

- Other factors:
  - **Enrollment timeframe**: may require several times to capture clear image
  - **Throughput**: may require several times to read
  - **Weakness**: living things can change, say voice, pregnancy can change patterns of retina, lost finger….

Biometrics

- Involves hash or encryption or both to store and to compare

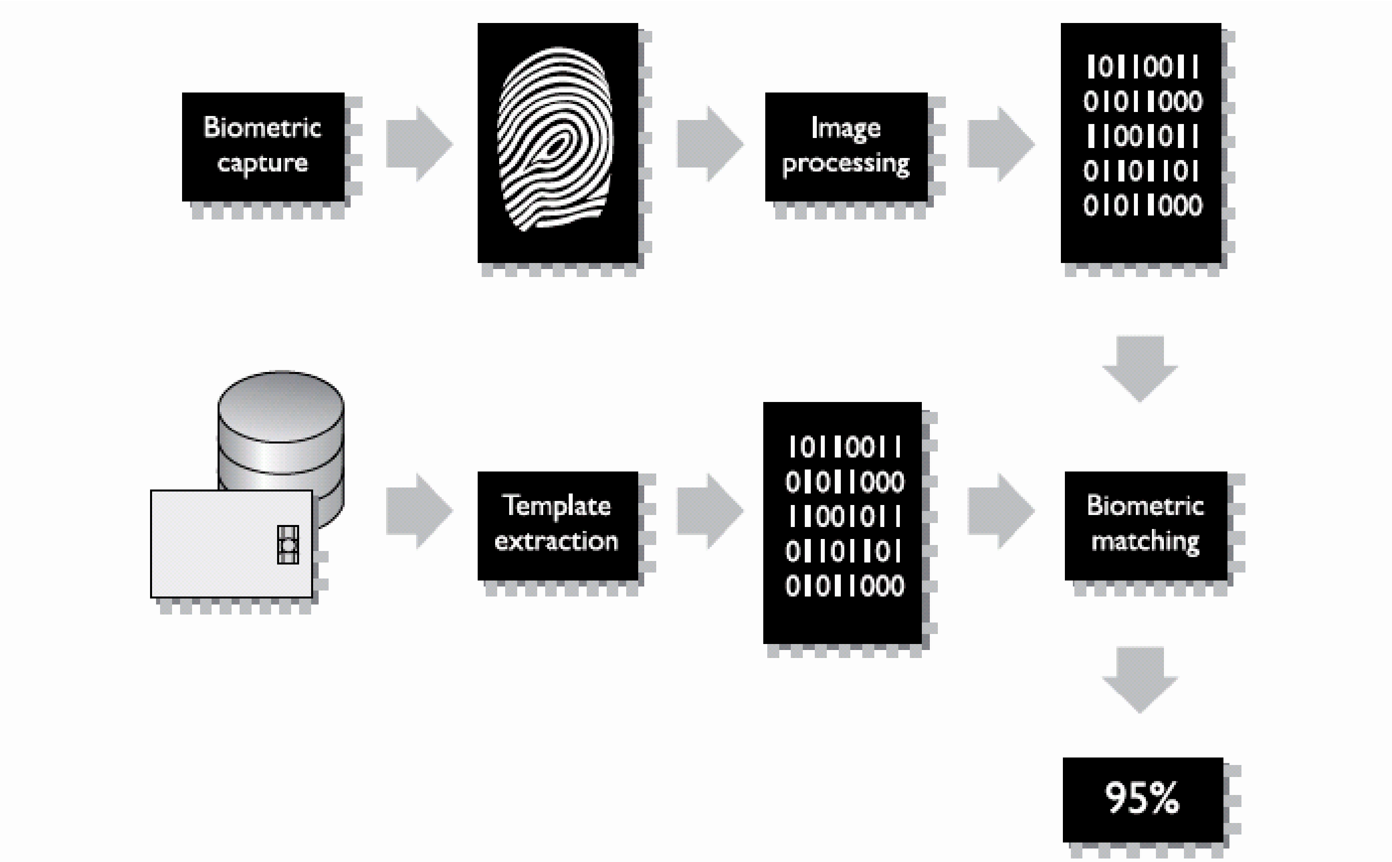


Figure 4-7 Biometric data is turned into binary data and compared for identity validation.

Biometrics

- **Physiological:**
  - **Fingerprint**
  - **Palm Scan**: including fingerprints of each finger
  - **Hand Geometry**: groove, shape of hand, the length and width of hand and finger
  - **Retina Scan**: scan the blood-vessel pattern of retina, extremely unique
  - **Iris Scan**: unique patterns, rifts 裂口, color, rings, corona 冠狀物 and furrow 皺紋
  - **Facial Scan**:
  - **Hand Topography**: different peaks and valleys of hand
- **Behavioral:**
  - **Signature dynamics**: pattern, speed, pressure and the way hold pen
  - **Keyboard Dynamics**: type a specific phrase, capture style and speed, more effective for password typing.
  - **Voice Print**: enroll several different word, jumble words, repeats the seq of works given. This technology can avoid recording and playback.

Questions

What is derived from a passphrase?

A. Personal password

B. Virtual password

C. User ID

D. Valid password

What role does biometrics play in access control?

A. Authorization

B. Authenticity

C. Authentication

D. Accountability

E. Implement and manage authorization mechanisms

- **Authorization**
  - Determine what is authorized after authentication.
- **Access Criteria**
  - Define the level of detail (read, write, delete….)
- **Default to No Access**
  - Start from zero access
  - If access is not explicitly allowed, it should be implicitly denied
- **Authorization creep**
  - person works long in a company and often assign more and more access right.
  - Solution: User recertification periodically
- **Need-to-know**
  - **Least Privilege**: *absolutely* require in order to perform job duties
  - **Need-to-know**: business need to have access to resources
  - Management will decide, and should be descried in policy

Access Control Models

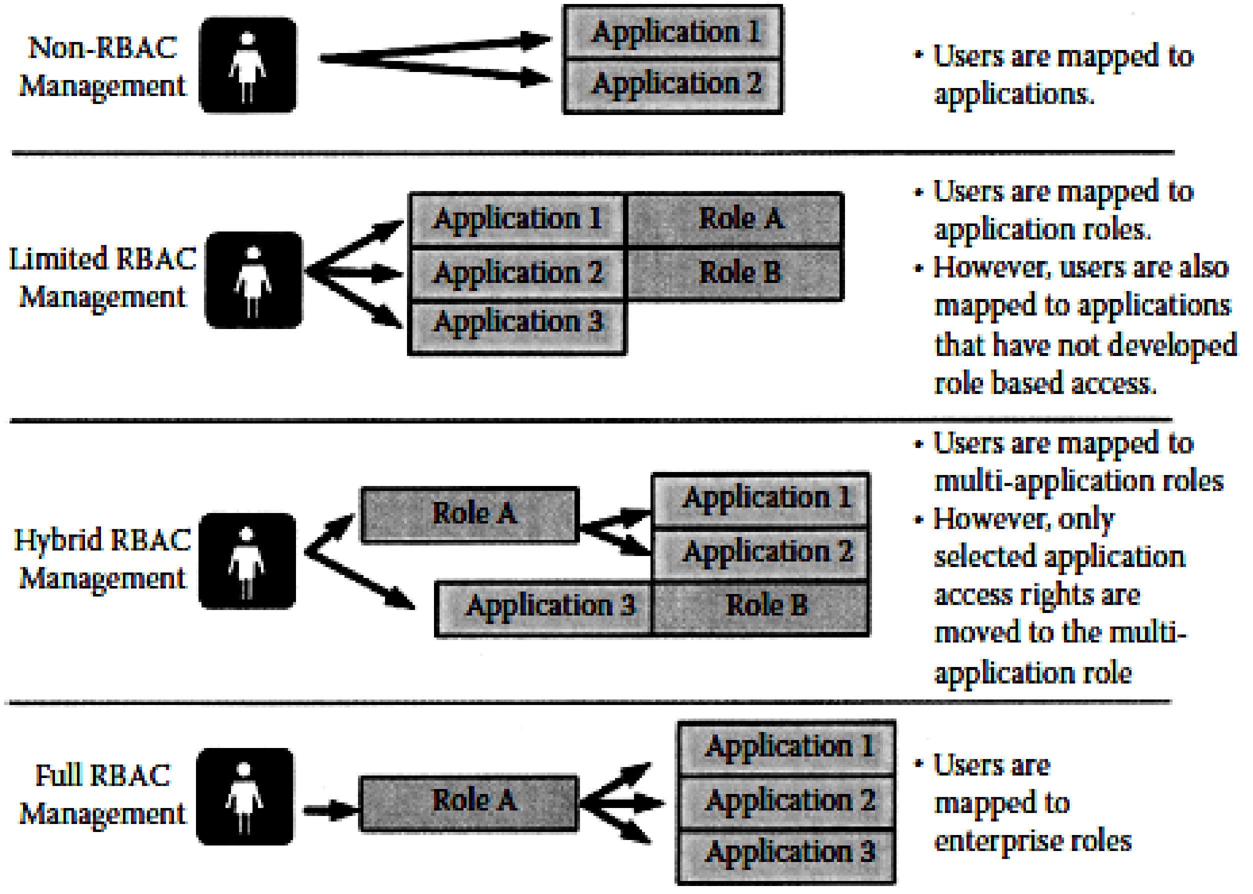
- **Discretionary Access Control (DAC)**
  - owner can define the own ACL and assign owned object to any subject
  - windows, linux, macintosh, unix
- **Mandatory Access control (MAC)**
  - The operating system makes the final decision, not users and data owners.
  - Both object and subject are classified security level (such as secret, top secret, confidential, public…)
  - Used in military institution, in special type s of Unix, SE Linux, Trusted Solaris

Access Control Models

- **Role-Based Access control (RBAC) (nondiscretionary access control)**
  - centralized administrated set of controls
  - based on the role of user holds (eg. Research and development analyst)
  - system will check the role’s access levels before allowing the access of object
  - Ideal for high employee turnover environment

Access Control Models

- **Different RBAC approach**



- Users are mapped to applications.

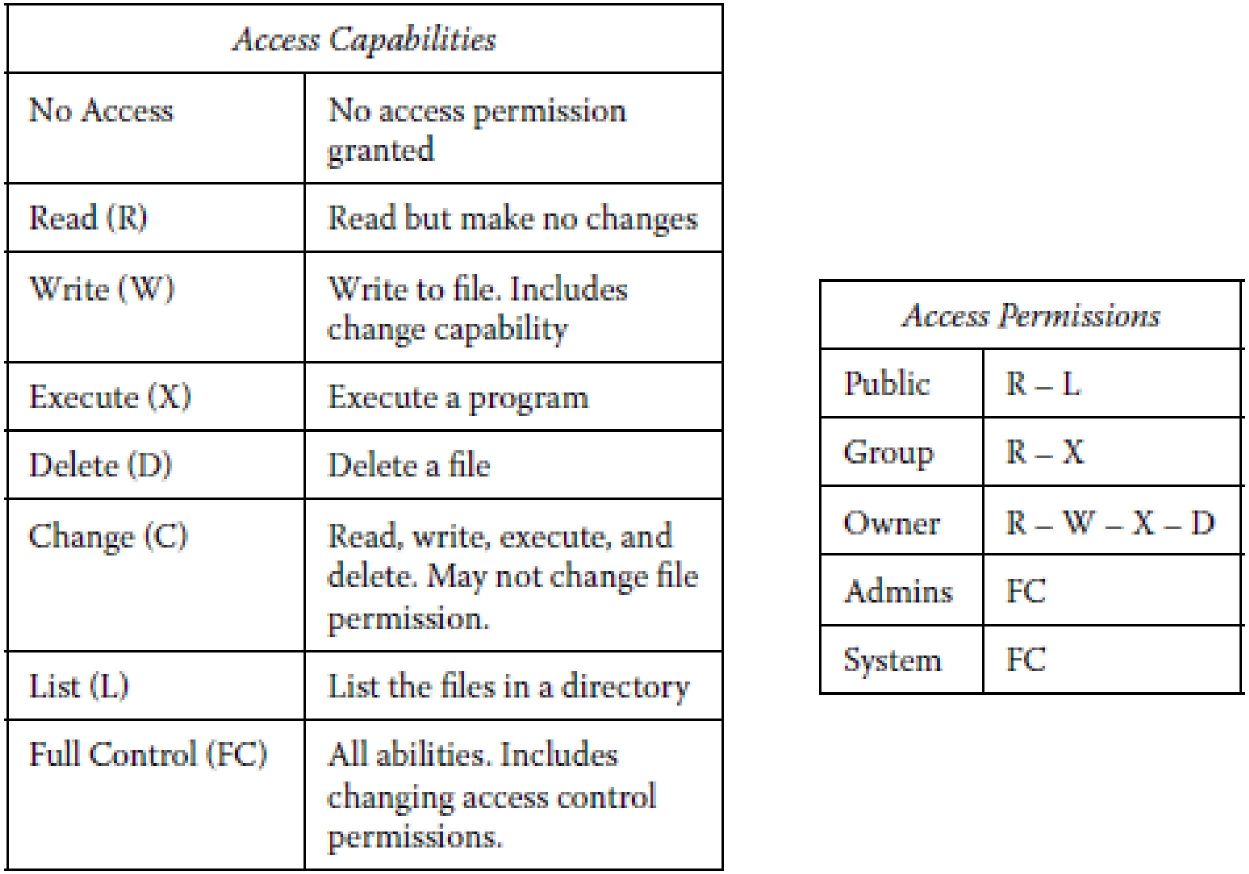
- Users are mapped to application roles.
- However, users are also mapped to applications that have not developed role based access.

- Users are mapped to multi-application roles
- However, only selected application access rights are moved to the multi-application role

- Users are mapped to enterprise roles

Figure 1.26 Role-based access control architecture.

Access Permission Example



Access Capabilities	
No Access	No access permission granted
Read (R)	Read but make no changes
Write (W)	Write to file. Includes change capability
Execute (X)	Execute a program
Delete (D)	Delete a file
Change (C)	Read, write, execute, and delete. May not change file permission.
List (L)	List the files in a directory
Full Control (FC)	All abilities. Includes changing access control permissions.

Access Permissions	
Public	R – L
Group	R – X
Owner	R – W – X – D
Admins	FC
System	FC

Figure 1.23 An example of access permissions. Access permissions are applied to an object based on the level of clearance given to a subject.

Questions

Which of the following is not an advantage of a centralized access control administration?

A. Flexibility

B. Standardization

C. A higher level of security

D. No need for different interpretations of a necessary security level

What determines if an organization is going to operate under a discretionary, mandatory, or nondiscretionary access control model?

A. Administrator

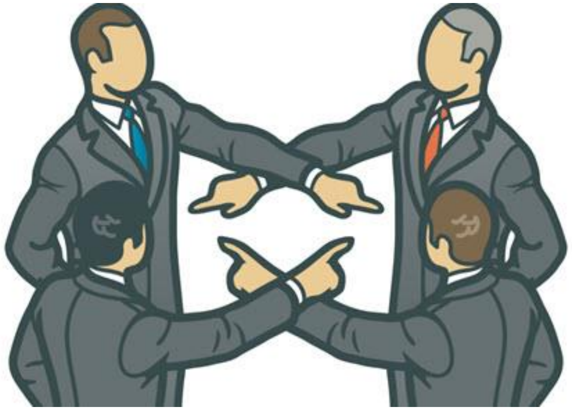
B. Security policy

C. Culture

D. Security levels

B3. Accountability

- **Including**
  - **Strong identification:** able to identify individual
  - **Strong authentication:** able to verify
  - **User training and awareness**
  - **Comprehensive, timely and thorough monitoring**
  - **Accurate and consistent audit logs**
  - **Independent audits**
  - **Polices enforcing accountability**
  - **Organizational behavior supporting accountability:** culture, expectation.



B3. Accountability

- **Accountability**
  - users are accountable for their actions
  - Consideration: store audit **securely**, keep right size, log high-privileged account as well.
- **Review of Audit Information**
  - can be manual or automatic
  - event-oriented or periodical
  - audit-reduced tool: reduce the amount of information within audit log
- **Keystroke Monitoring**
  - can record and review keystrokes entered by user
  - normally not all the time, only when suspicious
  - concern about privacy issue, state so in security policy, security awareness training and banner notice.

Most concern & dangerous

- **Protecting Audit Data and Log information**
  - Most concern and **Dangerous** if intruder is able to delete or modify the audit log
  - Scrubbing: deleting incriminating data within audit log

B4 Session Management

- **Desktop Sessions:** can be controlled and protected by:
  - **Screensavers**
  - **Timeouts**
  - **Automatic Logouts**
  - **Session/login limitation:** Single or multiple session → security or convenience
  - **Schedule limitation:** non-business hours?

B4 Session Management

- **Logical session** in web browsers becomes more critical for information security professionals
  - **HTTP sessions**, which allow associating information with individual visitors
    - **Assigning unique session ID** to every connection
    - **Sequential session ID**: easily guessable
    - **Random Session ID**: prevent guessing
    - **Time-stamp or time-based** validation: prevent replay attack

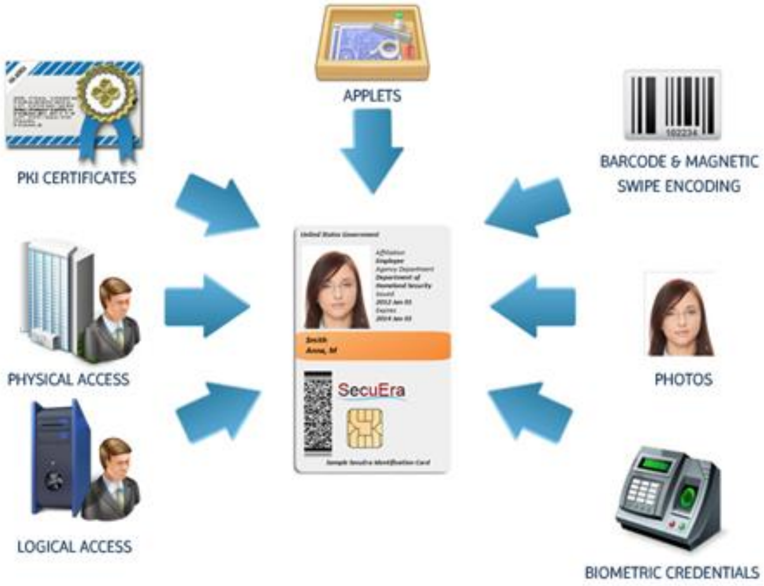
B5. Registration & proofing of identity

- In company, proofing may come from department head or HR.
- In Web, proofing may come from email address or phone number
- Roles
  - **Applicant**
  - **PIV Sponsor**: validate requirement and sponsor
  - **PIV Registrar**: perform background check
  - **PIV Issuer:** issue identity credential
  - **PIV Digital Signatory**: signing applicant
  - **PIV Authentication Certification Authority (CA)**

***PIV = Personal Identity Verification**

B7. Credential management systems

- Challenges: More technology, system, profile, hacking, complexity,
- Require: **unified**, robust and enterprise-wide solution → Credential Management System
- Example: Avaya Professional Credentials.



C. Integrate identity as a service (e.g. cloud identity)
D. Integrate 3-rd party identity services (on premise)

- **Identity-as-a-Service (IDaaS)** is cloud-based services for identity and access management function to target systems on **company's premises and in the cloud.**
- Including:
  - **Single Sign-on (SSO) Authentication**: to internal & external services
  - **Federation**: Federated identity to multiple systems or companies
  - **Authorization Controls**: not "all-or-nothing"
  - **Administration**: Add/change/delete profiles
  - **Integration** of Directory services
  - **Audit Log**
- **Security concerns:**
  - 3rd party management
  - Internet
  - SSO: know one pwd will know all.

F. Prevent or mitigate access control attacks

- **Toxic Combination:** Societe Generale took a $7.2 billion hit in fraudulent trades in 2008, this is example internal damage more than external.
- Control:
  - **Transparency**: who has what
  - **Preventive**: procedure for profile creation/**transfer**/deletion
  - **Detective**: Re-Certification periodically

F. Prevent or mitigate access control attacks

- **General controls:**
  - Control **Physical** Access to systems/computers
  - Control **Electronic** Access to password files
  - **Hash / Encrypt password files**
  - Create strong password policy
  - User password masking
  - Deploy **multifactor** authentication
  - **Use Account Lockout controls**, but beware massive account lockout attack
  - Use **Last Logon** Notification
  - **Educate** user about Security
  - **Audit** Access Controls
  - Actively manage Accounts: **Disable** ASAP when leaving
  - **Use Vulnerability Scanners**: password cracking tools to detect weak password

G. Manage the identity and access provisioning lifecycle

- Lifecycle
  - **Provisioning**: new or change profile
  - **Review**: Monitoring
  - **Revocation**: Termination of profile