Identity and Access Management

Identity and access management architecture

Identity and access management (IAM) is a framework of business processes, policies, and technologies that facilitates the management of electronic or digital identities.

By IAM, information technology (IT) managers can control user access to critical information within their organizations.

IAM systems can be deployed on-premises, provided by a third-party vendor through a cloud-based subscription model, or deployed in a hybrid model.

Components of IAM

On a fundamental level, IAM encompasses the following components:

- How individuals are identified in a system (understand the difference between identity management and authentication);
- How roles are identified in a system and how they are assigned to individuals;
- Adding, removing, and updating individuals and their roles in a system;
- Assigning levels of access to individuals or groups of individuals; and
- Protecting the sensitive data within the system and securing the system itself.

Authentication and Authorization

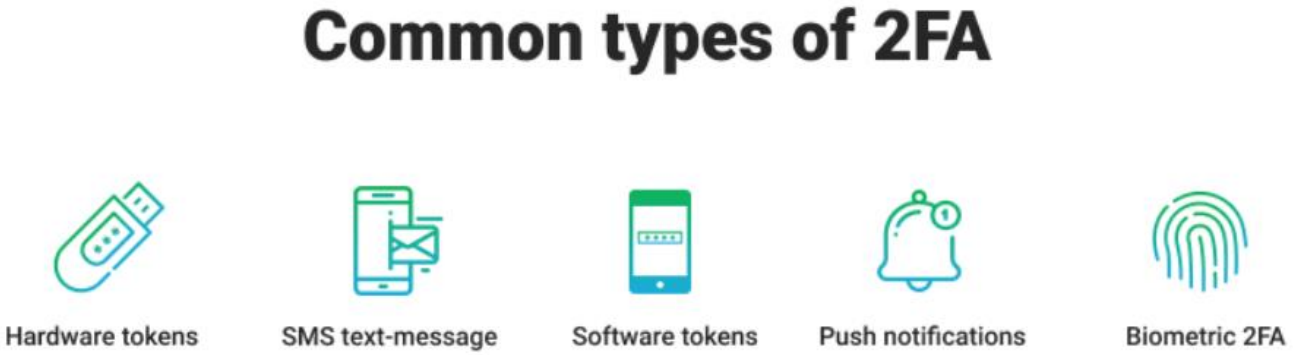
Any combination of the following 3 factors will be considered Strong Authentication:

- What you know
  - Password
  - Passphrase
- What you are
  - Iris
  - Fingerprint
- What you have
  - Token
  - Smartcard

2 primary forms of Authorization:

- Coarse-Grain
  - High-level and overarching entitlements
  - Create, Read, Update, Modify
- Fine-Grain
  - Detailed and explicit entitlements
  - Based on factors such as time, dept, role, and location

Types of 2FA


Common types of 2FA
Hardware tokens
SMS text-message
Software tokens
Push notifications
Biometric 2FA

Types of digital authentication

- **Unique passwords:** The most common type of digital authentication is the unique password. To make passwords more secure, some organizations require longer or more complex passwords that require a combination of letters, symbols, and numbers.
- **Pre-shared key (PSK): PSK is another type of digital authentication in which the password is shared among users authorized to access the same resources—**think of a branch office Wi-Fi password. This type of authentication is less secure than individual passwords.

Identity and Access Management tools

IAM technologies and tools

- IAM technologies are designed to simplify the user provisioning and account setup process.
- These systems should reduce the time to complete these processes with a controlled workflow that decreases errors and the potential for abuse while allowing automated account fulfillment.
- An IAM system should allow administrators to view and change evolving access roles and rights instantly.
- IAM systems should be used to provide flexibility to establish groups with specific privileges for specific roles so that access rights based on employee job functions can be uniformly assigned.

Benefits of IAM

- Access privileges are granted per policy, and all individuals and services are properly authenticated, authorized, and audited.
- Companies that properly manage identities have greater control of user access, which reduces the risk of internal and external data breaches.
- Automating IAM systems allows businesses to operate more efficiently by decreasing the effort, time, and money required to manually manage access to their networks.
- In terms of security, an IAM framework can make it easier to enforce policies regarding user authentication, validation, and privileges and address issues regarding privilege creep.
- IAM systems help companies better comply with government regulations by allowing them to show corporate information is not being misused. Companies can also demonstrate that any data needed for auditing can be made available on demand.

IAM solutions approach

Businesses need to identify who within the organization will lead in developing, enacting, and enforcing identity and access policies.

IAM impacts every department and every type of user (employee, contractor, partner, supplier, customer, etc.), so the IAM team must comprise a mix of corporate functions.

Organisations need to follow the right approach to implement IAM. Let’s discuss that in the next few slides.

Steps for building an effective IAM architecture

- Make a list of usage, including applications, services, components, and other elements users will interact with. This list will help validate that usage assumptions are correct and will be instrumental in selecting the features needed from an IAM product or service.

- Understand how the organization's environments, such as cloud-based applications and on-premises applications, link together. These systems might need a specific type of federation (Security Assertion Markup Language OpenID Connect, for instance).

Steps for building an effective IAM architecture

- Know the specific areas of IAM most important to the business. Answering the following questions will help:
  - Is multifactor authentication needed?
  - Do customers and employees need to be supported in the same system?
  - Are automated provisioning and de-provisioning required?
  - What standards need to be supported?

Implementations should maintain documentation to better define expectations and responsibilities for IAM success. Businesses should also centralize security and critical systems around identity. Perhaps most importantly, organizations should create a process for evaluating the efficacy of current IAM controls.

IAM risks

- It is important to collect and keep only important Biometric data. Organizations should know what biometric data they have, what they need, how to get rid of what they don't require, and how and where data is stored.

- Cloud-based IAM can be of concern when the provisioning and de-provisioning of user accounts aren't handled correctly if there are too many vulnerable inactive assigned user accounts, and if there is sprawl in admin accounts. Organizations must ensure lifecycle control over all aspects of cloud-based IAM to prevent malicious actors from accessing user identities and passwords.

Future of IAM Implementations

- The move to the cloud, the adoption of microservices architectures, the digitalization of the modern world, and the resulting growth in cyber threats continue to expand the use cases for IAM.
- *“To meet these new challenges, IT leaders must evolve their IAM systems,”* says Mary Ruddy, research vice president at Gartner.
- Here are four ways to evolve that
  - Integrate more closely with security and fraud systems.
  - Support higher levels of automation and communication between IAM modules.
  - Incorporate a development security operations (DevSecOps) approach.
  - Implement customer data management policies that respect customer consent and preferences more.

Ways to improve IAM

Integrate more closely with security and fraud systems. Compromised identity credentials continue to be a major element in data breaches, and the number of these breaches, including identity-related fraud (such as account takeovers), is growing.

Incorporate a development security operations (DevSecOps) approach. This requires a change in organizational mindset and is especially important for organizations developing their own applications and services.

Implement customer data management policies that respect customer consent and preferences more. This is necessary to meet new and expanding privacy regulations and evolving customer expectations.

Decentralized identity

The number of identities for people, things, services, and robotic process automation bots keeps growing, and the walls between identity domains are blurring IAM architecture.

Blockchain-enabled and decentralized identities are forcing IAM systems to allow users to create, prove (via trusted third parties), and register their identity and related relationship identifiers to utilize digital services. For organizations, this will reduce their costs and operational risks by eliminating the need for replicated identity repositories and data

Next-generation adaptive access services

One of the most pronounced trends in IAM today is the use of analytics.

“Whereas traditional adaptive authentication was rule-based, the next generation of adaptive access services combines rules with machine learning and advanced analytics; Rules are useful but limiting. You may not have thought of all possible scenarios,” says Paul Rabinovich, senior director at Gartner.

For example, unsupervised learning is good at anomaly detection. An organization can establish a baseline for a user or a group of “similar” users, and it can detect that today the user is behaving differently and take corrective action.

Privileged access management (PAM)

“PAM is all about securing the keys to your kingdom; it is one of the most critical security controls to implement,” says Gartner senior director Felix Gaehtgens.

Data breaches resulting from privileged account compromise are a top concern with IAM in the cloud. Privileged access management (PAM) solutions, including PAM analytics that monitor for high-risk situations, are available to combat this concern. PAM solutions are required for the platform as a service (PaaS) and infrastructure as a service (IaaS), which are rising as organizations build agile, intelligent IAM platforms.