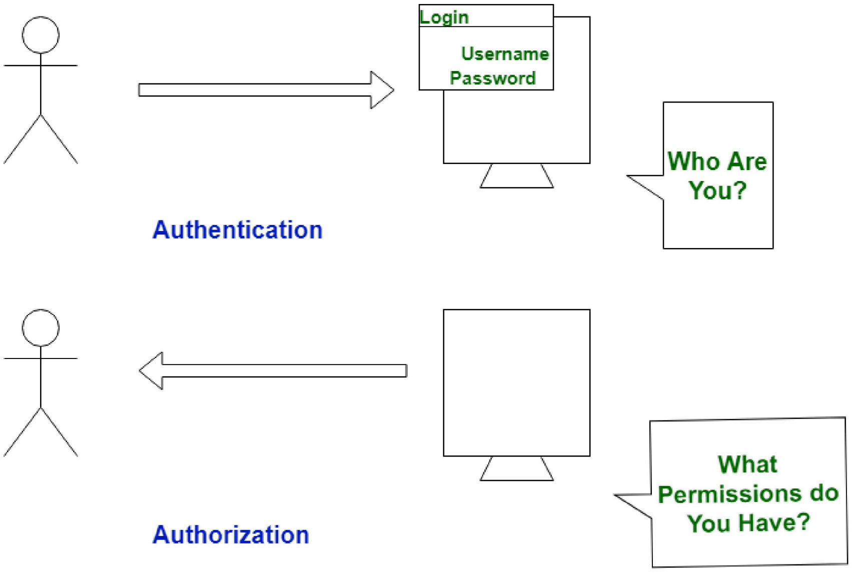
Difference between Authentication and Authorization

Difficulty Level : Easy • Last Updated : 01 Sep, 2022

Both Authentication and Authorization area units are utilized in respect of knowledge security that permits the safety of an automatic data system. Each area unit terribly crucial topics usually related to the online as key items of its service infrastructure. However, each of the terms area units is completely different with altogether different ideas. whereas indeed, they're usually employed in an equivalent context with an equivalent tool, they're utterly distinct from one another. In the authentication process, the identity of users is checked for providing the access to the system. While in the authorization process, a person's or user's authorities are checked for accessing the resources. Authentication is done before the authorization process, whereas the authorization process is done after the authentication process.



Authentication	Authorization
In the authentication process, the identity of users are checked for providing the access to the system.	While in authorization process, a the person’s or user’s authorities are checked for accessing the resources.
In the authentication process, users or persons are verified.	While in this process, users or persons are validated.
It is done before the authorization process.	While this process is done after the authentication process.
It needs usually the user’s login details.	While it needs the user’s privilege or security levels.
Authentication determines whether the person is user or not.	While it determines **What permission does the user have?**
Generally, transmit information through an ID Token.	Generally, transmit information through an Access Token.
The OpenID Connect (OIDC) protocol is an authentication protocol that is generally in charge of user authentication process.	The OAuth 2.0 protocol governs the overall system of user authorization process.
Popular Authentication Techniques-	Popular Authorization Techniques-
	• Role-Based Access Controls (RBAC) • SON web token (JWT) Authorization • SAML Authorization • OpenID Authorization • OAuth 2.0 Authorization

Authentication	Authorization
- Password-Based Authentication - Passwordless Authentication - 2FA/MFA (Two-Factor Authentication / Multi-Factor Authentication) - Single sign-on (SSO) - Social authentication	
The authentication credentials can be changed in part as and when required by the user.	The authorization permissions cannot be changed by user as these are granted by the owner of the system and only he/she has the access to change it.
The user authentication is visible at user end.	The user authorization is not visible at the user end.
The user authentication is identified with username, password, face recognition, retina scan, fingerprints, etc.	The user authorization is carried out through the access rights to resources by using roles that have been pre-defined.
Example: Employees in a company are required to authenticate through the network before accessing their company email.	**Example:** After an employee successfully authenticates, the system determines what information the employees are allowed to access.