Welcome to Authentication and Authorization in Node.js

Skills Network

After you are finished reading this document, you will be able to:

- Define authentication.
- Explain session-based, token-based, and passwordless authentication.
- Compare and contrast different types of authentications, including session-based, token-based, and passwordless.

The authentication process confirms a user's identity using credentials by validating who they claim to be. Authentication assures an application's security by guaranteeing that only those with valid credentials can access the system. Authentication is the responsibility of an application's backend.

Three popular authentication methods in Node.js include:

1. Session-based
2. Token-based
3. Passwordless

Let's explain a little bit about each of these methods and compare them.

Session-based

Session-based authentication is the oldest form of authentication technology. Typically, the flow of a session is as follows:

1. The user uses their credentials to log in.
2. The login credentials are verified against the credentials in a database. The database is responsible for storing which resources can be accessed based on the session ID.
3. The server creates a session with a session ID that is a unique encrypted string. The session ID is stored in the database.
4. The session ID is also stored in the browser as a cookie.
5. When the user logs out or a specified amount of time has passed, the session ID is destroyed on both the browser and the database.

Token-based

Token-based security entails two parts: authentication and authorization. Authentication is the process of providing credentials and obtaining a token that proves the user's credentials. Authorization refers to the process of using that token so the resource server knows which resources the user should have access to.

Token-based Authentication

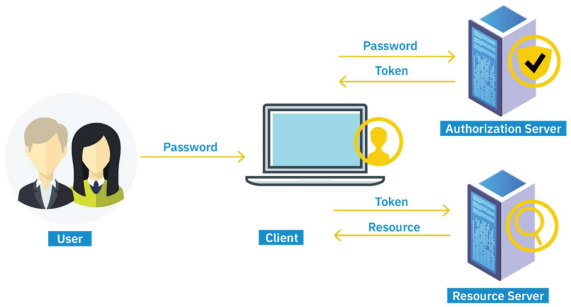
Token-based authentication uses access tokens to validate users. An access token is a small piece of code that contains information about the user, their permissions, groups, and expirations that get passed from a server to the client. An ID token is an artifact that proves that the user has been authenticated.

The token contains three parts, the header, the payload, and the signature. The header contains information about the type of token and the algorithm used to create it. The payload contains user attributes, called claims, such as permissions, groups, and expirations. The signature verifies the token's integrity, meaning that the token hasn't changed during transit. A JSON web token, pronounced "jot" but spelled JWT, is an internet standard for creating encrypted payload data in JSON format.

A user's browser makes a call to an authentication server and gets access to a web application. The authentication server then passes back an ID token which is stored by the client as an encrypted cookie. The ID token is then passed to the app on the web server as proof that the user has been authenticated.

Token-based Authorization

This flowchart shows the workflow of a token through the authorization process.



The authorization process gets executed when the web application wants to access a resource, for example, an API that is protected from unauthorized access. The user authenticates against the Authorization server. The Authorization server creates an access token (note that the ID token and access token are two separate objects) and sends the access token back to the client, where the access token is stored. Then when the user makes requests or resources, the token is passed to the resource, also called an API server. The token gets passed with every HTTP request. The token contains embedded information about the user's permissions without the need to access those permissions from the authorization server. Even if the token is stolen, the hacker doesn't have access to the user's credentials because the token is encrypted.

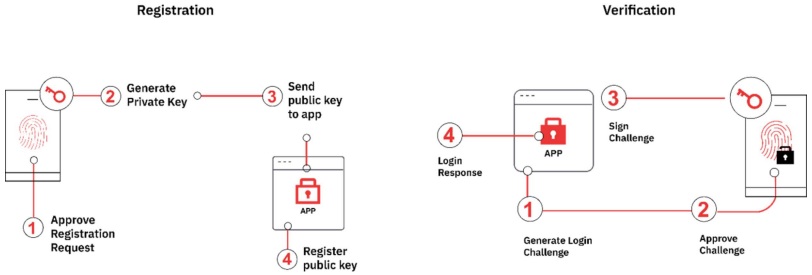
Passwordless

With passwordless authentication, the user does not need login credentials, but rather, they gain access to the system by demonstrating they possess a factor that proves their identity. Common factors include biometrics such as a fingerprint, a "magic link" sent to their email address, or a one-time passcode sent to a mobile device. Password recovery systems now commonly use passwordless authentication.

Passwordless authentication is achieved using Public Key and Private Key Encryption. In this method, when a user registers for the app, the user's device generates a private key/public key pair that utilizes a factor that proves their identity, as noted above.

The public key is used to encrypt messages, and the private key is used to decrypt them. The private key is stored on the user's device, and the public key is stored with the application and registered with a registration service.

Anyone may access the public key, but the private key is only known to the client. When the user signs into the application, the application generates a login challenge, such as requesting biometrics, sending a "magic link," or sending a special code via SMS, encrypting it with the public key. The private key allows the message to be decrypted. The app then verifies the sign-in challenge and accepts the response to authorize the user.



In this reading, you learned that:

- Authentication is the process of confirming a user's identity using credentials by validating who they claim to be.
- Session-based authentication uses credentials to create a session ID stored in a database and the client's browser. When the user logs out, the session ID is destroyed.
- Token-based authentication uses access tokens, often JWTs, that get passed between server and client with the data that is passed between the two.
- Passwordless authentication uses public/private key pairs to encrypt and decrypt data passed between client and server without the need for a password.