A JSON Web Token (JWT) is a JSON object defined in RFC 7519 as a secure way to represent a set of information between two parties (such as a client and a server).

Explanation:

• JWT is a method for transmitting data securely, where the data is either encrypted or signed to ensure its integrity and authenticity.

• The token consists of three main parts:

1. Header: Contains information about the type of token (JWT) and the encryption algorithm used.

2. Payload: Contains the data or claims, such as the username or user permissions.

3. Signature: Verifies the integrity of the data using a secret key or a public certificate.

Purpose:

To provide a secure and efficient way of exchanging information between two parties while ensuring that the data cannot be tampered with during transmission.