For all PPTM Adversary A given two messages m_0, m_1 and and encryption c of one random message m_b between the two, then should not be able to figure out original message. A can also query any other ciphertext other than c to get its message.

$$pr(A(c) == b; st\ c \notin Q) = negl(n)$$

Proof:

Assuming our MAC is secure and enc scheme is CPA secure our construction will only return decryption if decrypted message and tag are valid message tag,

since we proved the security of mac.

$$Pr[Vrfy(\langle m, t \rangle] = 1 | m \notin Q] = negl(n)$$

Hence this hides ciphertext server,

$\Pr(\text{Valid Query}) = \text{negl}(n)$
and since our encryption scheme is also CPA secure any CPA attack also donot work

Hence
$\Pr(A(C) == b; \text{ s.t } C \notin Q) = \text{negl}(n)$

Hence proved.