The CRLs and OCSP status responses shall be digitally signed to support authentication and integrity using a key size and hash algorithm that satisfy the requirements for signing PIV information, as specified in Table 2, and that are at least as large as the key size and hash algorithm used to sign the certificate.

CRLs and OCSP messages rely on object identifiers to specify which signature algorithm was used to generate the digital signature. The object identifiers specified in Table 3 must be used in CRLs and OCSP messages to identify the signature algorithm.