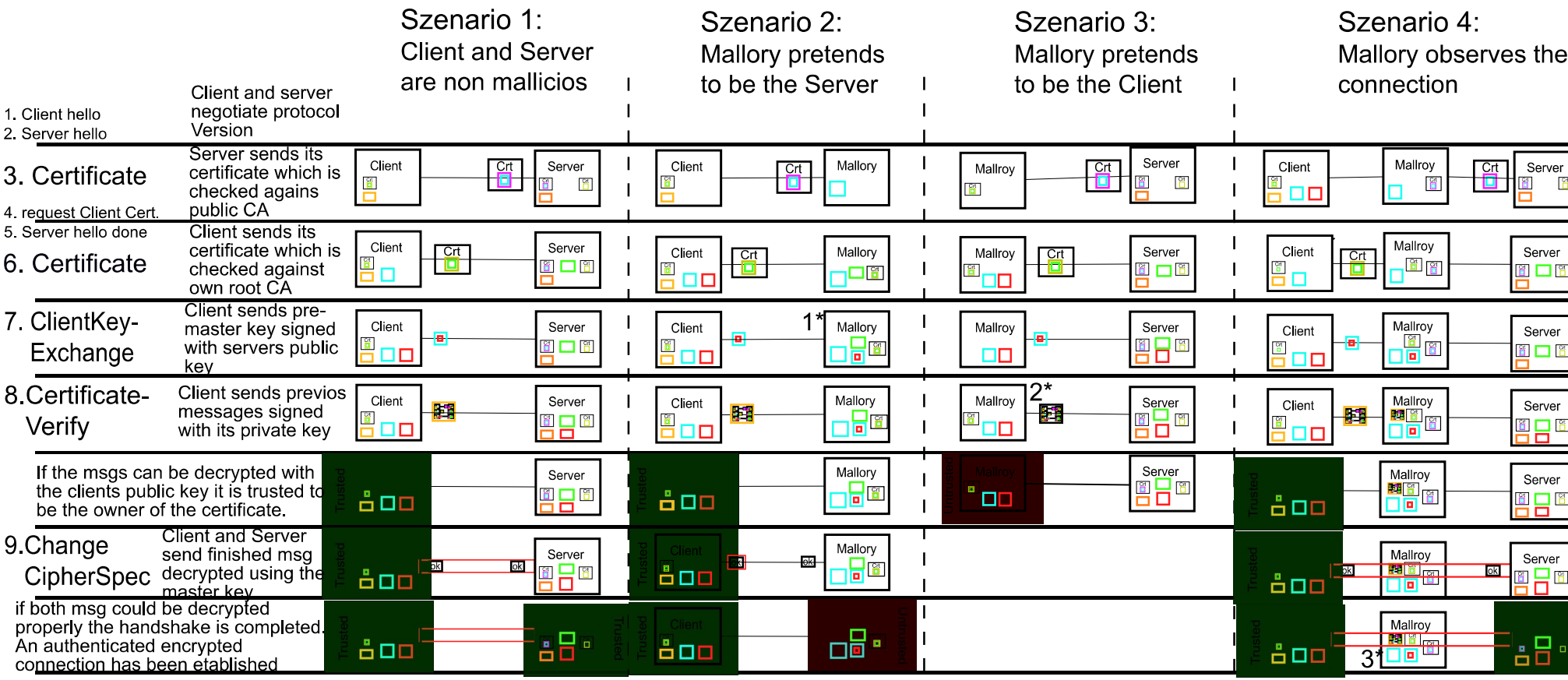
Node ECP Server - Security Model (SSL)

Filename: SM-0200.svg
Project (in-dev): NodeECPtest1
Snapshot: alpha 0.2.4-0200
Content Type: Security Model
Date: Jan 31 2017
Author: dsalex1

Legend

Https Client: Client
Https Server: Server
Attacker: Mallory
Symetric Key:
Server public Key:
Server private Key:

Client cert.: Crt
Cert signed by trus. CA: Crt
Selfsigned Root CA cert.: Crt
Client public key:
Client private key:



1*: Due to the llack of the Server's private key the encrypted pre-master key couldn't be decrypted

2*: Due to the lack of the Client's private key the Certificate Verify msg couldn't be signed properly

3*: All information ratherd is non sense nor useful to hijack the connection