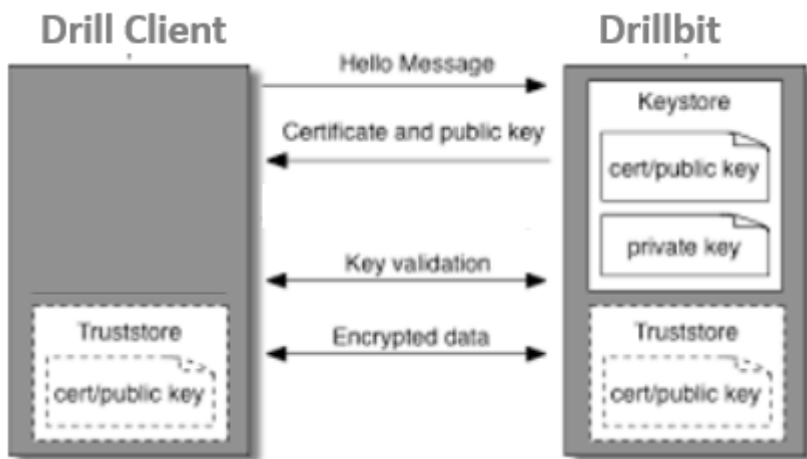


Using SSL/TLS for Encryption

You can enable SSL for Drill in a secure or unsecure MapR cluster. SSL (Secure Sockets Layer), more recently called TLS, is a security mechanism that encrypts data passed between the Drill client and Drillbit (server). SSL also provides one-way authentication through which the Drill client verifies the identity of the Drillbit.

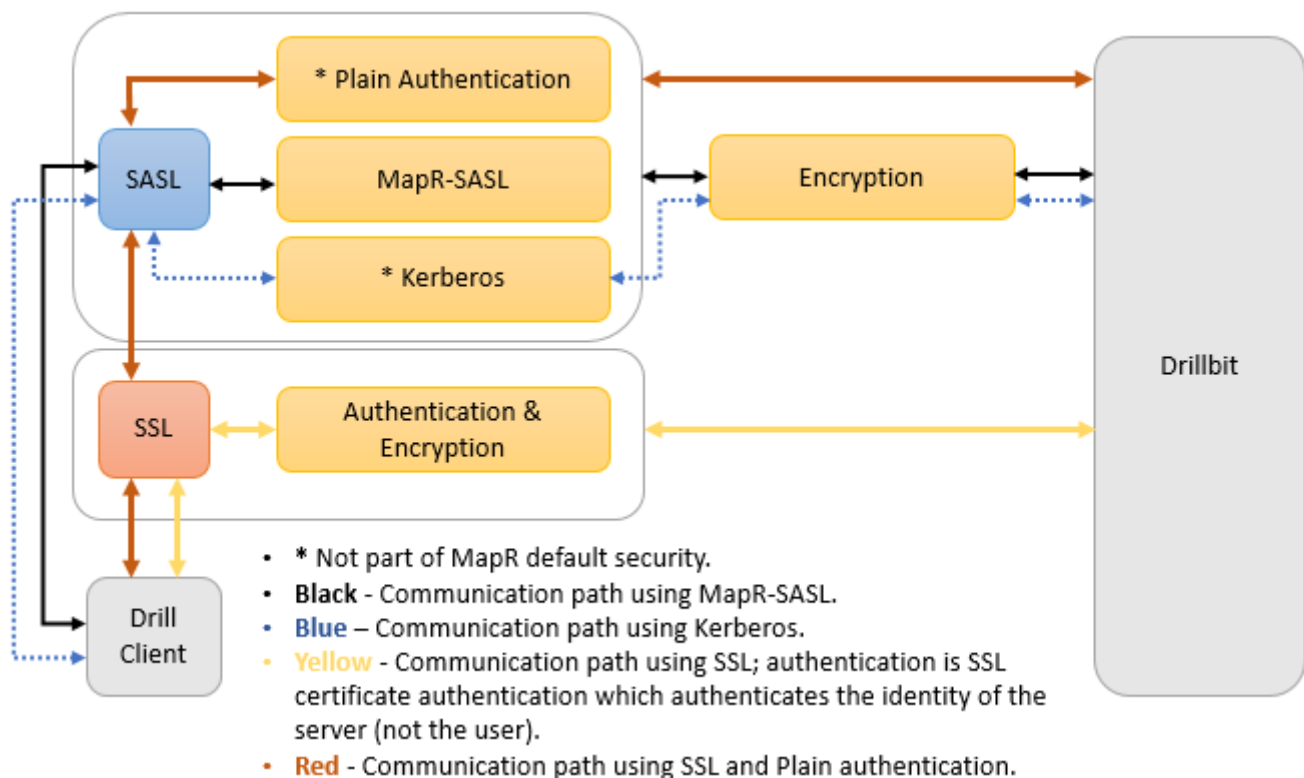
Authentication occurs during the SSL handshake when the Drillbit (server) presents its certificate to the client, and the client checks if the certificate exists in its truststore or if the certificate is signed by a trusted CA (Certificate Authority) that exists in its truststore.


The following diagram depicts the communication between the Drill client and the Drillbit (server):



The SASL feature in Drill provides authentication and an option to encrypt data, however the encryption feature is not available when using Plain authentication. If you need to use Plain authentication (certain BI tools only use Plain authentication), you can enable SSL to encrypt data. You can have both SASL and SSL enabled when using Plain authentication only. For any other scenario, using SSL and SASL encryption together is strongly discouraged.

The following diagram depicts the SSL communication paths between the Drill client and Drillbit (server), including the scenario where Plain authentication is used:



 **Note:** The REST API supports HTTPS. SSL is not supported for communication between Drillbits.

The following sections provide information about how to use certificates in secure and unsecure MapR clusters, enabling and configuring SSL, connection parameters, and common SSL issues.