# H-MAC

H-Mac is Message Authentication Code which is a industry standard as CBC-MAC id deemed to be slow.

H-MAC is defined as:

**(Gen,h):** A fixed length hash function.

**(Gen,H):** Hash function after applying MD transform to (Gen,h)

**Fixed constants:** IV (Initialization Vector), opad and ipad

H-Mac tag = $H^s_{IV}( k \hat{} opad || H^s_{IV}((k \hat{} ipad) || m))$