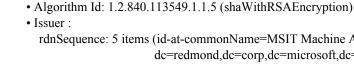## X.509 certificate

| Version |
| Certificate serial number |
| Certificate algorithm identifier for certificate issuer's signature |
| Issuer |
| Validity Period |
| Subject |

| Subject public-key information | Algorithm identifier |
| | Public-key value |

Optional {
| Issuer unique identifier |
| Subject unique identifier |
| Extension Fields |

| Certificate authority's digital signature |

- Version : v2
- Serial Number : 0x3599b31300010000d76f
- Algorithm Id: 1.2.840.113549.1.1.5 (shaWithRSAEncryption)
- Issuer :
  rdnSequence: 5 items (id-at-commonName=MSIT Machine Auth CA 2, dc=redmond,dc=corp,dc=microsoft,dc=com)
- Validity :
  notBefore : utcTime: 14-04-09 21:56:49 (UTC)
  notAfter : utcTime: 16-04-08 21:56:49 (UTC)
- Subject : rdnSequence: 1 item (id-at-commonName=*.pipe.skype.com)
- Subject Public Key Info :
  algorithm (rsaEncryption)
  subjectPublicKey: 3082010a0282010100965b89dc...
- Extension (id-ce-keyUsage) :
  Extension Id: 2.5.29.15 (id-ce-keyUsage)
  KeyUsage: b0 (digitalSignature, keyEncipherment, dataEncipherment)
- Signature: 44104b3b11cb672e0fbaafd455e...