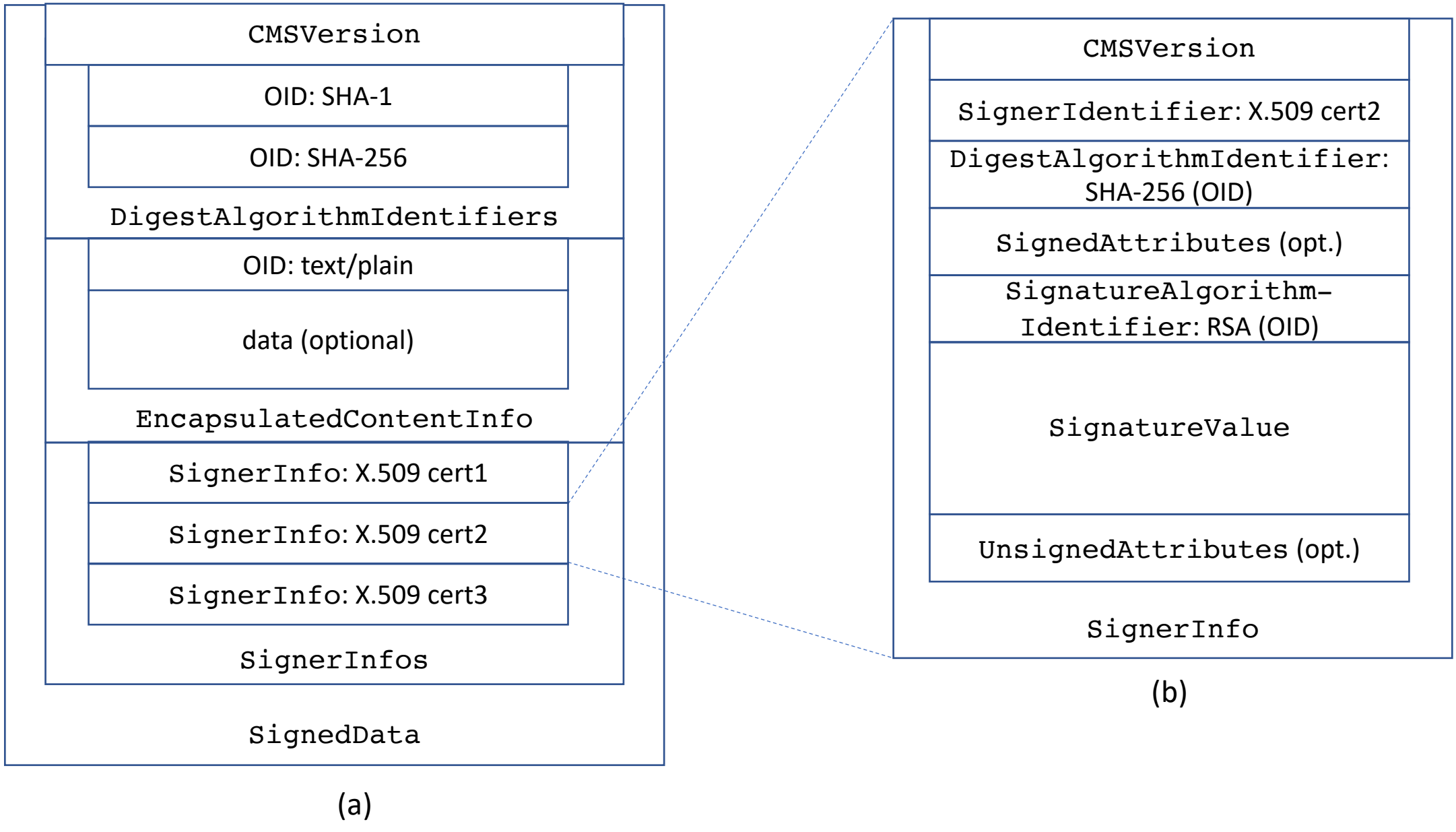
CMSVersion
OID: SHA-1
OID: SHA-256
DigestAlgorithmIdentifiers
OID: text/plain
data (optional)
EncapsulatedContentInfo
SignerInfo: X.509 cert1
SignerInfo: X.509 cert2
SignerInfo: X.509 cert3
SignerInfos
SignedData
(a)
CMSVersion
SignerIdentifier: X.509 cert2
DigestAlgorithmIdentifier: SHA-256 (OID)
SignedAttributes (opt.)
SignatureAlgorithm-Identifier: RSA (OID)
SignatureValue
UnsignedAttributes (opt.)
SignerInfo
(b)