**🔐 Authentication (AuthN) — *"Who are you?"***

**Definition:**  
Authentication is the process of verifying the **identity** of a user, system, or service.

**Example:**  
When you log in to your Gmail with a username and password, Google checks your credentials. If they match, you’re authenticated.

**Methods:**

* Username & Password
* OAuth (e.g., "Sign in with Google")
* Multi-Factor Authentication (MFA)
* Biometric (fingerprint, face ID)
* Service account key in cloud (for non-human users)

**In GCP:**

* IAM authenticates users using Google credentials.
* Service accounts authenticate apps and services.

**✅ Authorization (AuthZ) — *"What can you do?"***

**Definition:**  
Authorization determines **what actions** an authenticated user or service can perform (access control).

**Example:**  
After you log in to Gmail (authenticated), can you read only your own emails or someone else’s? That’s authorization.

**Mechanisms:**

* IAM Roles & Permissions
* ACLs (Access Control Lists)
* Policies (like GCP IAM policy bindings)

**In GCP:**

* IAM roles (Viewer, Editor, Owner, Custom) authorize what a user/service account can do.
* For example:
  + roles/storage.admin lets you manage Cloud Storage.
  + roles/viewer only allows read access.

**👥 Real-World Analogy:**

* **Authentication**: Showing your ID card at the building entrance.
* **Authorization**: Security guard checks if your ID grants access to the server room.

**💡 Summary Table:**

| **Feature** | **Authentication** | **Authorization** |
| --- | --- | --- |
| Question | Who are you? | What are you allowed to do? |
| Purpose | Validate identity | Grant or deny access rights |
| Happens first? | ✅ Yes | 🚫 Only after successful authentication |
| Involves | Credentials (passwords, keys, MFA) | Policies, roles, permissions |
| Example in GCP | User logs in with Google account | User has roles/compute.admin on a project |