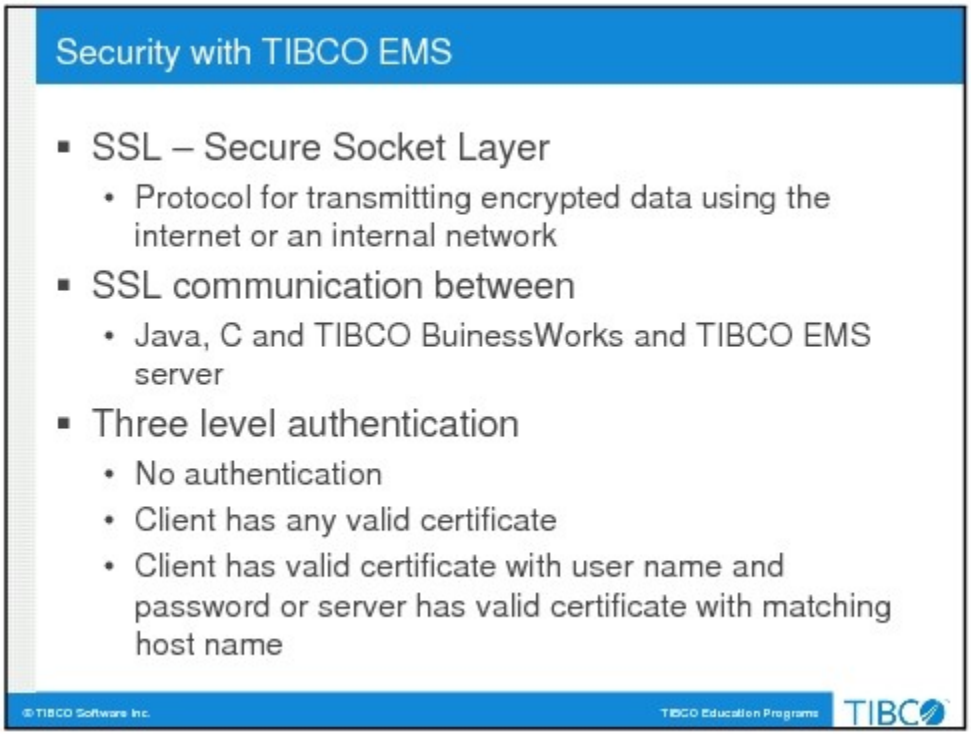

Security with TIBCO EMS

SSL is a protocol for transmitting encrypted data. SSL uses digital certificates and private keys to encrypt data. Some supported digital certificate formats:

- PEM
- DER
- PKCS#7
- PKCS#12
- Java Key Store
- Entrust Store.

Some supported private key formats:

- PEM
- DER
- PKCS#8
- PKCS#12.

EMS Server and C clients support OpenSSL for SSL. Java clients use JSSE(from Sun JavaSoft) or SSL implementation from Entrust.

Security is a key advantage of TIBCO EMS, providing facilities that support security requirements at both the client and server levels. Security is better implemented in EMS (as opposed to RV) since EMS has a centralized infrastructure. SSL is used between JMS clients and server as well as between routed and FT servers.

TIBCO EMS supports three levels of authentication:

- **No authentication**: When you enable SSL in tibemsd.conf, you need to provide digital certificates against ssl_server_identity and private keys against ssl_server_key and optionally password for the

private key. Last two parameters are optional if certificate contains private key with no password for the key. In this level when any client connects to EMS server in SSL mode, EMS supplies digital certificates, but client can ignore the certificate and can trust any server. NOTE:- For TIBCO BusinessWorks client, it's mandatory to create Keystore Resource with digital certificates in TIBCO Business Studio.

- **Client has any valid certificate**: If you have enabled client authorization in tibemsd.conf by setting parameters ssl_require_client_cert=yes and by specifying certificate using ssl_server_trusted e.g. ssl_server_trusted= /opt/tibco/soa/ems/8.2/samples/certs//client_root.cert.pem, then client has to supply digital certificate when making connection to TIBCO EMS server in SSL mode.
- **Client has valid certificate with user name and password**: This is similar to second level, but it also includes user name and password along with certificates from clients. For server, host name matching with certificate entry can be enabled.