Encryption of data in transit 27

Last Updated: 2024-10-30

Db2® uses the Transport Layer Security (TLS) protocol to securely transmit data between servers and clients. TLS technology uses both asymmetric cryptography (for example, public key encryption) and symmetric cryptography to make this work. 27

You can use TLS to protect data in transit on all networks that use TCP/IP. In other words, a TLS connection is a secured TCP/IP connection.

Public key encryption for server authentication

TLS uses public-key algorithms to exchange encryption key information and digital certificate information. Public key encryption is used to ensure that a client can trust the certificate that is used by a server.

Public key cryptography uses two different encryption keys during a TLS session:
– A public key to encrypt data.
– An associated private key to decrypt it.

With public-key cryptography, the public key is not secret, but the messages it encrypts can be decrypted only by using it's associated private key. The private key must be securely stored in a file that is called a keystore.
Public-key algorithms alone do not ensure secure communication, you also need to verify the identity of whoever is communicating with you. To do this authentication, TLS uses digital certificates.

Distribution and use of digital certificates

To facilitate encryption of data in a Db2 environment, the following tasks need to happen for each Db2 server within your organization:

1. A member of your organization uses IBM Global Security Kit (GSKit) to create a public and private key pair.
2. The public key is sent to a certificate authority (CA) where a certificate is created and signed.
3. The server's certificate (which includes the server's public key) is distributed to all of the Db2 clients (and servers) within your organization for storage within their local keystores.

Once the certificates for each server have been distributed within your network, all of the parts needed to make TLS work are in place.

Before data is encrypted for transmission between Db2 nodes in your network, a TLS handshake occurs. This enables a client to check the validity of a server's certificate and, if the certificate is trusted, create a session key by using the server's public key. The session key is used to encrypt data traveling between the client and server for the duration of the connection.