Use the PRF to build a secure MAC.

A MAC is Message Authentication Codes. The components of the authentication protocol involves :

1. A key generation algorithm that returns a secret key ‘k’
2. A MAC generating algorithm that returns a tag for a given message ‘m’ where the tag ‘t’ = $MAC_k(m)$
3. A verification algorithm that returns a bit b = $Verify_k(m_1, t_1)$, given a message m_1 and a tag t_1.
4. If the message is not modified then with high probability, the value of b is true otherwise false.

A MAC(Gen, MAC, Verify) is secure if for all probabilistic polynomial-time adversaries A:

$Pr[MAC\text{-}Game(n) = 1] <= negl(n)$

If F is a PRF, then the below mentioned scheme gives a secure fixed length MAC :

1. $Gen(1^n)$ chooses k to be a random n-bit string
2. $MAC_k(m) = F_k(m) = t$ (the tag)
3. $Verify_k(m, t) = Accept$, iff $t = F_k(m)$