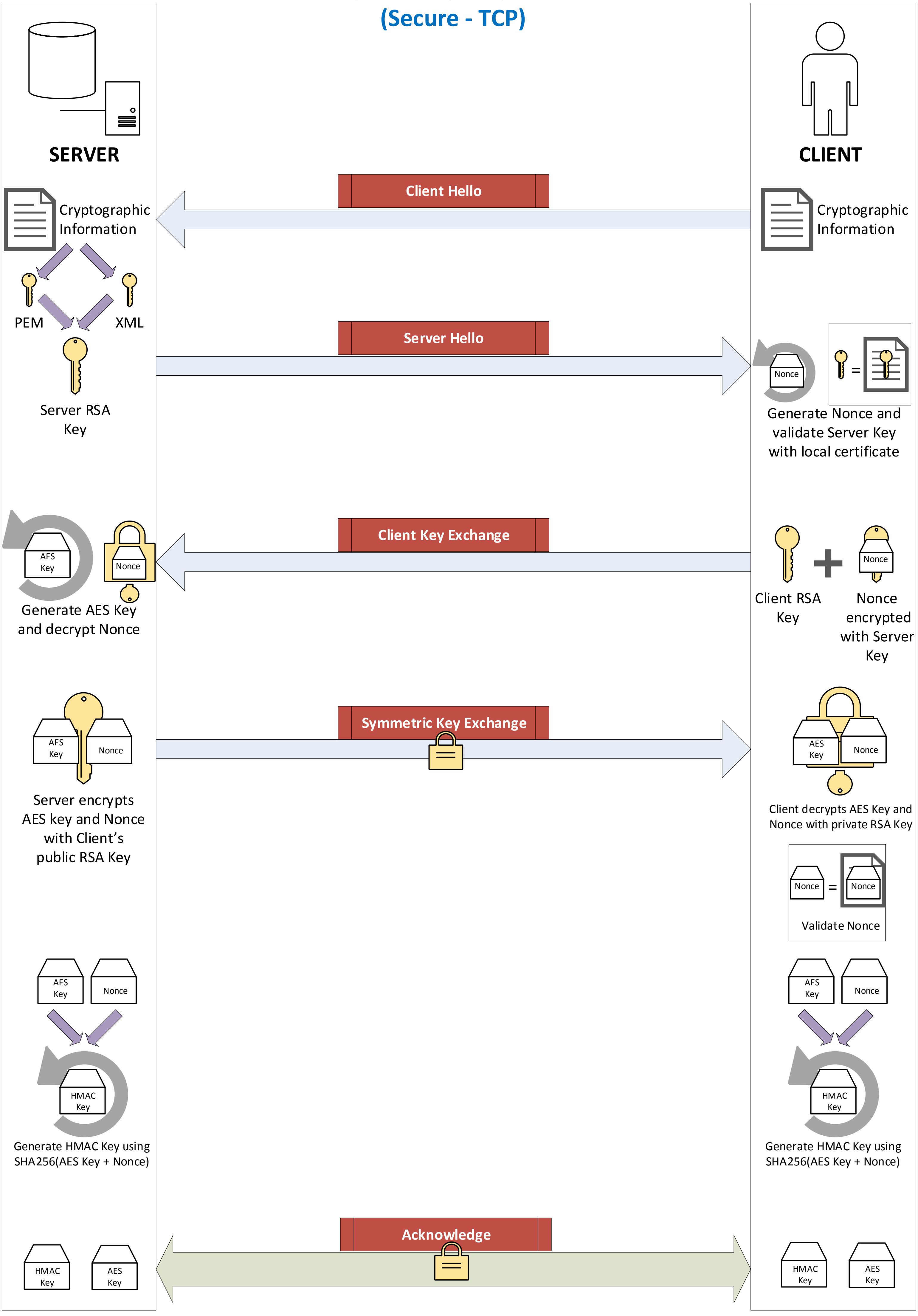
Key Exchange Algorithm
(Secure - TCP)



SERVER
CLIENT
Client Hello
Cryptographic Information
PEM
XML
Server RSA Key
Cryptographic Information
Server Hello
Nonce
=
Generate Nonce and validate Server Key with local certificate
Client Key Exchange
AES Key
Nonce
Generate AES Key and decrypt Nonce
Client RSA Key
Nonce
Nonce encrypted with Server Key
Symmetric Key Exchange
AES Key
Nonce
Server encrypts AES key and Nonce with Client’s public RSA Key
AES Key
Nonce
Client decrypts AES Key and Nonce with private RSA Key
Nonce
=
Nonce
Validate Nonce
AES Key
Nonce
HMAC Key
Generate HMAC Key using SHA256(AES Key + Nonce)
AES Key
Nonce
HMAC Key
Generate HMAC Key using SHA256(AES Key + Nonce)
Acknowledge
HMAC Key
AES Key
HMAC Key
AES Key

TECHNICAL INFORMATION

- 4096 Bit RSA with PKCS1 cipher and OAEP padding
- 256 Bit AES Cipher Block Chaining (CBC) + 16 Byte IV + 16 Byte Blocksize + SHA256
- UTF8 Encoding
- Nonce: SHA256 Hashed cryptographic random Integer (range 0 – (2^63 – 1))
- HMAC: SHA256(HMAC_KEY[32:] + SHA256(HMAC_KEY[:32] + ENCRYPTED_MESSAGE))