Why is the Server's Root Certificate so important?

In the context of SSL/TLS handshake, a root certificate is a digital certificate that identifies a trusted Certificate Authority (CA) and is used to verify the identity of a server during the SSL/TLS handshake process.

When a client attempts to establish an SSL/TLS connection with a server, the server sends its SSL/TLS certificate to the client. The client then verifies the server's certificate by checking its signature using the public key of the CA that issued the certificate. To establish trust, the client must have the CA's root certificate in its trusted root store.

If the client does not have the root certificate for the CA that issued the server's SSL/TLS certificate in its trusted root store, it will return a "certificate not found" error during the handshake process. This means that the client cannot verify the identity of the server and cannot establish a secure connection.

To resolve this issue, the client must obtain the root certificate for the CA that issued the server's SSL/TLS certificate and add it to its trusted root store. The client can obtain the root certificate by downloading it from the CA's website or by contacting the CA directly. Once the root certificate is added to the trusted root store, the client should be able to establish a secure connection with the server.