CYBER GIRLS

Identity and Access Management

An initiative of cybersafe. FOUNDATION

Course Objectives

On completing this course, you will be able to:

- Understanding of IAM concepts and technologies.
- Knowledge of IAM models.
- Understanding of IAM standards and regulation.
- Understanding of IAM best practices.

Course Outline

1. Introduction to Identity and Access Management
2. Models for Access Control
3. Identity and Access Management Process
4. IAM and PKI
5. Implementing Trust in IAM
6. IAM Best Practices
7. Case Studies in IAM Security
8. IAM for Regulatory Compliance
9. Identity and access management project

Introduction to Identity and Access Management

Identity and Access Management

What is IAM?

Identity and Access Management (IAM) refers to the set of policies, processes, and technologies used to manage digital identities and control access to resources.

CYBER GIRLS

The 3 As of IAM

Authentication

Password OTP Biometrics Digital Certificate

Authentication: This verifies the identity of a user or service trying to access a resource. Imagine it as checking someone's ID at the entrance to a building. Common methods of authentication include usernames and passwords, multi-factor authentication (MFA), and biometric scans.

Authorization

Access Control

Authorization: Once a user is authenticated, authorization determines what permissions they have on a resource. Continuing with the building analogy, this would be checking someone's ID to see if they have access to a specific floor or room. In IAM, authorization policies define what actions a user can take on a resource, such as read-only access, edit access, or full control.

Accounting

Logs Behavioural Analytics

Endpoint and Network Monitoring

Accounting: This tracks the usage of resources by users or services. Think of it like a security log that keeps track of who entered the building, what floor they went to, and when they left. Accounting data helps with tasks like auditing security breaches, identifying suspicious activity, and ensuring compliance with regulations.

Key Concepts in IAM

Core Principles

Least Privilege

Need to Know

Least Privilege: This principle dictates that users and systems should only be granted the minimum level of access necessary to perform their tasks. Think of it as giving someone a key to their office door, but not the master key to the entire building. In IAM, least privilege is implemented through role-based access control (RBAC). Users are assigned roles with predefined permissions, ensuring they only have access to the resources required for their specific function.

Separation of Duty

Protects against:
- Insider Threat
- BEC
- Social Engineering

Separation of Duty (SoD): This principle emphasizes distributing tasks across multiple users or systems. No single user should have complete control over a critical process. In IAM, SoD is achieved by dividing tasks like creating a user account, approving a transaction, and reconciling financial statements among different users. This ensures no single user can manipulate the system undetected.

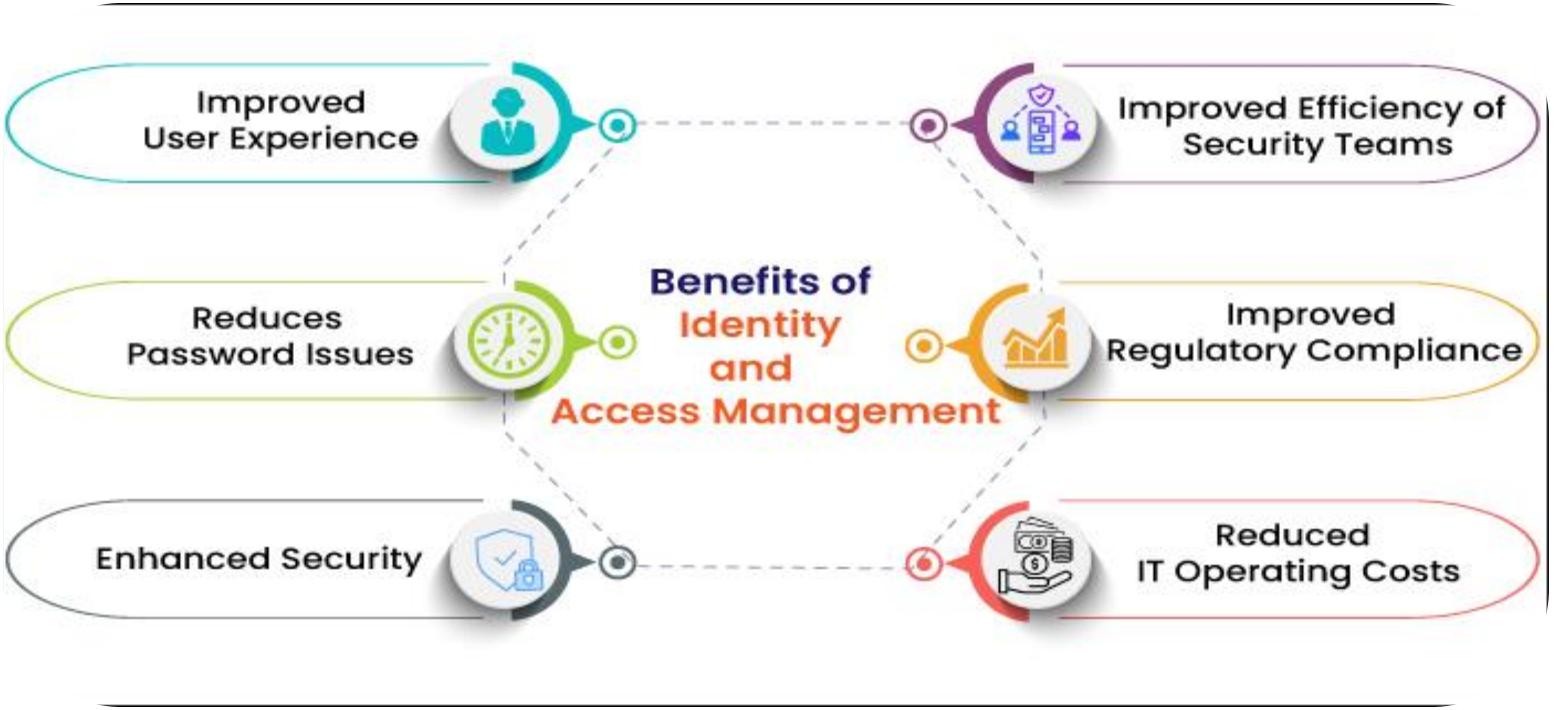
Zero Trust

Trust but Verify

Zero Trust: This is a security framework that constantly verifies access requests, regardless of a user's location or device. It assumes no one is inherently trustworthy, and every access attempt needs to be validated.In IAM, zero trust leverages multi-factor authentication (MFA) and continuous monitoring to verify access requests. Even if a hacker steals credentials, they'd likely be denied access at subsequent checkpoints within the system.

Benefits of IAM

IAM is becoming increasingly important in modern enterprise environments due to the growing number of digital identities, the increasing complexity of access control, and the need for regulatory compliance.


Improved User Experience
Improved Efficiency of Security Teams
Reduces Password Issues
Benefits of Identity and Access Management
Improved Regulatory Compliance
Enhanced Security
Reduced IT Operating Costs

Summary

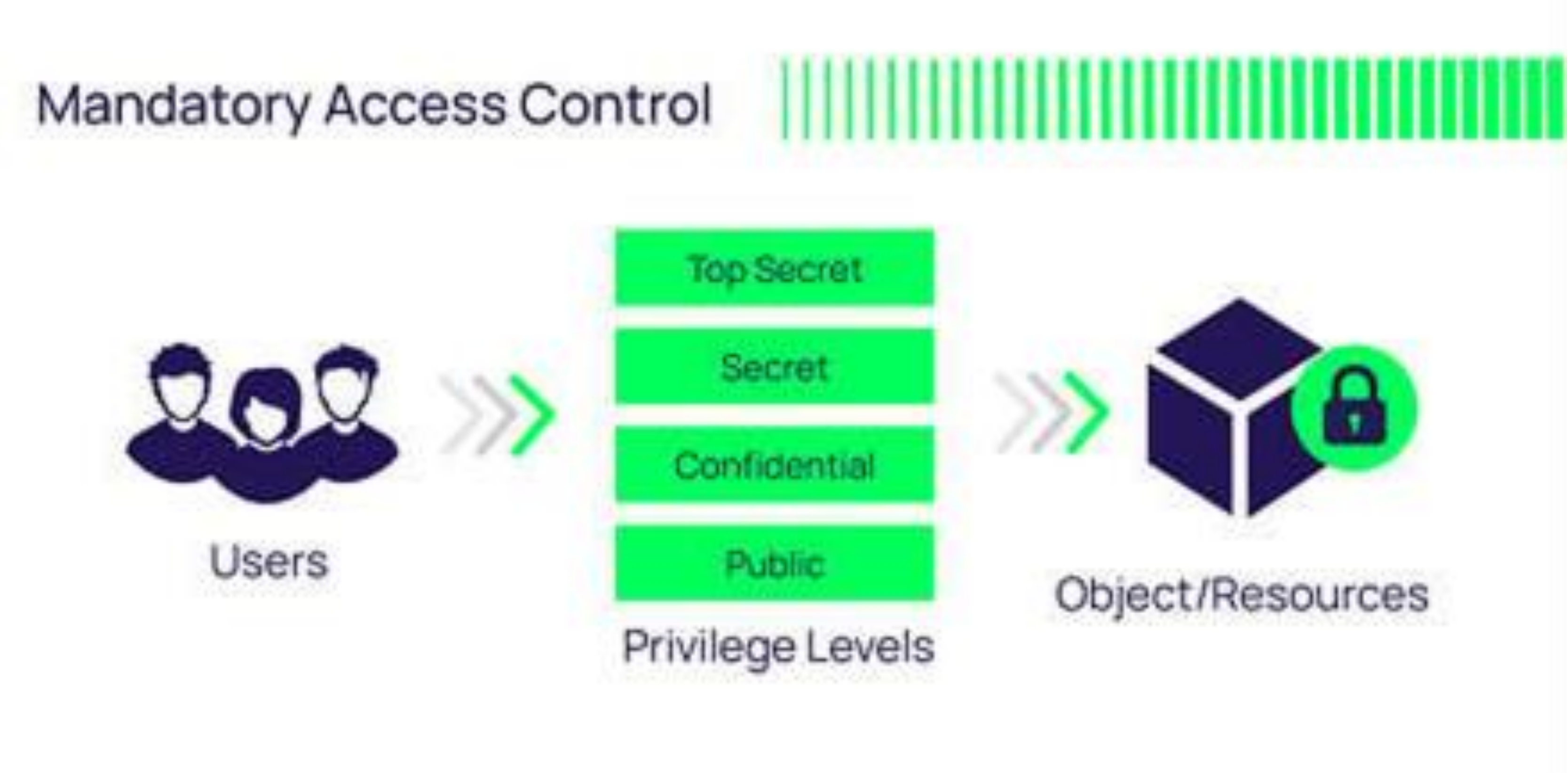
The goal of IAM is to ensure that only authorized users have access to the resources they need, while preventing unauthorized access and data breaches.

Models for Access Control

Models for Access Control

Mandatory Access Control (MAC)

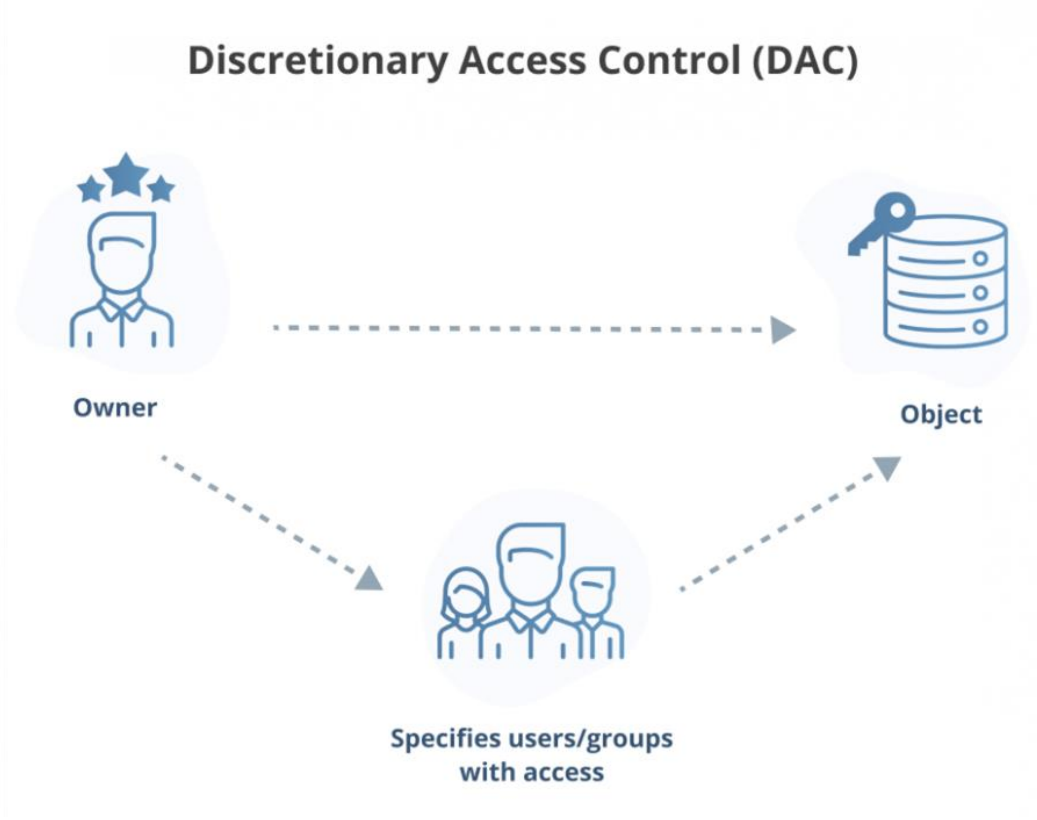
MAC enforces access control based on security labels assigned to objects and users



Models for Access Control Cont'd

Discretionary Access Control (DAC)

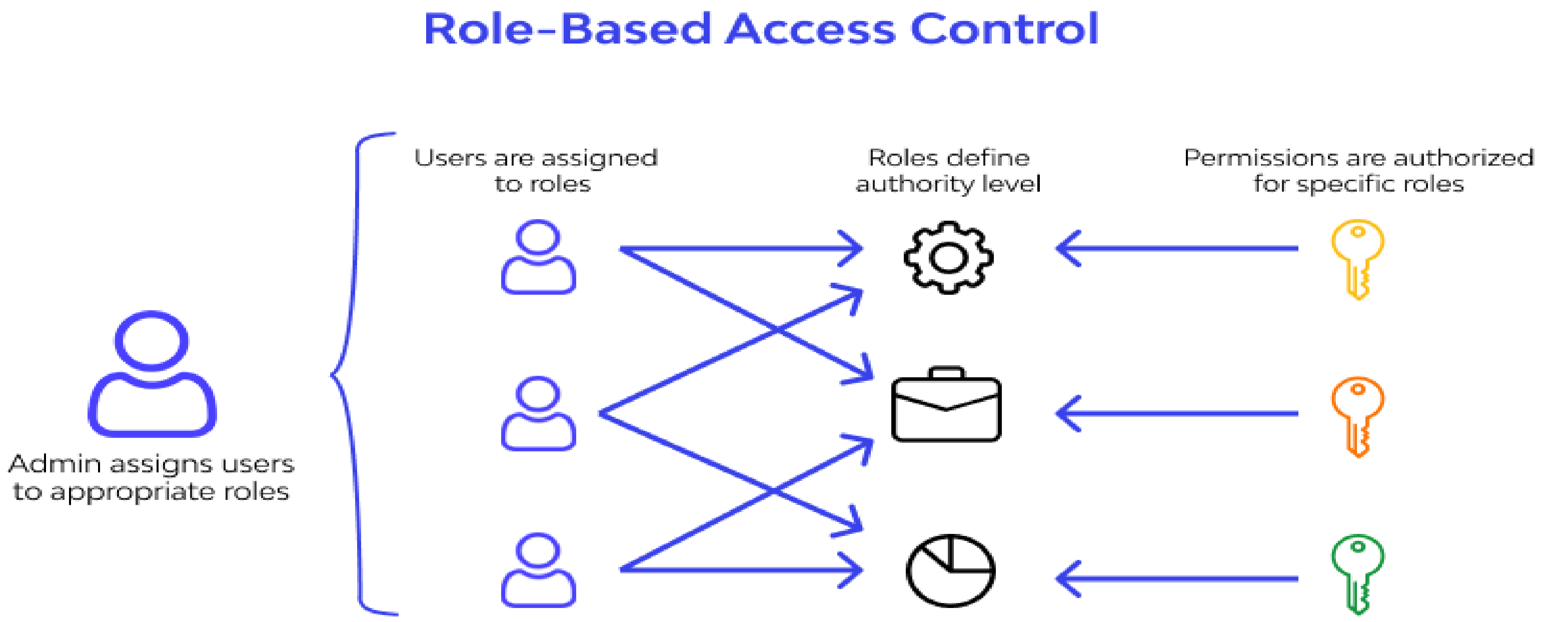
DAC places privilege management in the hands of resource owner


Discretionary Access Control (DAC)
Owner
Object
Specifies users/groups with access

Models for Access Control Cont’d

Role Based Access Control (RBAC)

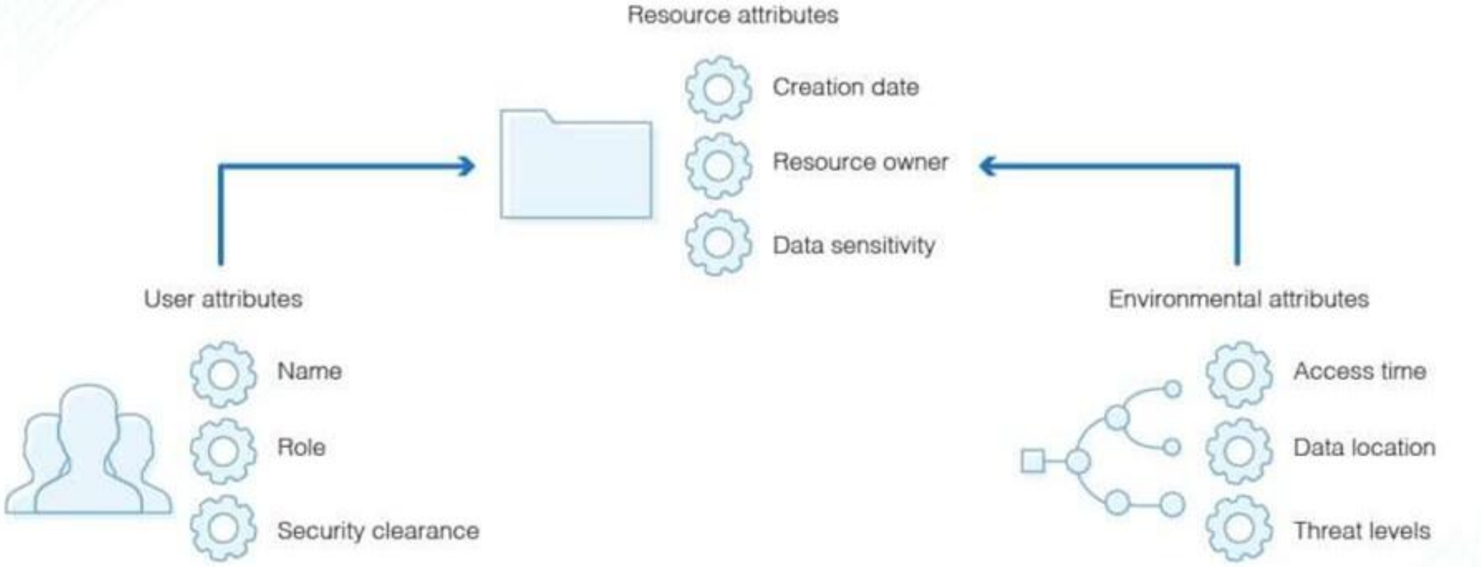
RBAC is based on defining roles for users and assigning permissions to those roles.


Role-Based Access Control
Users are assigned to roles
Roles define authority level
Permissions are authorized for specific roles
Admin assigns users to appropriate roles

Models for Access Control Cont'd

Attribute Based Access Control (ABAC)

ABAC uses attributes, such as user roles, time of day, and location, to determine access.



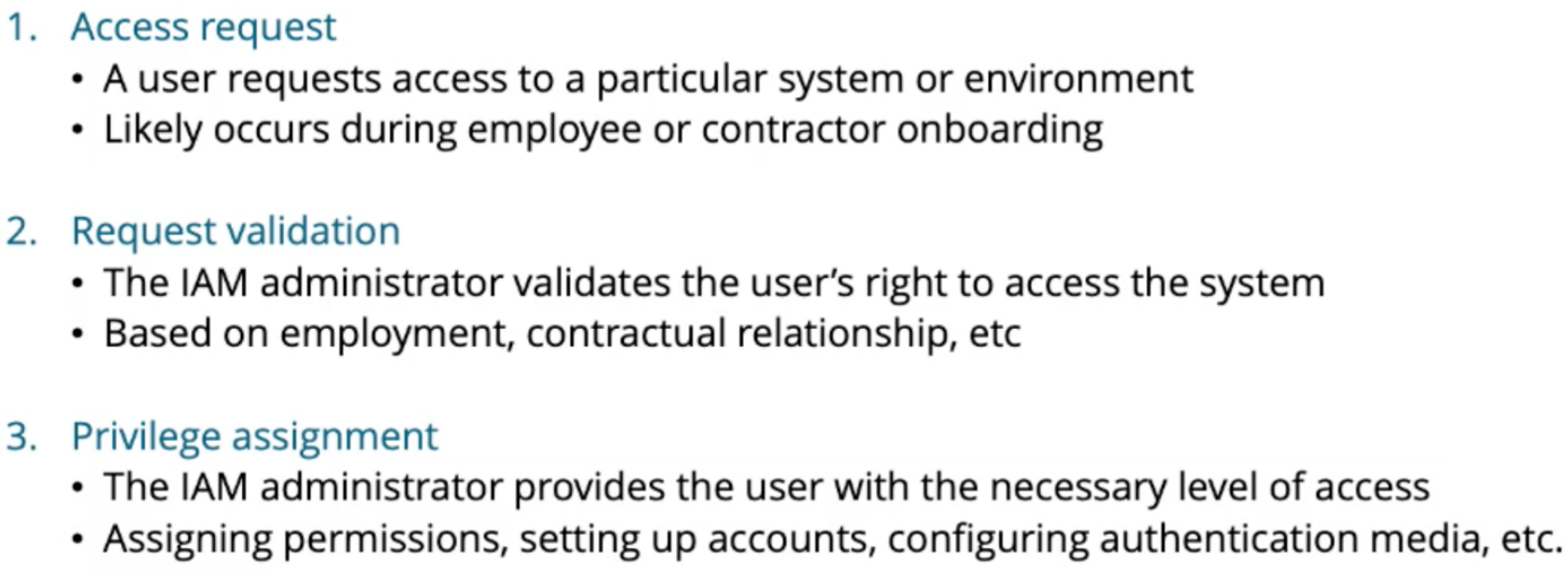
Summary

Each access control model has its own strengths and limitations, and organizations may choose to implement one or more models depending on their specific needs.

Identity and Access Management Process

High-Level Overview of IAM Process

Provisioning is the process of onboarding users into the AMS



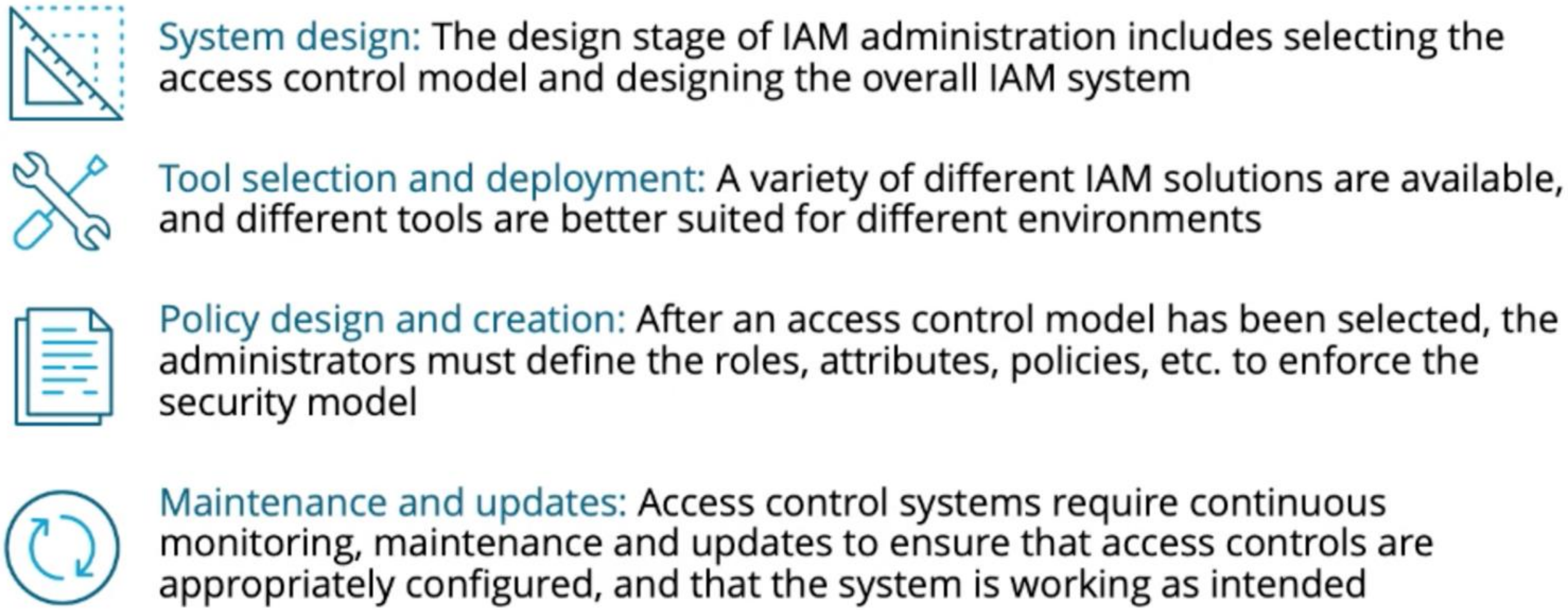
1. Access request
   - A user requests access to a particular system or environment
   - Likely occurs during employee or contractor onboarding

2. Request validation
   - The IAM administrator validates the user’s right to access the system
   - Based on employment, contractual relationship, etc

3. Privilege assignment
   - The IAM administrator provides the user with the necessary level of access
   - Assigning permissions, setting up accounts, configuring authentication media, etc.

High-Level Overview of IAM Process Cont’d

Administration includes the design of the IAM system to implementation to continuous monitoring.



System design: The design stage of IAM administration includes selecting the access control model and designing the overall IAM system

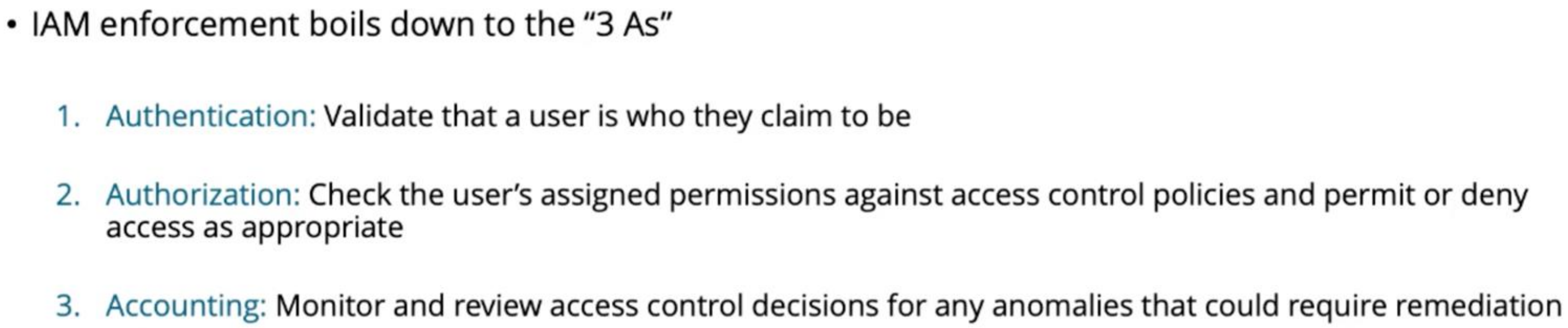
Tool selection and deployment: A variety of different IAM solutions are available, and different tools are better suited for different environments

Policy design and creation: After an access control model has been selected, the administrators must define the roles, attributes, policies, etc. to enforce the security model

Maintenance and updates: Access control systems require continuous monitoring, maintenance and updates to ensure that access controls are appropriately configured, and that the system is working as intended

High-Level Overview of IAM Process Cont’d

Enforcement involves deploying the right tools including monitoring and auditing to ensure the system works as designed.



- IAM enforcement boils down to the “3 As”

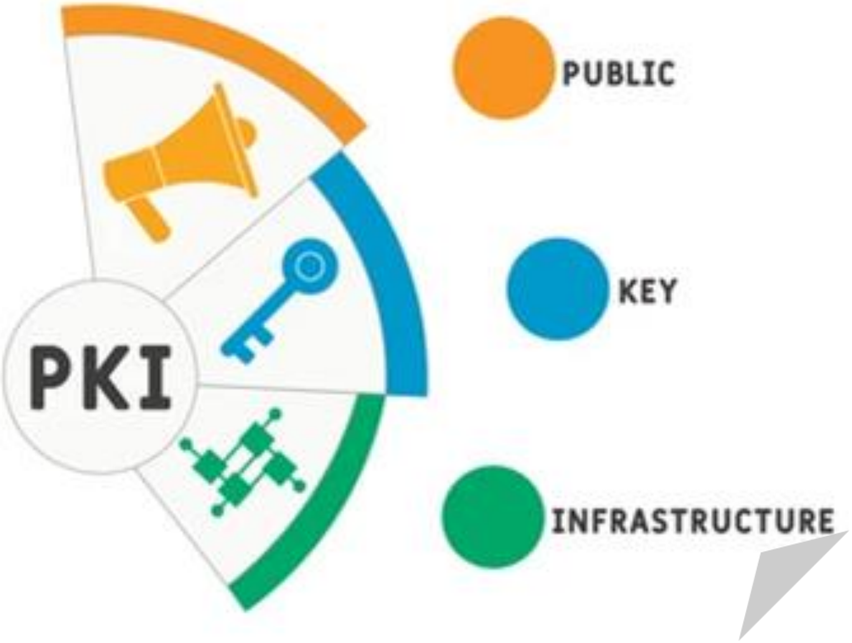
1. Authentication: Validate that a user is who they claim to be
2. Authorization: Check the user’s assigned permissions against access control policies and permit or deny access as appropriate
3. Accounting: Monitor and review access control decisions for any anomalies that could require remediation

Summary

Effective IAM processes can help organizations improve security, reduce the risk of data breaches, and ensure compliance with regulatory requirements.

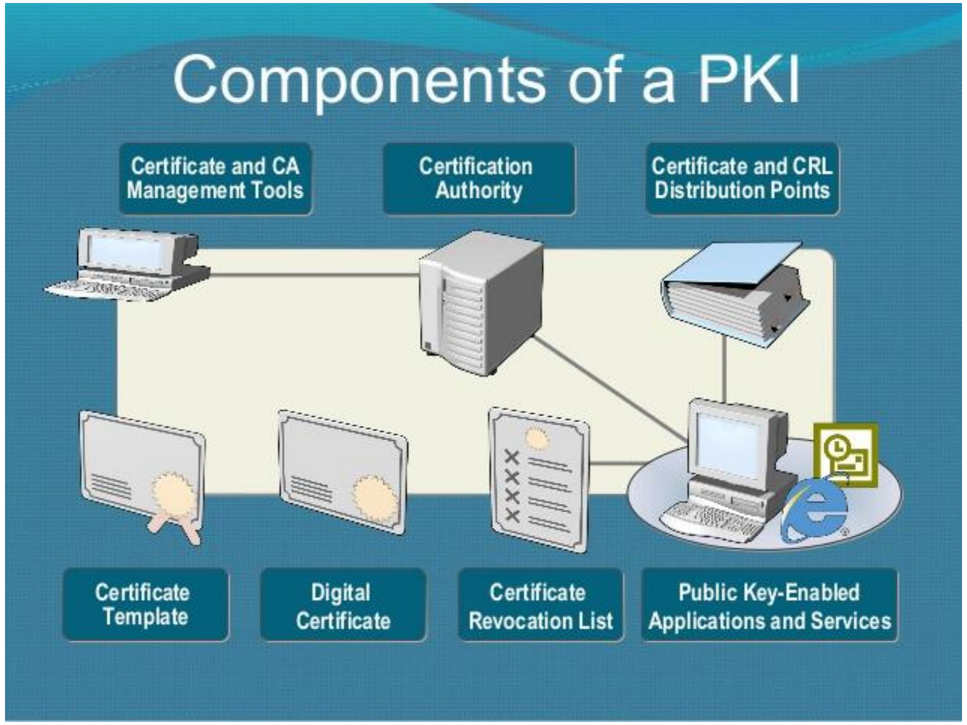
IAM and PKI

Introduction to PKI



Public Key Infrastructure (PKI) is a framework for managing digital certificates, encryption keys, and other security credentials.

PKI Management



Components of a PKI

Certificate and CA Management Tools

Certification Authority

Certificate and CRL Distribution Points

Certificate Template

Digital Certificate

Certificate Revocation List

Public Key-Enabled Applications and Services

Public Key Infrastructure (PKI) is the foundation for secure communication in today's digital world.

It relies on cryptography to establish trust between entities by using digital certificates to verify identities and encrypt data.

However, maintaining a robust PKI requires effective management practices

Components of PKI Management

Certificate Authorities: Trusted entities issuing, managing, and revoking digital certificates (secure them with strong access controls and tamper-proof audit logs).

Certificate Lifecycle Management: Automate issuance, enrollment, renewal, revocation, and expiration.

Registration Authority (Optional): Verify user/entity identity requesting certificates (define authentication and data collection procedures).

Enrollment: Secure user/entity certificate requests with strong authentication and secure communication channels.

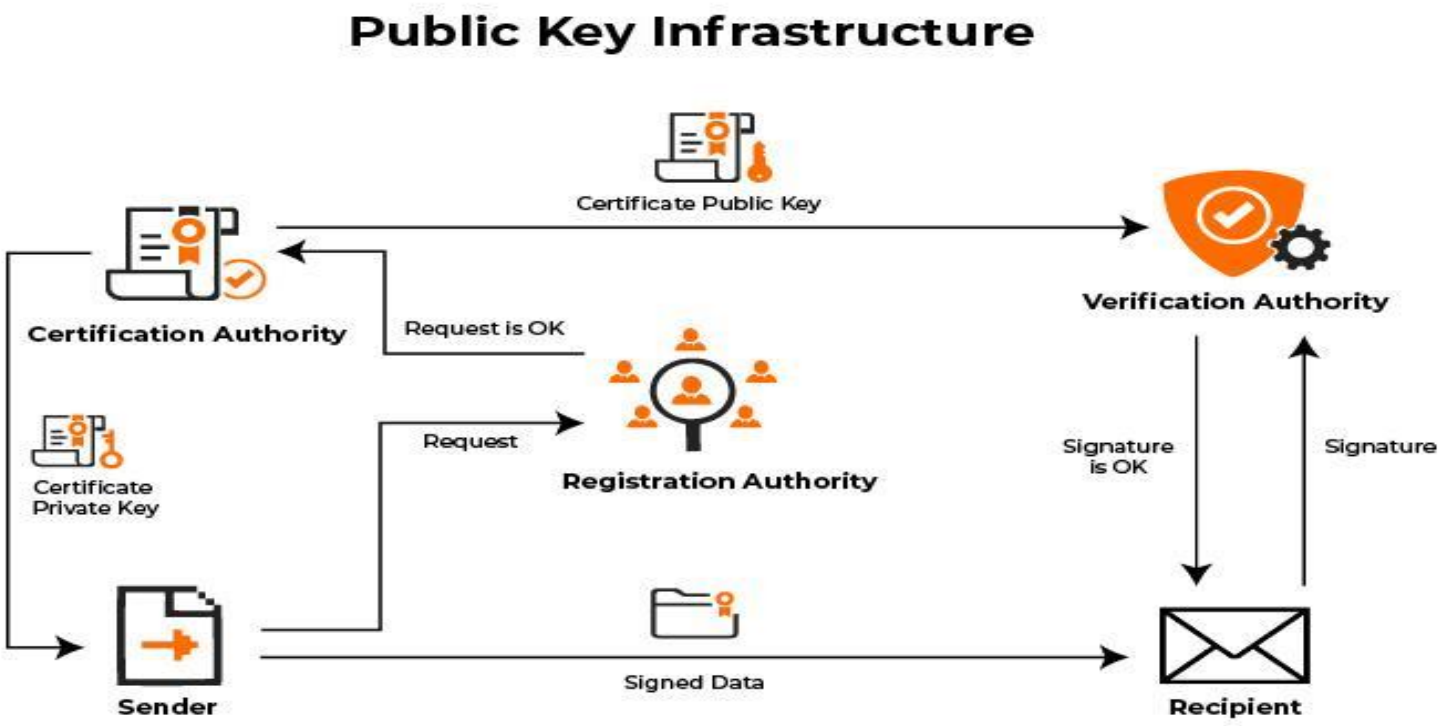
Policy Management: Define and enforce clear policies for certificate issuance, usage, and revocation.

Security Management: Secure CA servers, implement robust access controls, and regularly patch vulnerabilities.

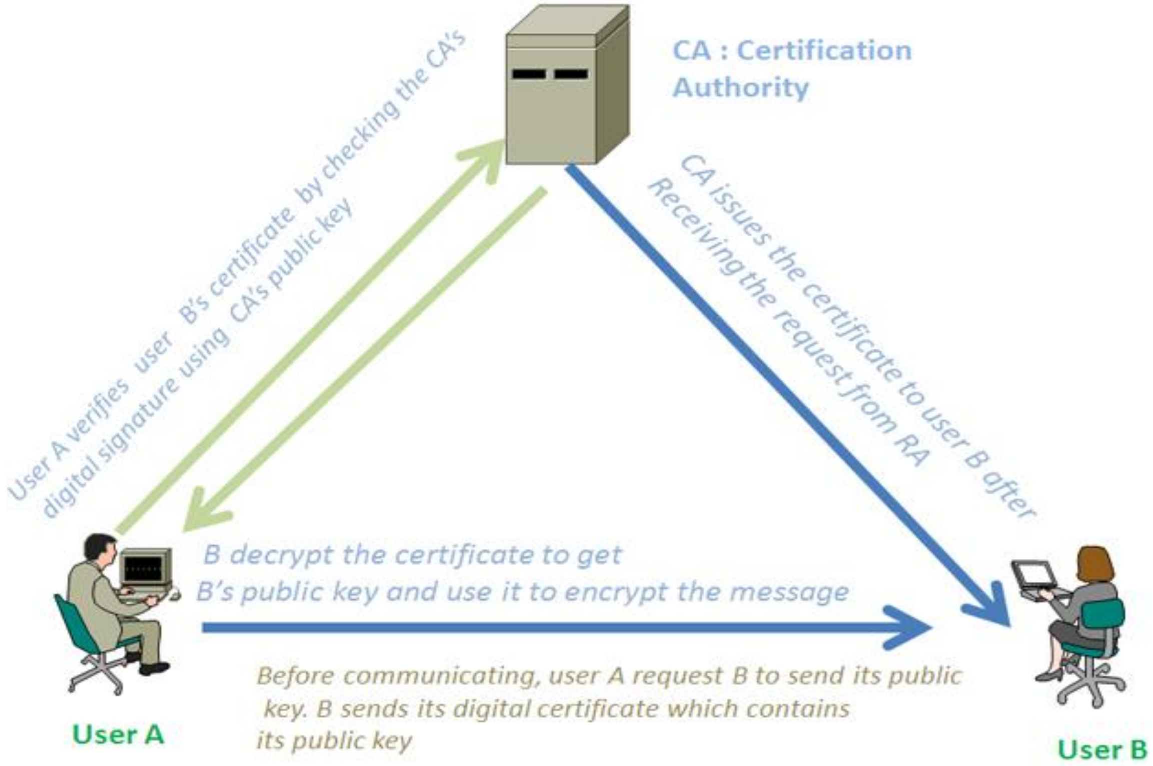
Auditing & Logging: Define auditing requirements, securely store logs, and conduct regular audits.

Role in PKI

PKI can be used as part of an IAM system to provide secure authentication, authorization, and encryption of data.



Digital Certificate



CA : Certification Authority

User A verifies user B's certificate by checking the CA's digital signature using CA's public key

CA issues the certificate to user B after Receiving the request from RA

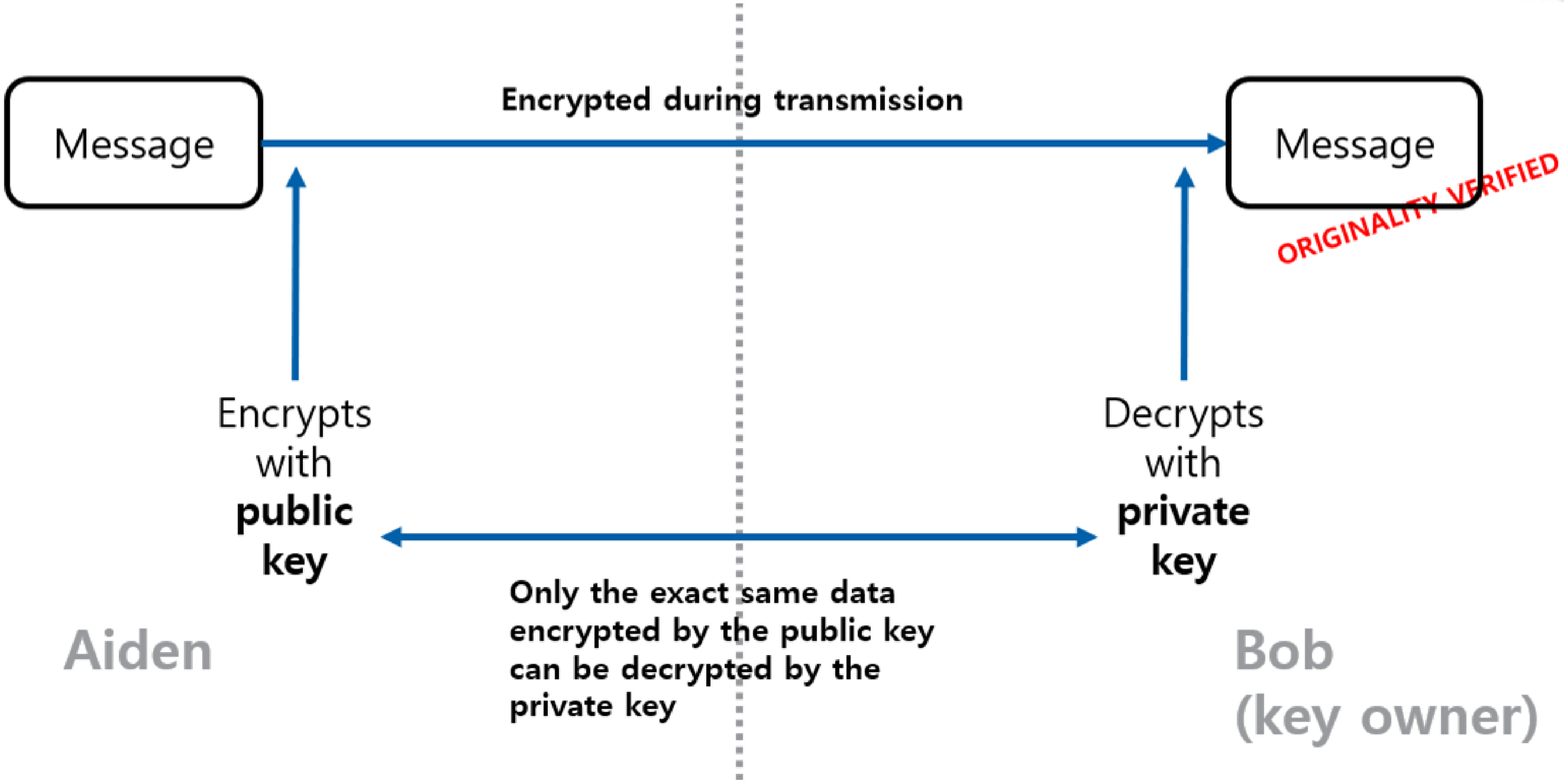
B decrypt the certificate to get B's public key and use it to encrypt the message

Before communicating, user A request B to send its public key. B sends its digital certificate which contains its public key

Simplified diagram: Secure communication with digital certifica'

PKI can be used to issue digital certificates that are used to verify the identity of users and devices.

PKI Security


Message
Encrypted during transmission
Message
ORIGINALITY VERIFIED
Encrypts with **public key**
Decrypts with **private key**
Only the exact same data encrypted by the public key can be decrypted by the private key
Aiden
Bob (key owner)

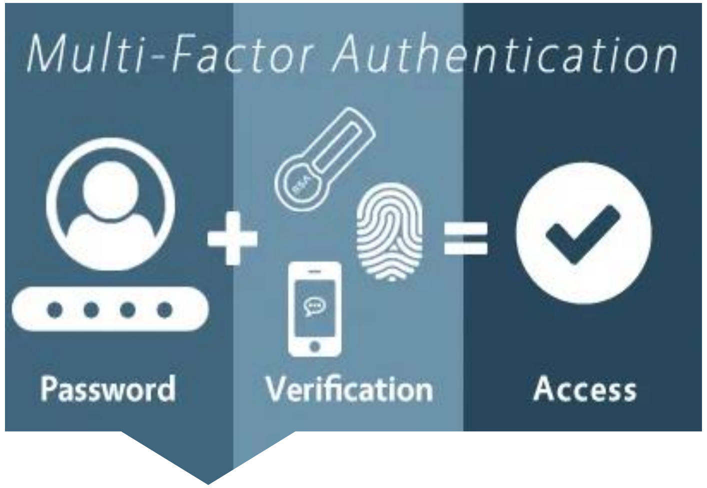
PKI can also be used to encrypt data in transit and at rest, ensuring that only authorized users can access it.

Summary

Implementing PKI as part of an IAM system can improve security, reduce the risk of data breaches, and help organizations meet regulatory requirements.

Implementing Trust in IAM

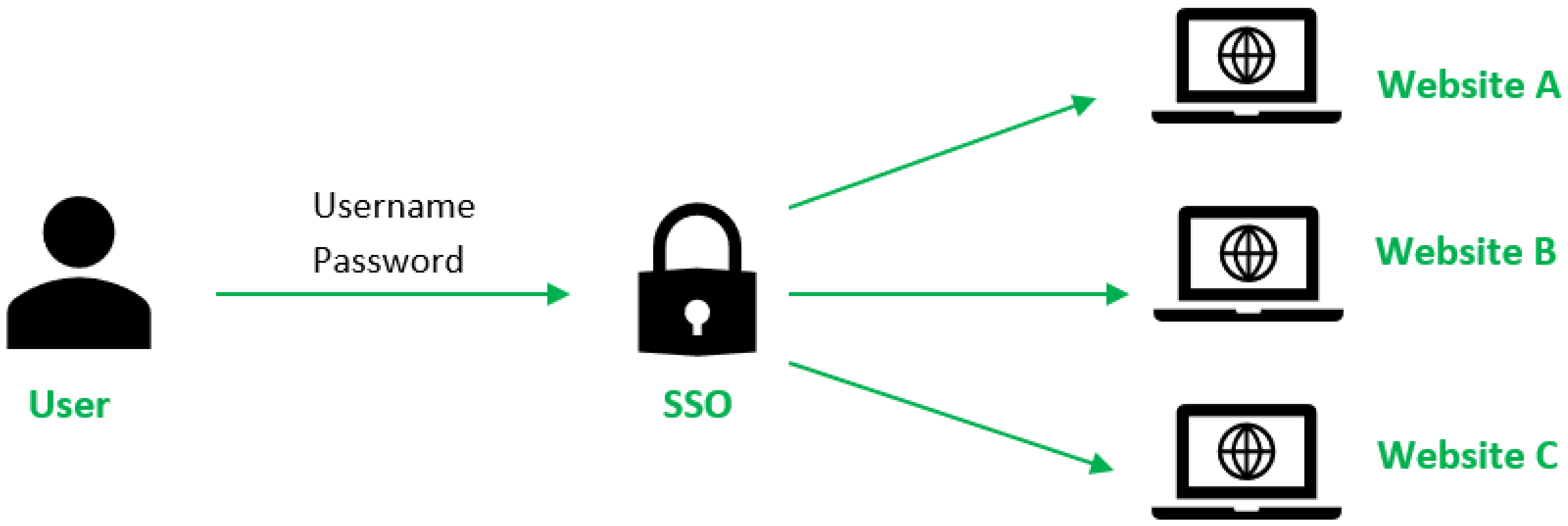
Introduction to Trust



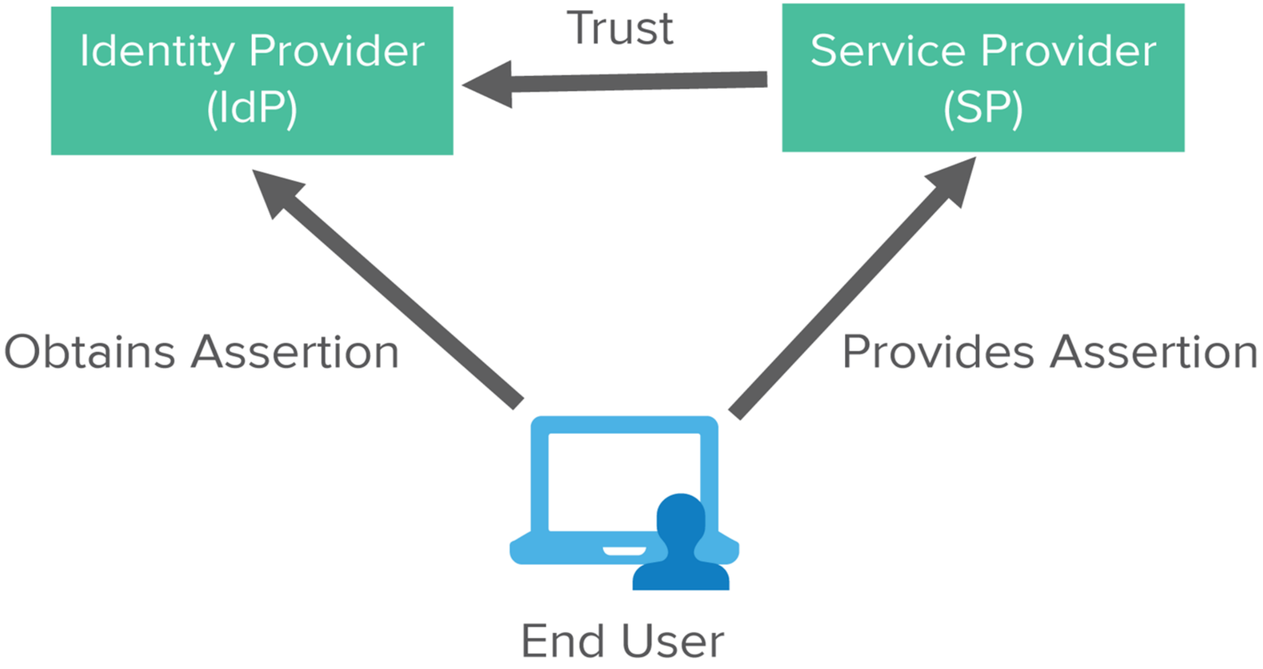
- Trust is a critical component of IAM, as it is essential to ensure that only authorized users are granted access to resources.
- Trust can be established through several methods, including multi-factor authentication, biometrics, and digital certificates.

Single Sign-On

Single sign-on (SSO) is a method of authentication that allows users to log in once and access multiple applications or resources without needing to enter separate login credentials for each one.

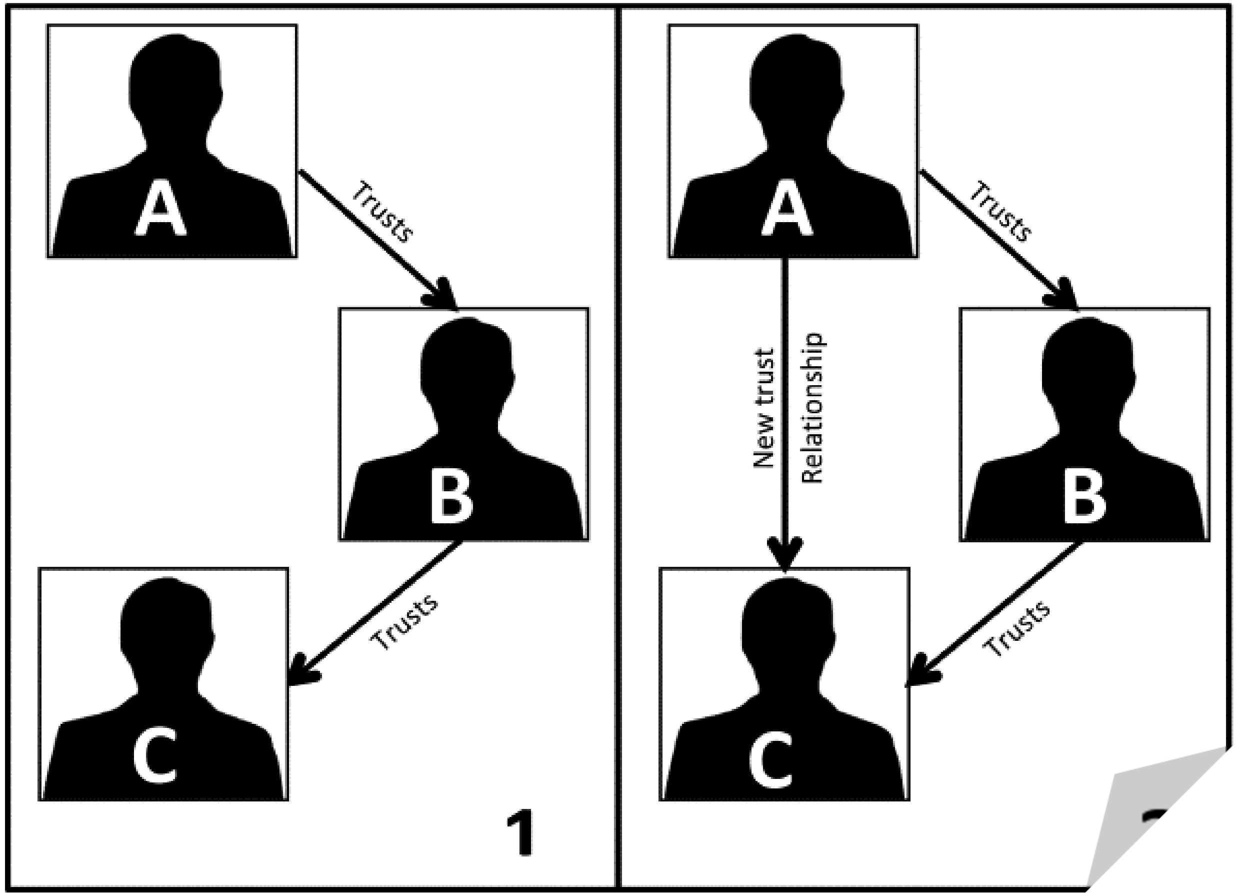


Federation



Federation is a method of identity management that allows users to access resources across multiple domains or organizations using a single set of credentials.

Transitive trust



Transitive trust is a method of establishing trust between multiple entities by relying on the trust established between other entities. For example, if entity A trusts entity B and entity B trusts entity C, then entity A can trust entity C through transitive trust.

Summary

Implementing trust, SSO, federation, and transitive trust in an IAM system is essential to ensure the security and integrity of digital assets and to prevent unauthorized access and data breaches.

Summary

IAM best practices encompass a comprehensive collection of guidelines and strategic recommendations designed to optimize the implementation and management of an effective Identity and Access Management (IAM) system.

These practices are essential for ensuring robust security, operational efficiency, and regulatory compliance within an organization.

Case Studies in IAM Security

Class Activity 1

In this class activity, we will review case studies of real-world IAM security incidents and discuss the lessons learned.

Divide the class into small groups and assign each group one of the following case studies:

The Target data breach in 2013
The Equifax data breach in 2017
The Capital One data breach in 2019

To be continued……

Class Activity 1 (Cont.)

In their groups, students should review the case study and discuss the following questions:

- What were the root causes of the security incident?
- What were the consequences of the security incident for the organization and its customers?
- What could the organization have done to prevent the security incident?
- What IAM best practices could the organization have implemented to improve its security posture?

After the group discussion, each group should present their findings to the class and facilitate a group discussion on the key lessons learned from the case study.

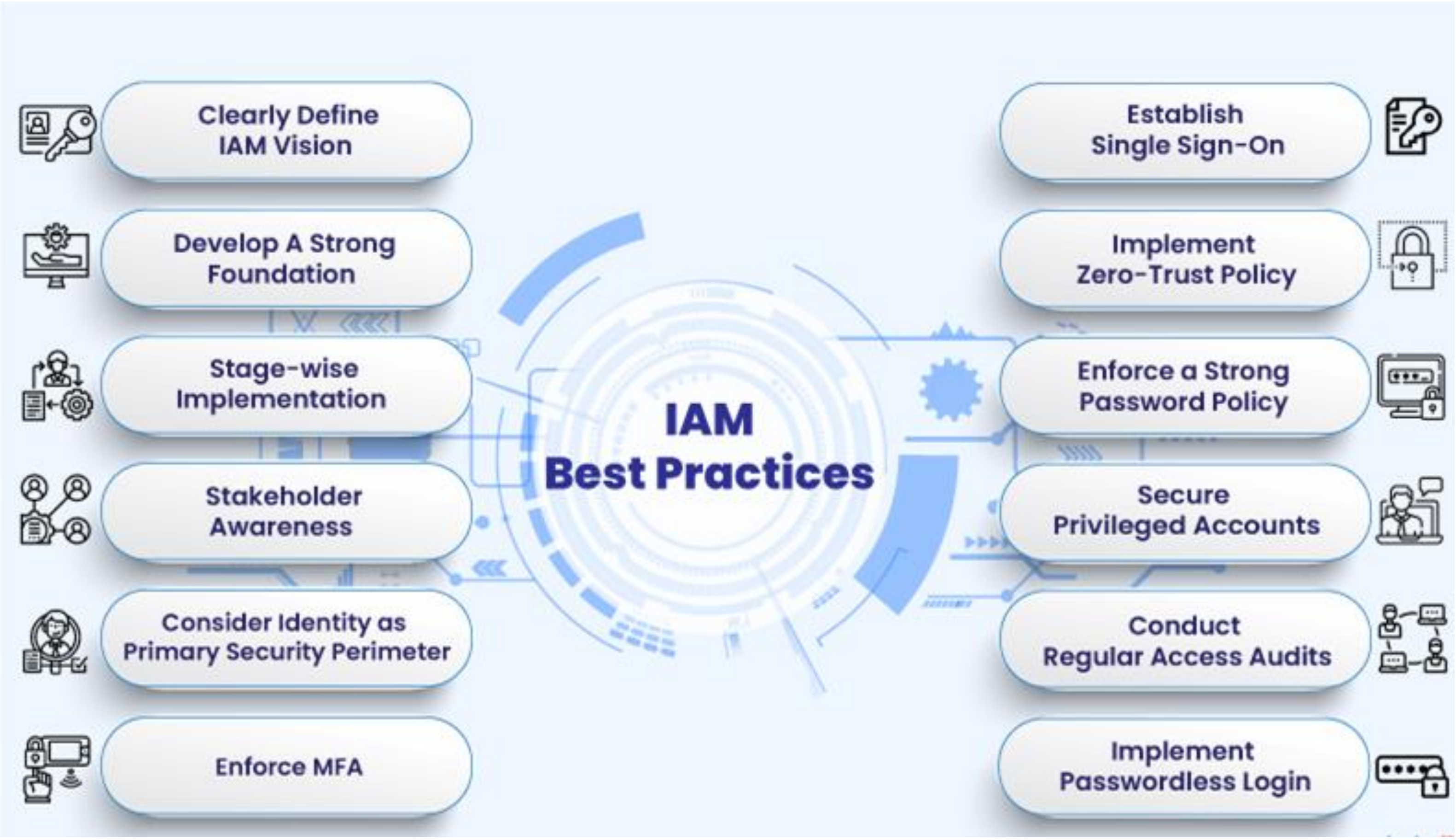
Summary

Case studies offer real-world examples illustrating the significant impact of IAM (Identity and Access Management) security on organizations and the potential consequences of security incidents.

These studies highlight how effective IAM practices can enhance security posture, prevent unauthorized access, and mitigate risks, while also demonstrating the detrimental effects of IAM failures, such as data breaches, financial losses, and reputational damage.

IAM Best Practices

Some of the key IAM best practices include:

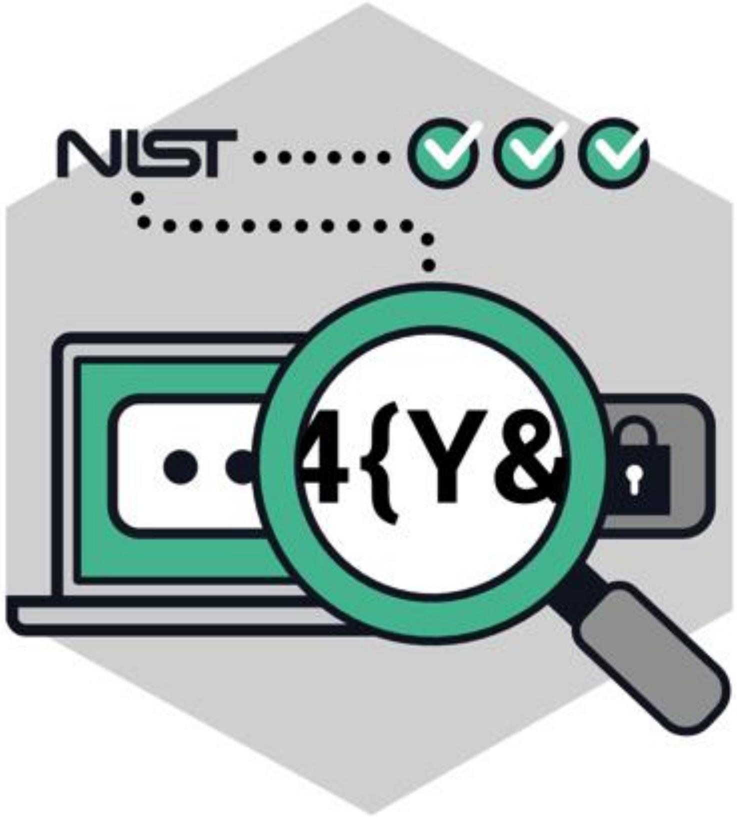


IAM Best Practices

- Clearly Define IAM Vision
- Develop A Strong Foundation
- Stage-wise Implementation
- Stakeholder Awareness
- Consider Identity as Primary Security Perimeter
- Enforce MFA
- Establish Single Sign-On
- Implement Zero-Trust Policy
- Enforce a Strong Password Policy
- Secure Privileged Accounts
- Conduct Regular Access Audits
- Implement Passwordless Login

Some of the key IAM best practices include:

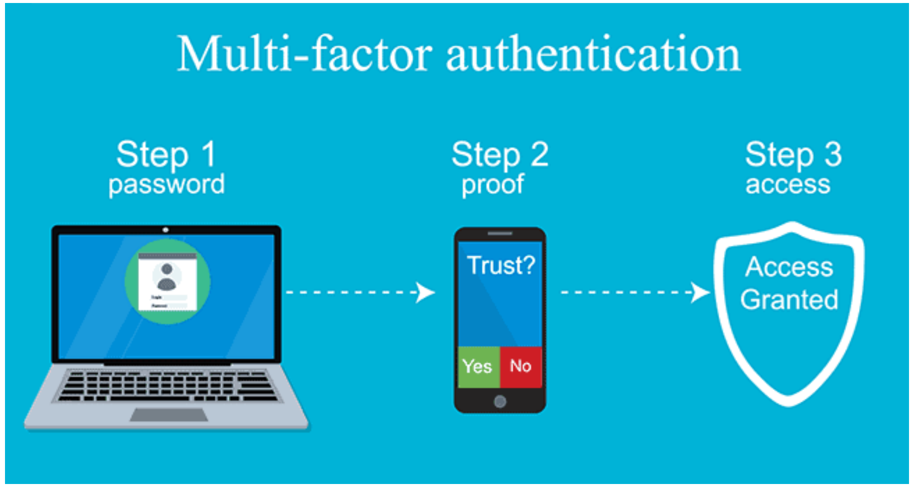
Password Security Policy



- ☒ Previous breach exposures
- ☒ Less than 8 characters
- ☒ Context-specific words
- ☒ Dictionary words
- ☒ Repetitive characters
- ☒ Password hints

Some of the key IAM best practices include:

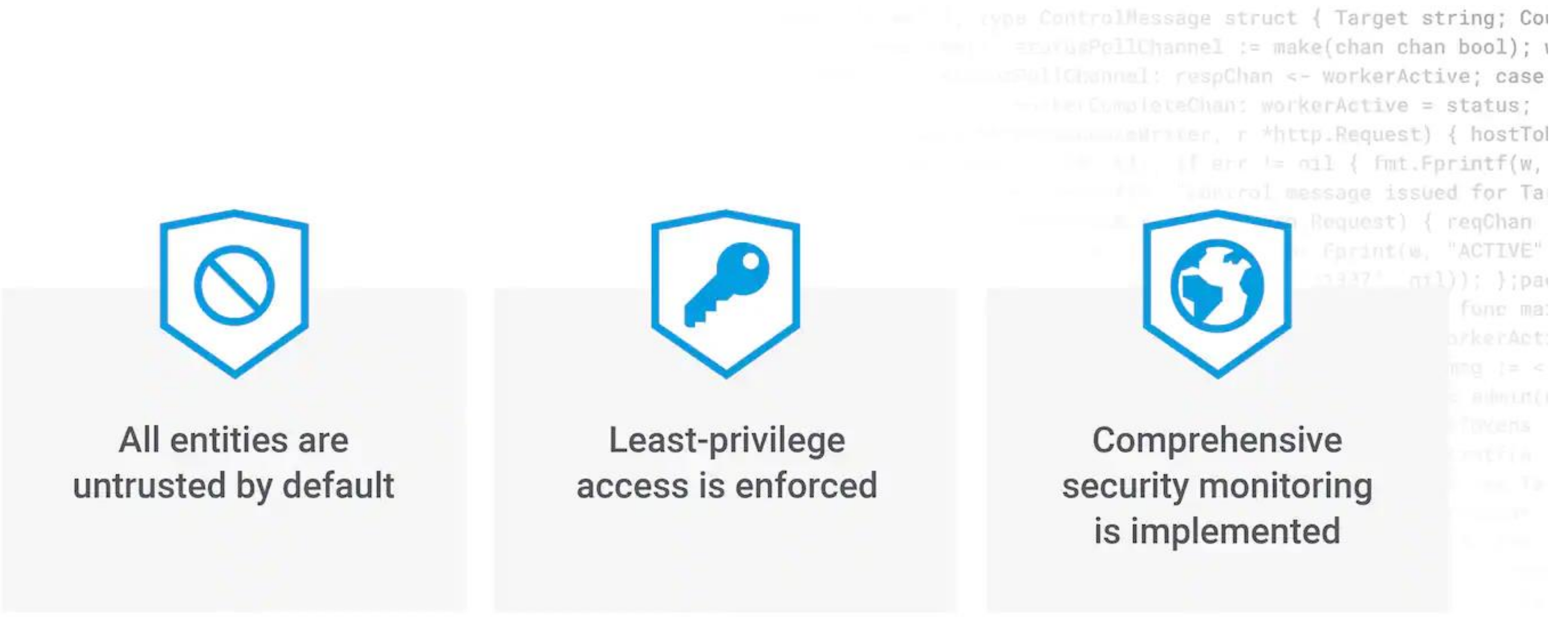
Enforce MFA



Enforcing MFA (Multi-Factor Authentication) in IAM (Identity and Access Management) strengthens security by adding an extra layer of verification during the sign-in process.

Some of the key IAM best practices include:

Zero Trust Security Policy



```
type ControlMessage struct { Target string; Co
statusPollChannel := make(chan chan bool); 
statusPollChannel: respChan <- workerActive; case
workerCompleteChan: workerActive = status;
r *http.Request) { hostTo
if err != nil { fmt.Fprintf(w,
Control message issued for Ta
Request) { reqChan
fmt.Fprint(w, "ACTIVE"
nil)); };pa
func ma
workerAct
```

All entities are untrusted by default

Least-privilege access is enforced

Comprehensive security monitoring is implemented

IAM for Regulatory Compliance

IAM Requirements for Government

- Enforcing MFA for all user access significantly reduces the risk of unauthorized access even if credentials are compromised.
- Granting users only the minimum access permissions necessary for their job functions minimizes potential damage from compromised accounts.
- Distributing tasks and access across multiple users prevents any single person from having complete control over critical processes.
- Comprehensive logging of user activity allows for monitoring, identifying suspicious behavior, and ensuring accountability.

IAM for compliance

- Regulatory compliance refers to the set of rules and regulations that organizations must follow to protect sensitive data and ensure privacy.
- Many industries, such as healthcare, finance, and government, are subject to strict regulatory requirements for data security and privacy, such as HIPAA, PCI DSS, and GDPR.
- IAM can help organizations meet these regulatory requirements by providing a framework for managing and securing user identities and access to sensitive data.

Key IAM Requirements for Data Protection

- Maintaining an audit trail of user activity to demonstrate compliance with regulatory requirements.
- Ensuring that only authorized users have access to sensitive data and applications.
- Implementing strong authentication mechanisms, such as MFA, to prevent unauthorized access to sensitive data.
- Enforcing data encryption to protect sensitive data from unauthorized access or disclosure.

Summary

By implementing IAM for regulatory compliance, organizations can reduce the risk of regulatory violations and penalties, as well as improve their overall security posture.

However, it is important for organizations to stay up-to-date with the latest regulatory requirements and ensure their IAM systems are compliant with all applicable regulations.

Thank You