Homework Problems : Public Key Authentication

Recall RSA Full-Domain Hash (RSA-FDH) signature scheme described in the lecture, and

1. Prove that RSA-FDH is Existentially Unforgeable against a Known Message Attack (KMA).
2. Prove that RSA-FDH is Existentially Unforgeable against a Chosen Message Attack (CMA).

In each of the above proofs, an outline of the proof-idea will be sufficient.
Rigorous mathematical proofs are not required, but will be appreciated.