

10.9. Ensuring Endpoint Authenticity

10.9. Ensuring Endpoint Authenticity

[RFC2818] [RFC6125] TLS

10.9. Ensuring Endpoint Authenticity

In order to prevent man-in-the-middle attacks, the authorization server MUST require the use of TLS with server authentication as defined by [RFC2818] for any request sent to the authorization and token endpoints. The client MUST validate the authorization server's TLS certificate as defined by [RFC6125] and in accordance with its requirements for server identity authentication.