**Threat summary for MMN15 protocol only**

Threat: Man in The Middle

Threat description: A man-in-the-middle attack is a type of eavesdropping attack, where attackers interrupt an existing conversation or data transfer. After inserting themselves in the "middle" of the transfer, the attackers pretend to be both legitimate participants. This enables an attacker to intercept information and data from either party while also sending malicious links or other information to both legitimate participants in a way that might not be detected until it is too late.

Protocol threat description : The man in the middle can listen to an on going conversation between the client and the server and obtain the client ID, from now on he can communicate with the server with the ID he obtained, thus he can perform any action the original client would do.  
While the man in the middle listening and joining the data transferring process between the client and the server (with the client ID he obtained) he can obtain the public key from the client, generate his own RSA public / private keys, and send his public key to the server, the server will generate AES key and encrypt it with the MITM public key, then send it to the client, thus the MITM can decrypt the AES key with his private key, and when the original client will send a file, he can decrypt it with the decrypted AES key, thus leading to very dangerous actions such as changing the file contents to malicious links / code or read sensitive information such as credit card number / password / etc

Protocol threat mitigation: client ID validation / advanced encryption / SSL technology