This is a proposal to support ECDSA by making the following changes to the NDN-TLV packet format spec for the [Signature type](http://named-data.net/doc/ndn-tlv/signature.html).

## SignatureType[¶](#signaturetype)

[add the following]

| **Value** | **Reference** | **Description** |
| --- | --- | --- |
| 3 | SignatureSha256WithEcdsa | Integrity and provenance protection using an ECDSA signature over a SHA-256 digest |

### SignatureSha256WithEcdsa[¶](#signaturesha256withrsa)

SignatureSha256WithEcdsa defines an ECDSA public key signature that is calculated over the SHA256 hash of the Name, MetaInfo, Content, and SignatureInfo TLVs. The signature algorithm is defined in [[RFC5753], Section 2.1](http://tools.ietf.org/html/rfc5753#section-2.1).

SignatureInfo ::= SIGNATURE-INFO-TYPE TLV-LENGTH  
 SIGNATURE-TYPE-TYPE TLV-LENGTH(=1) 2  
 KeyLocator  
  
 SignatureValue ::= SIGNATURE-VALUE-TYPE TLV-LENGTH  
 BYTE+(=ECDSA over SHA256{Name, MetaInfo, Content, SignatureInfo})

Note

The SignatureValue size depends on the private key length used during the signing process. (63 bytes for a 224 bit key).

This type of signature ensures strict provenance of a Data packet, provided that the signature verifies and signature issuer is authorized to sign the Data packet. The signature issuer is identified using the KeyLocator block in the SignatureInfo block of SignatureSha256WithEcdsa. A KeyLocatorDigest is defined over the DER encoding of the SubjectPublicKeyInfo for an EC key as defined by [RFC 5480](http://www.ietf.org/rfc/rfc5480.txt). See the KeyLocator section for more detail.