**Does HTTPS configured without certificate?** No. According to the RFC 2818 specification, a certificate is needed as it's the way a server identifies itself to the client. The certificate doesn't need to be valid, i.e. the certificate doesn't have to be issued and signed by a CA that the browser trusts by default. Self Signed Certificate is enough too.  
===========================================================

When SSL is used, the target (the server) always authenticates itself to the initiator (the client). Optionally, if the target requests it, the initiator can authenticate itself to the target. Encryption scrambles the data that is transmitted. An SSL connection begins with a handshake during which the applications exchange digital certificates, agree on the encryption algorithms to be used, and generate the encryption keys to be used for the remainder of the session.

SSL provides the following security features:

* Server authentication - WebLogic Server uses its digital certificate, issued by a trusted certificate authority, to authenticate to clients. SSL minimally requires the server to authenticate to the client using its digital certificate. If the client is not required to present a digital certificate, the connection type is called one-way SSL authentication.
* Client Identity Verification - Optionally, clients might be required to present their digital certificates to WebLogic Server. WebLogic Server then verifies that the digital certificate was issued by a trusted certificate authority and establishes the SSL connection. An SSL connection is not established if the digital certificate is not presented and verified. This type of connection is called two-way SSL authentication, a form of mutual authentication.
* Confidentiality - All client requests and server responses are encrypted to maintain the confidentiality of data exchanged over the network.
* Data Integrity - Each SSL message contains a message digest computed from the original data. On the receiving end, a new digest is computed from the de-crypted data and then compared with the digest that came with the message. If the data is altered, the digests don't match and tampering is detected.