1.5. (updated) The very first step in this protocol requires that both communicating entities support TLS. Therefore, when A tries to communicate with B, the first exchange of messages between these two entities would comprise the former requesting a TLS session to be established. If the latter does not provide a relevant response, which requires B to send its valid digital certificate upon receiving a half symmetric key, A can suspect an impersonator and terminate the connection. This initial step is called the "hand-shake" and it is during this phase that a unique symmetric session key is generated by A upon receiving the other half key from B and vice-versa. Thus, all the data during the entire session is encrypted using this key. Furthermore, before the transmission of any data, A will authenticate itself to B with a single sign-on using the third party server s, which is the trusted identity provider of the former. The potential drawback with TLS is verifying the actual identity of A, since the latter does not have a digital certificate that it can authenticate itself on. However, the TLS channel itself is secure (even more secure in this case) enough to provide communication that is not compromised between the two entities, thus, preventing an intruder to perform an attack when the session is established. Moreover, for any “witness” *X,* with TLS the “request” service provider can have a secure communication channel to transmit and receive data from the former.