Defa3
Cyber Security

How Identification, Authentication & Authorization are used

How Identification, Authentication & Authorization are used

Defa3
Cyber Security

Identification

Identification is the process of claiming an identity within a system.

- **What it does:** Establishes who you claim to be
- **Examples:** Username, email address, account number, employee ID
- **Purpose:** Provides a way for the system to recognize you as a specific entity

sales@defa3.com

How Identification, Authentication & Authorization are used

Defa3
Cyber Security

Authentication

Authentication verifies that you are who you claim to be.

What it does: Validates your identity claim

Methods:

- Something you know (password, PIN, security questions)
- Something you have (smart card, security token, phone)
- Something you are (fingerprint, retina scan, facial recognition)
- Somewhere you are (location-based)

Purpose: Prevents impersonation and unauthorized access

sales@defa3.com

How Identification, Authentication & Authorization are used

Defa3
Cyber Security

Authorization

Authorization determines what an authenticated user is allowed to do.

- **What it does:** Controls access to resources and actions
- **Implementation:** Access control lists, role-based permissions, attribute-based access control
- **Purpose:** Ensures users can only access what they're permitted to

sales@defa3.com

How Identification, Authentication & Authorization are used

How They Work Together

1. A user claims an identity (identification)
2. The system verifies this claim (authentication)
3. Once verified, the system determines what the user can access (authorization)

Think of it like entering a secure building: showing your ID badge (identification), having security verify it's really you (authentication), and then being allowed to access only certain floors or rooms (authorization).

Defa3
Cyber Security

www.defa3.com

sales@defa3.com

+97145470666

Found this useful? Follow us!