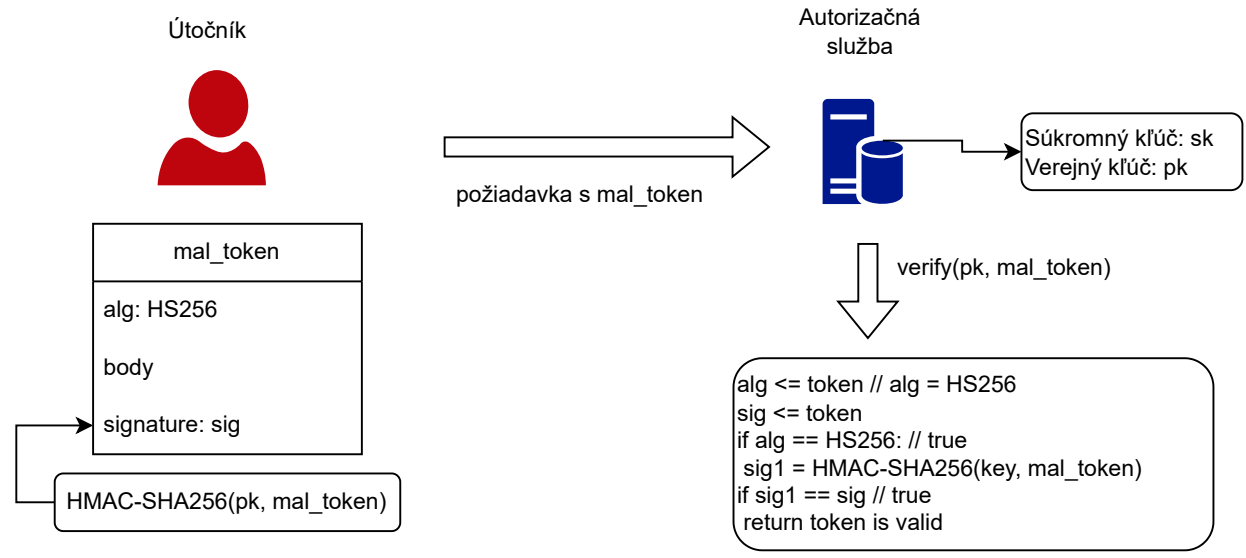
Útočník
Autorizačná služba
požiadavka s mal_token
Súkromný kľúč: sk
Verejný kľúč: pk
mal_token
alg: HS256
body
signature: sig
HMAC-SHA256(pk, mal_token)
verify(pk, mal_token)
alg <= token // alg = HS256
sig <= token
if alg == HS256: // true
sig1 = HMAC-SHA256(key, mal_token)
if sig1 == sig // true
return token is valid