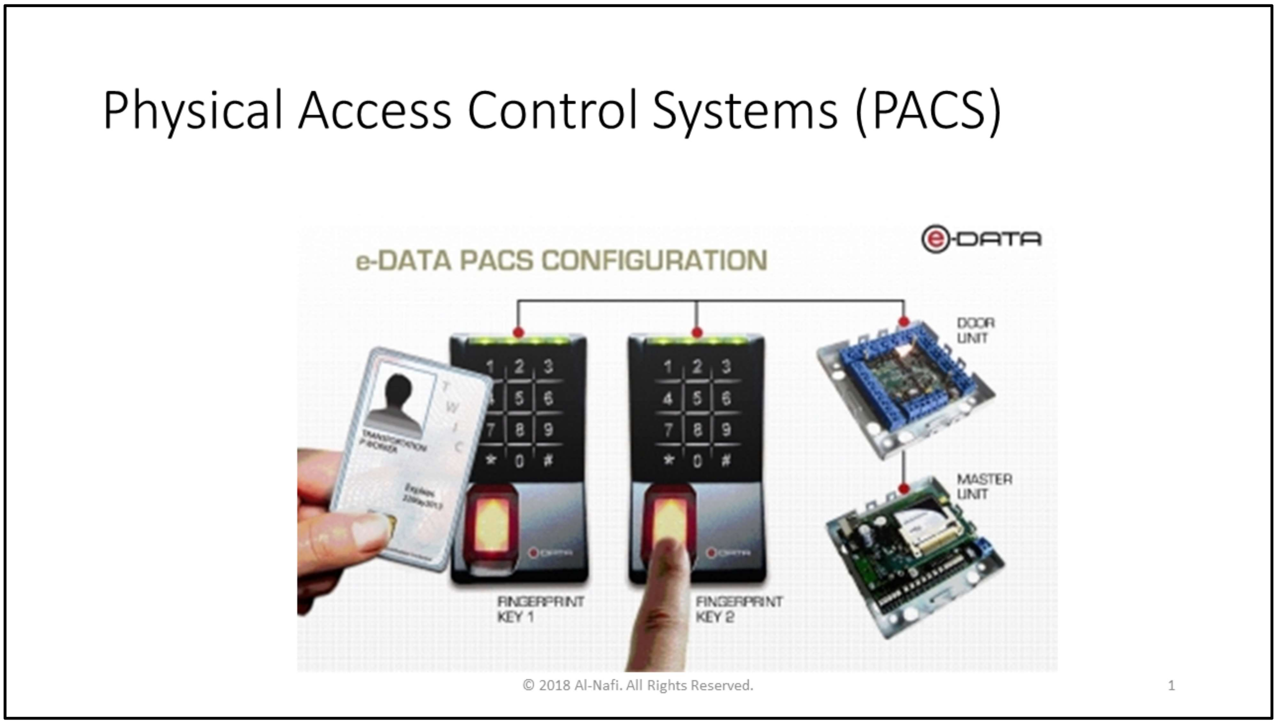


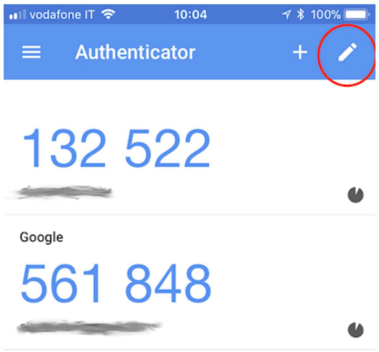
Physical Access Control Systems (PACS)

Special Publications 800-53r4 defines physical access control as “An automated system that manages the passage of people or assets through an opening(s) in a secure perimeter(s) based on a set of authorization rules.”

Devices

There are a range of devices (systems or components if logical) associated with logical and physical access control. Logical and physical access control devices include but are not limited to access tokens (hardware and software), keys, and cards.

Access control toke types



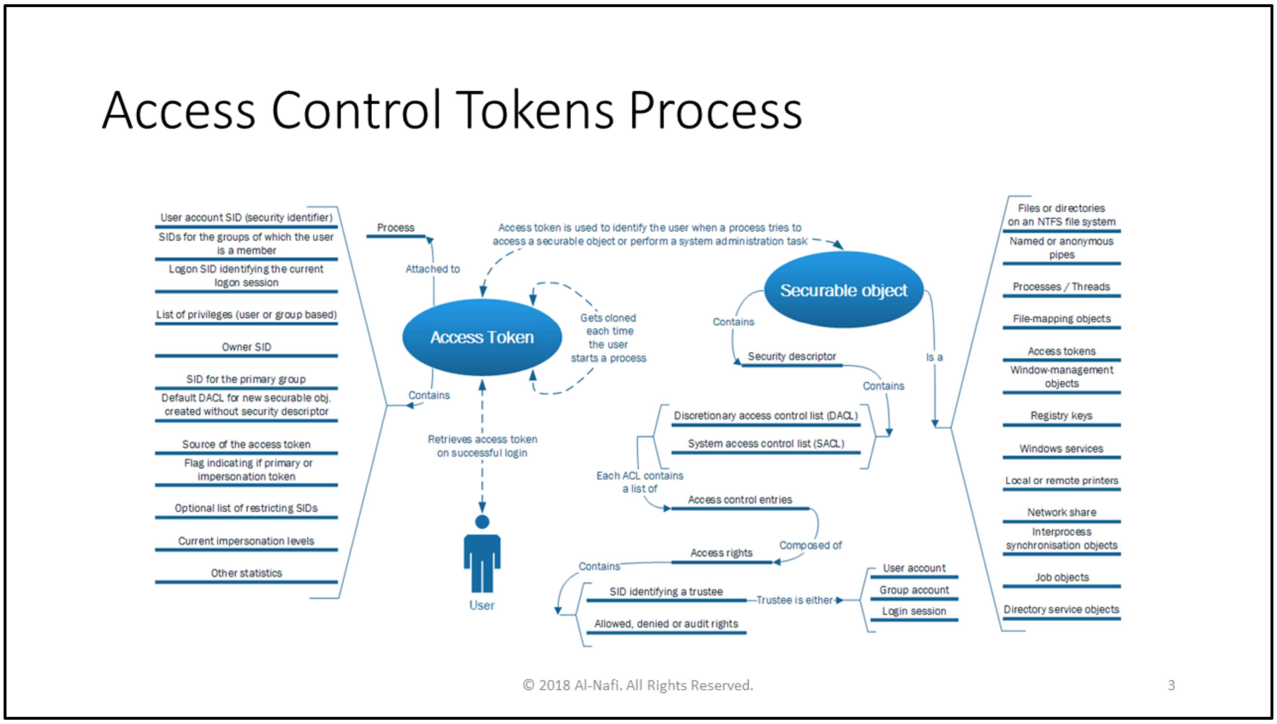
132 522

[redacted]

Google

561 848

[redacted]



Access Control Tokens Process

User account SID (security identifier)

SIDs for the groups of which the user is a member

Logon SID identifying the current logon session

List of privileges (user or group based)

Owner SID

SID for the primary group

Default DACL for new securable obj. created without security descriptor

Source of the access token

Flag indicating if primary or impersonation token

Optional list of restricting SIDs

Current impersonation levels

Other statistics

Process

Attached to

Access Token

Contains

Gets cloned each time the user starts a process

Retrieves access token on successful login

User

Access token is used to identify the user when a process tries to access a securable object or perform a system administration task

Securable object

Contains

Security descriptor

Contains

Is a

Discretionary access control list (DACL)

System access control list (SACL)

Each ACL contains a list of

Access control entries

Composed of

Access rights

Contains

SID identifying a trustee

Trustee is either

User account

Group account

Login session

Allowed, denied or audit rights

Files or directories on an NTFS file system

Named or anonymous pipes

Processes / Threads

File-mapping objects

Access tokens

Window-management objects

Registry keys

Windows services

Local or remote printers

Network share

Interprocess synchronisation objects

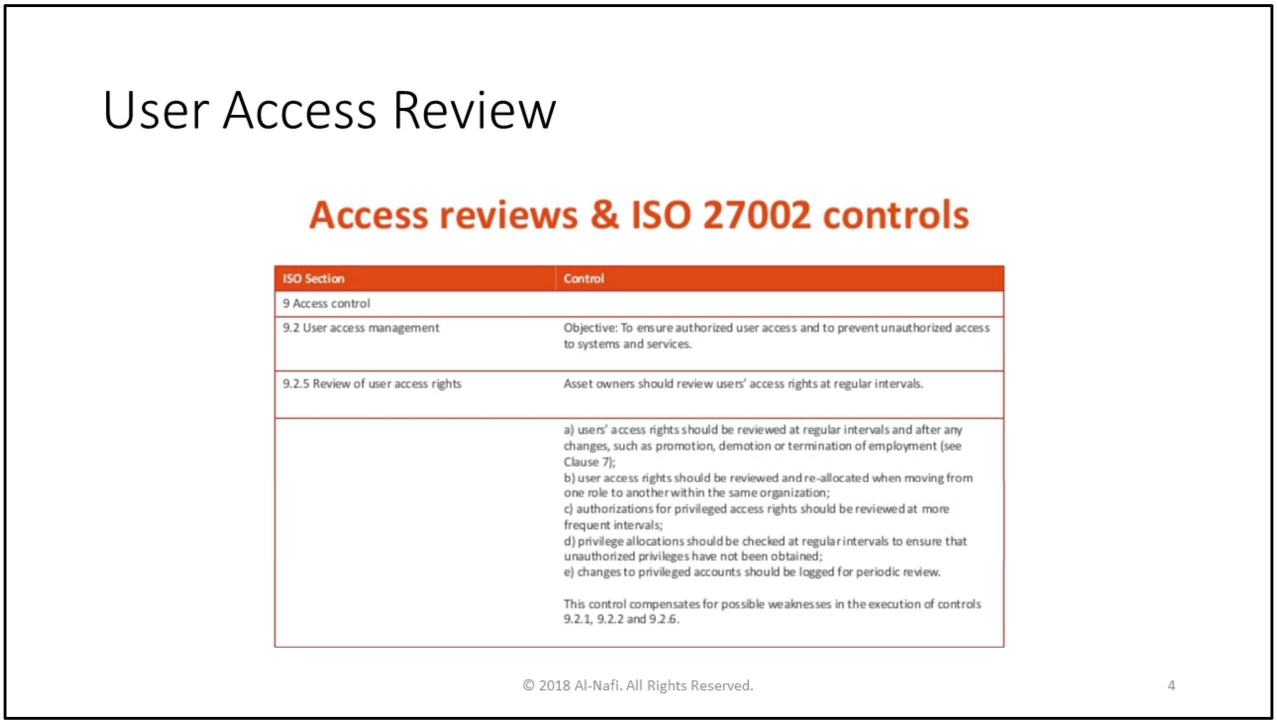
Job objects

Directory service objects

3

Access Control Tokens

Access control tokens are available in many different technologies and in many different shapes. The information that is stored on the token is presented to a reader that reads the information and sends it to the system for processing. The token may have to be swiped, inserted, or placed on or near a reader. When the reader sends information to the system, it verifies that the token belongs to the system and identifies the token itself. Then, the system decides if access is to be granted or denied based upon the validity of the token for the point where it is read based on time, date, day, holiday, or other condition used for controlling validation. When biometric readers are used, the token or key is the user’s retina, fingerprint, hand geometry, voice, or whatever biological attribute is enrolled into the system. Most biometric readers also require a PIN to index the stored data on the sample readings of the biological attribute. Biometric systems can also be used to determine whether a person is already in a database, such as for social service or national ID applications.



User Access Review

Access reviews & ISO 27002 controls

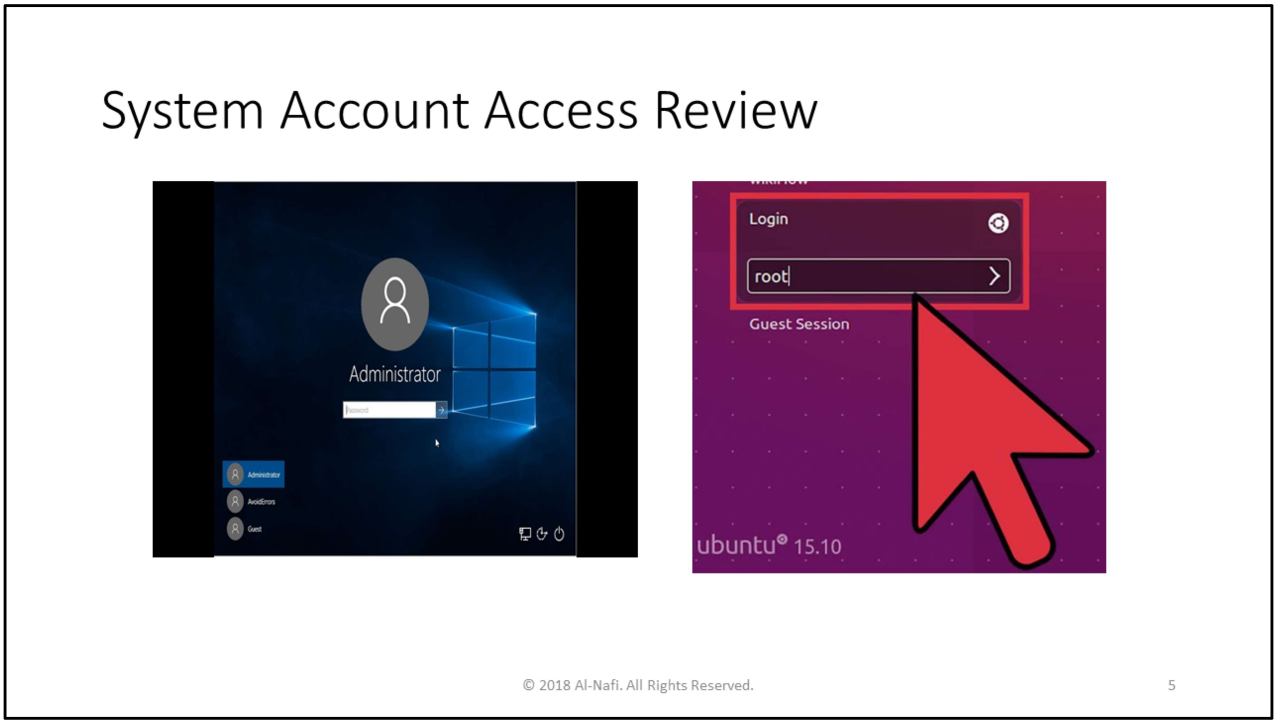
ISO Section	Control
9 Access control	
9.2 User access management	Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.
9.2.5 Review of user access rights	Asset owners should review users' access rights at regular intervals.
	a) users' access rights should be reviewed at regular intervals and after any changes, such as promotion, demotion or termination of employment (see Clause 7); b) user access rights should be reviewed and re-allocated when moving from one role to another within the same organization; c) authorizations for privileged access rights should be reviewed at more frequent intervals; d) privilege allocations should be checked at regular intervals to ensure that unauthorized privileges have not been obtained; e) changes to privileged accounts should be logged for periodic review. This control compensates for possible weaknesses in the execution of controls 9.2.1, 9.2.2 and 9.2.6.

At the development of the enterprise security architecture, the security architect will map business requirements to technology agnostic views or statements that enforce the security policy and answer business goals throughout the organization. These architectural views or statements are what provide guidance for implementation of cohesive technology solutions that come from specific design elements that are informed by the architecture. Within the lifecycle of identity and access provisioning, it is imperative that user access reviews are conducted on an on-going basis once an account has been created and provisioned. The review will be based upon the business requirements that are expressed within the enterprise security architecture. Scheduled and regular user access reviews could reveal vulnerabilities that might require the need for revocation, disablement, or deletion of an account.

These occurrences are causes for revocation/disablement/or deletion of user access:

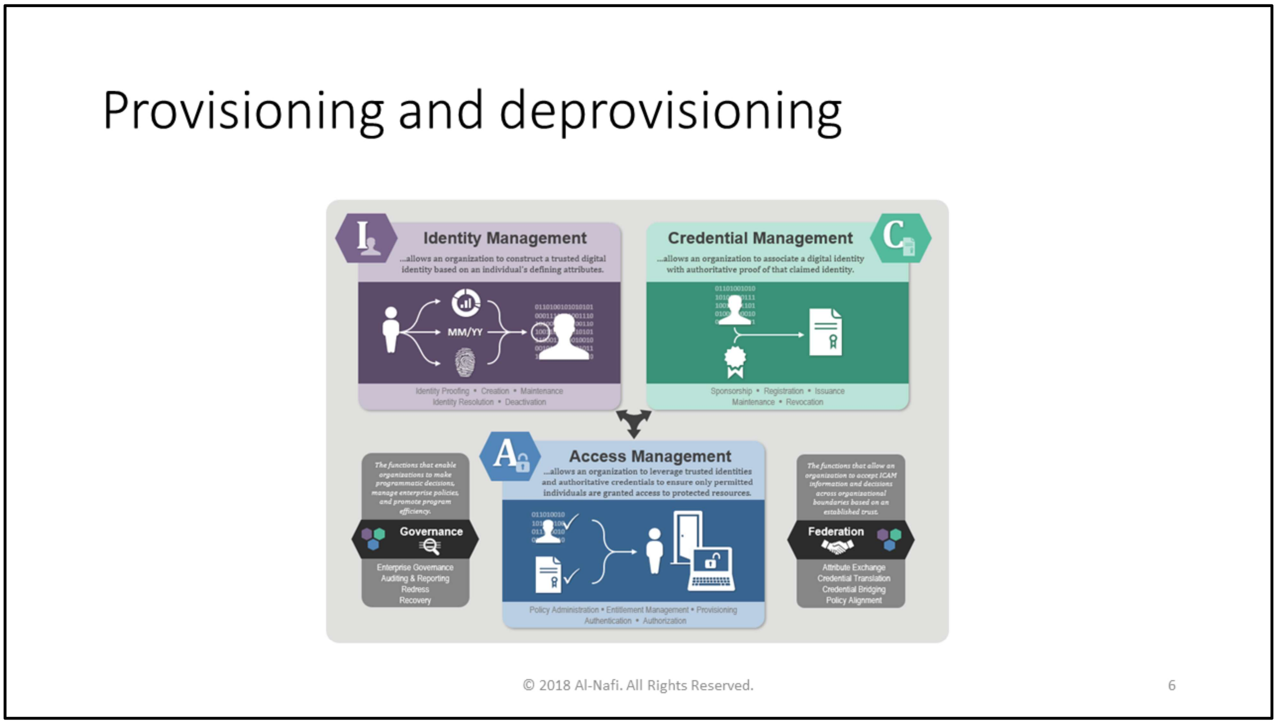
- If a user is voluntarily or involuntarily terminated from an organization.
- If an account has been inactive for a period that surpasses the organizational policy.

- If the user account is no longer appropriate for the job description or role.
- If user account privileges have experienced unnecessary access aggregation.



System Account Access Review

System accounts such as “administrator,” “sudo,” or “root” accounts present an often-exploited vulnerability for attackers. Making a non-linear representation between the user ID name and its function could represent the first layer of defense against attackers. Disconnecting the account name from the function is as simple as renaming the account to something that looks more like a traditional user name or randomly generated name. In addition to identifying an account by the name, an attacker could also identify the account by other attributes such as system assigned static numeric ID. Therefore, “security by obscurity” or only renaming the system account is insufficient due diligence to protect them from anything more than trivial exploitation efforts.



Provisioning and deprovisioning

I
Identity Management
...allows an organization to construct a trusted digital identity based on an individual's defining attributes.
MM/YY
Identity Proofing • Creation • Maintenance
Identity Resolution • Deactivation
C
Credential Management
...allows an organization to associate a digital identity with authoritative proof of that claimed identity.
Sponsorship • Registration • Issuance
Maintenance • Revocation
A
Access Management
...allows an organization to leverage trusted identities and authoritative credentials to ensure only permitted individuals are granted access to protected resources.
Policy Administration • Entitlement Management • Provisioning
Authentication • Authorization
The functions that enable organizations to make programmatic decisions, manage enterprise policies, and promote program efficiency.
Governance
Enterprise Governance
Auditing & Reporting
Redress
Recovery
The functions that allow an organization to accept ICAM information and decisions across organizational boundaries based on an established trust.
Federation
Attribute Exchange
Credential Translation
Credential Bridging
Policy Alignment

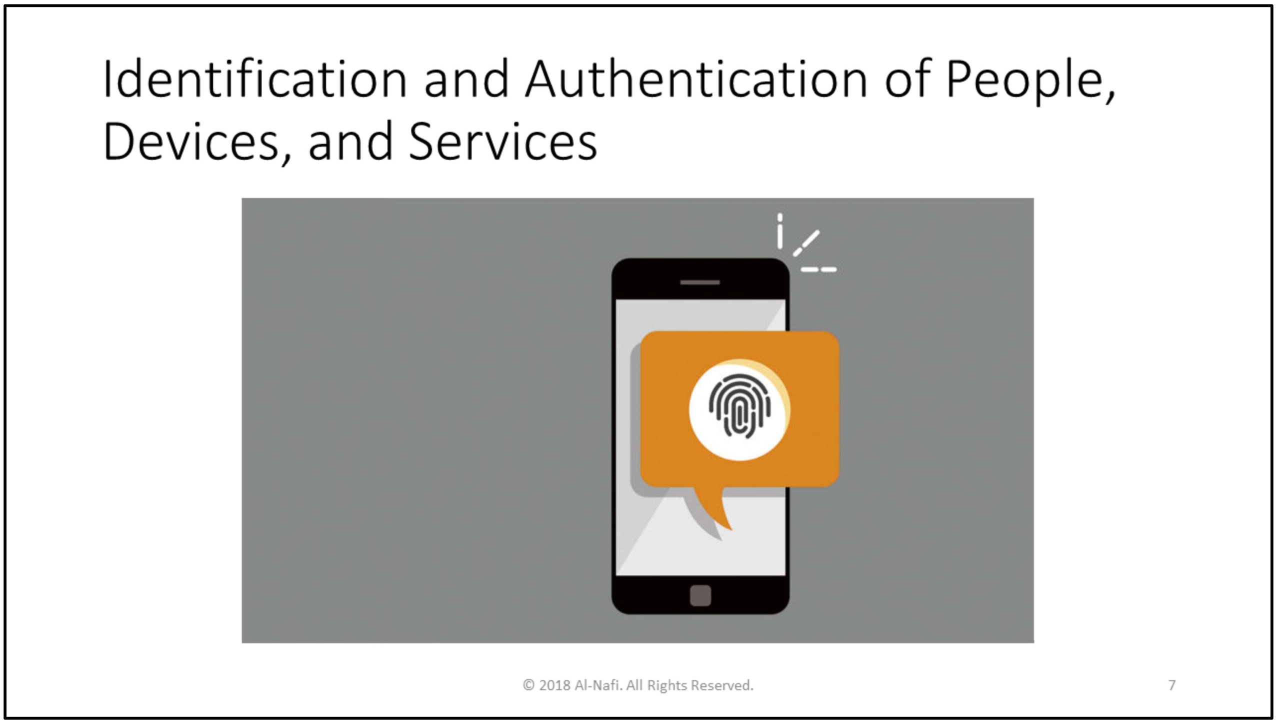
Provisioning and deprovision of access and identities involves a list of activities that are driven by business needs and requirements, job function and role, asset classification and categorization, and dynamic legal and regulatory issues. Users needing access to system resources go through a process of provisioning that rightly begins with the data/information owner expressing a business need for the stated access.

Vulnerabilities that are readily ascribed to technology often have their introduction by means of a lack of due care and due diligence related to administrative controls. Identity and access management (IAM) forms a lifecycle that begins with provisioning or enrollment, access and consumption of resources, and finally deprovisioning or revocation of access.

The Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance 4.7.1. As-is Analysis provides for three phases that manage the Provisioning and Deprovisioning process.

- Provision a user account and apply user permissions

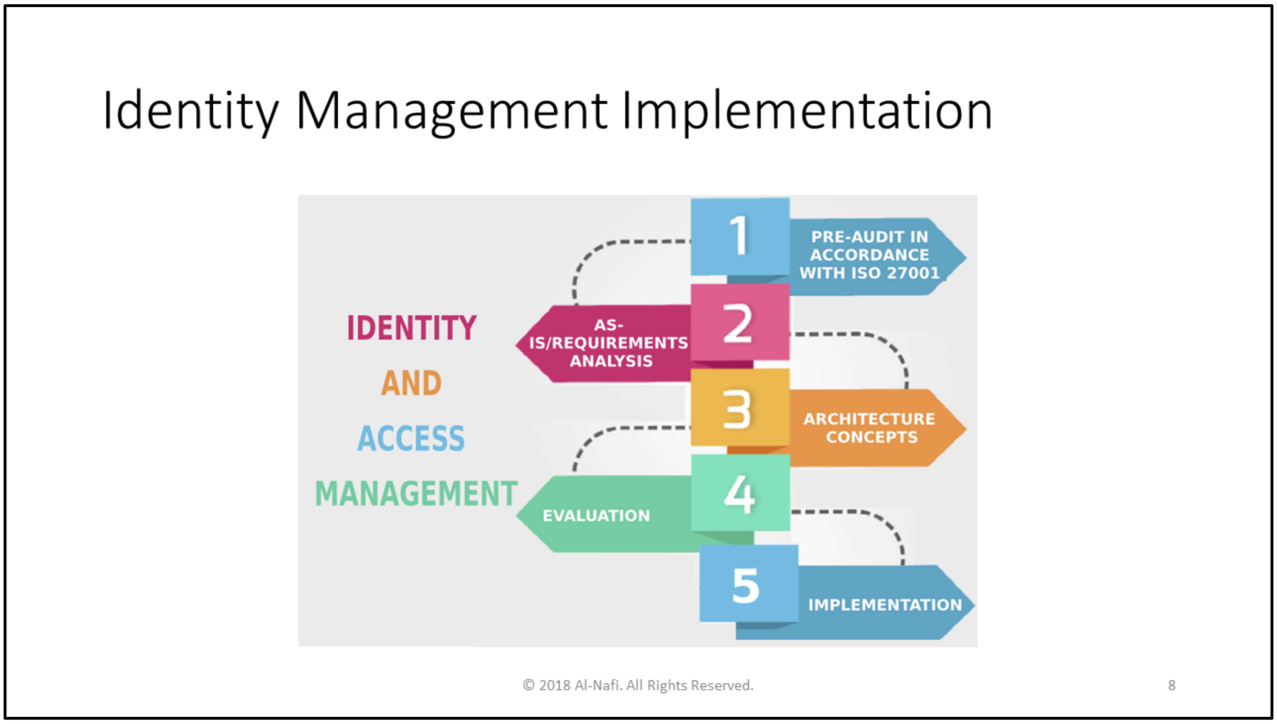
- Modify user permissions
- Deprovision user account and end user permissions



Identification and Authentication of People, Devices, and Services

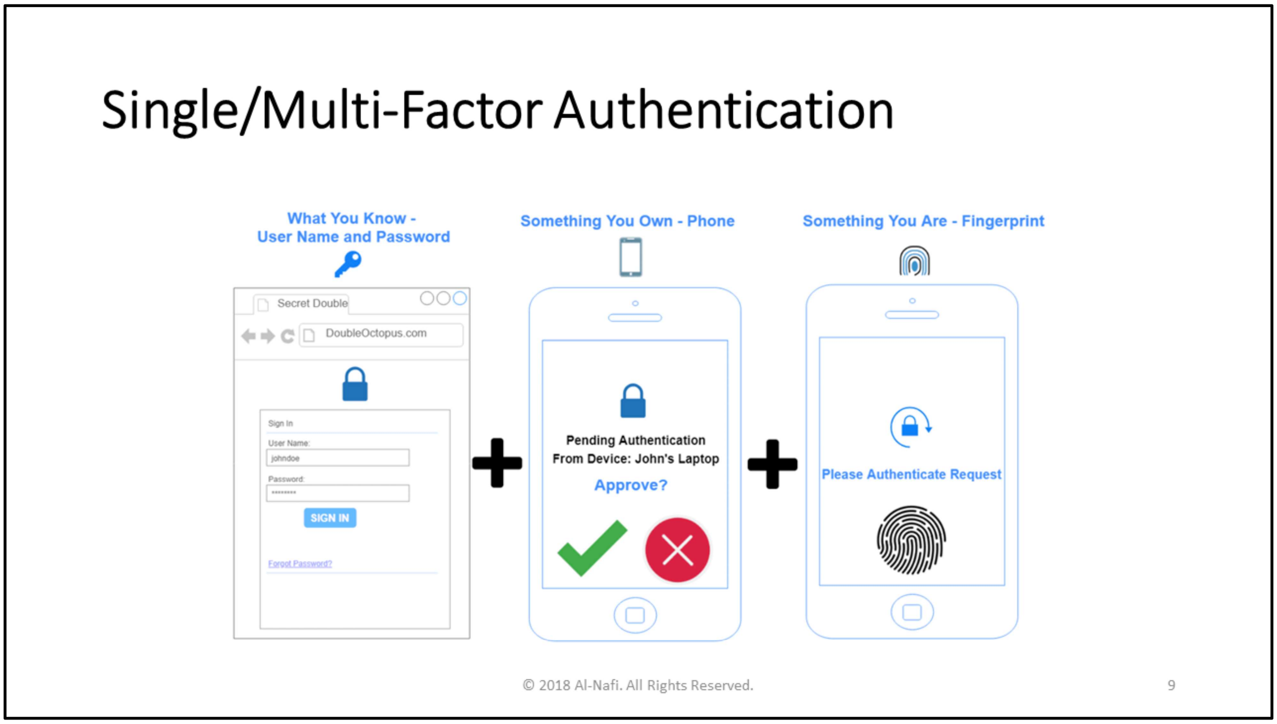
Identification

The objective of identification is to bind a user to the appropriate controls based on the unique user instance. For example, once the unique user is identified and validated through authentication, his or her identity within the infrastructure is used to allocate resources based on predefined privileges.



Identity Management Implementation

An identity represents the initial attribute in a linear succession of attributes to protect access and use of a system. Providing an identity to access a system is simply an assertion or claim of an entity. An assertion or claim made by an entity should be followed by rigorous proof that the entity's claim is legitimate. The attributes that follow an identity to prove out a legitimate claim are authentication, authorization, and usually some form of accountability. The downstream effect of proper identification includes accountability with a protected audit trail and the ability to trace activities to individuals. It also includes the provisioning of rights and privileges, system profiles, and availability of system information, applications, and services.



Single/Multi-Factor Authentication

9

Authentication within a system involves presenting evidence that an identified entity should be allowed access through a control point. Standard evidence for being allowed to log into a system includes three primary factors:

- Something you know, such as a password or PIN
- Something you have, such as a token or smart card
- Something you are or do, such as biometrics or a fingerprint

Single factor authentication involves a user or entity providing one type of evidence to support an assertion or claim for access to a system. The factor could be related to something the entity knows, something the entity has, something the entity is, or somewhere the entity is. One factor or type of evidence can have multiple methodologies. As an example, if an entity provided a password and a PIN that would be two methodologies of the same factor (something you know); thus, these two elements would be considered a single factor.

Multi-factor authentication involves an entity providing more than one factor of proof of their identity. An example of this would be an entity providing both a password and an iris scan to authenticate to a source. Each factor of authentication may represent an additional hurdle that needs to be overcome by the unauthorized. As the factors of authentication grow, then so grows the layers of defense or of defense in depth. Multifactor systems may increase the complexity of systems management or decrease or otherwise impact the productivity of the user attempting to gain access to the system. Burgeoning authentication methodologies include location and node. Location authentication makes use of geo-location data that can allow or disallow authentication from or to specific global locations. Service providers such as Netflix and Amazon use location authentication to protect against intellectual property content leakage or theft. Node authentication allows for device-type recognition to be used as a means of authentication. Examples of node authentication could include a specific smartphone, laptop, desktop, etc.