

Dokumentpakken

Dokumentpakken i Posten signering er basert på ASiC-E standarden ([Associated Signature Containers, Extended form](#)). Profilen er lagd for å ligne på den som er brukt for [sikker digital post](#). Les mer om [profilen som er benyttet for ASiC](#).

Pakken skal inneholde dokumentet som skal signeres (en PDF eller ren tekstfil), en fil kalt `manifest.xml` som beskriver metadata for dokumentet (emner, hvem som skal signere osv.), samt en fil kalt `signatures.xml` som er signaturen over hele dokumentpakken.

Dokument

Filen er enten PDF eller en ren tekstfil, og kan maksimalt være 3 MB (3 145 728 bytes) stor. Denne filen refereres til med det påkrevde `href`-attributtet i `document`-elementet i `manifest.xml`. Se eksempler for [synkrone](#) og [asynkrone](#) oppdrag.

manifest.xml

Filen følger skjemaet `http://signering.posten.no/schema/v1` som finnes i dette repoet. Eksempler finnes under «Steg 1: opprette signeringsoppdraget» for de ulike integrasjonsmønstrene.

signatures.xml

Filen følger skjemaet `http://uri.etsi.org/2018/v1.2.1#`. Se katalogen [thirdparty](#) for kopier av de relevante standardskjemaene.

Eksempel på komplett fil

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<XAdESSignatures xmlns="http://uri.etsi.org/2018/v1.2.1#">
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#" Id="Signature">
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n" />
      <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
      <Reference Id="ID_0" URI="document.pdf">
        <DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#sha256" />
        <DigestValue>LPJNuL+wow4m6DsQxbninhSWHlwfp0JecwQzYp0LmCQ=
```

```

</Reference>
<Reference Type="http://uri.etsi.org/01903#SignedProperties" URI="#Sign
  <Transforms>
    <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20
  </Transforms>
  <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
  <DigestValue>cV6hPhJ6f8hnl0J9czhubj08rWhJmzCQsomx0DfYyYM=</DigestVa
</Reference>
</SignedInfo>
<SignatureValue>VTc0CBKyuD0DRsJx7JJf6c2iH+TndFcxlaj0nP99snV6magufrPR8JSYad
XgIY9jfkAVLtAbiko9VcRpSopP1zj6tM3lrSao0/LBKP0rWNZCQINgw8f3pkGbi1bUKVwhb
+bc2rZiZoaWg0ByhsFZ25hWrl+GgC3PNsEzA+WN3JbGAQ00xtKudRG1vMjdjfsGtmvFYVQ0
5Vxdfovoia3x6zm5zbHWRQdVoUTS3vv5Mv6GAs7JAnDwSNxRVSizN5Q0B6xB60xRn+BFwdVe
cuReWIXY2r8yocS9MAZxFG+4SAHGxjJkNkgLHg==
</SignatureValue>
<KeyInfo>
  <X509Data>
    <X509Certificate>MIIDYzCCAkugAwIBAgIEIyZ/HzANBgkqhkiG9w0BAQsFADBiMQ
CBMCTk8xDTALBgNVBACTBE9zbG8xETAPBgNVBAoTCEF2c2VuZGVyMREwDwYDVQQQ
cjERMA8GA1UEAxMIQXZzZW5kZXIwHhcNMTQwNTIwMTIwMDA3WhcNMTUwNTE1MTI
CQYDVQQGEWJOTzELMAkGA1UECBMCTk8xDTALBgNVBACTBE9zbG8xETAPBgNVBAo
MREwDwYDVQQLEWhBdnNlbmRlcjERMA8GA1UEAxMIQXZzZW5kZXIwggEiMA0GCSq
A4IBDwAwggEKAoIBAQC0q505/fn9fDCZjvMlSWJNEj0kVLeFo233MEfhOU0hU44
ZCzWR58Eo8Fn90bEIosI8rCvw8XsNaDaeVgZ3PDtXTuA8luL/IphWXfuHxdmFm3
J215NIScrZGkgBKjb7uVo+usGYUpqkbj15kctTziRZo0k2i73iJd1+DjPGZ20zA
qE+pRwpHQ0kMiRlNrZxDD1mTJR2RLYYp/guW93YbIgJv4mhV3ZpJL8idU2YECkM
ZU0E5Us4SvuDPrg48ELE140AtXQb8xyuGrLhCm5JyHhAFJM0IoIGwqPAGMBAAG
DgQWBBSpQuhFDLFSUauhNrCbX+g8QXv9oTANBgkqhkiG9w0BAQsFAA0CAQEAAE
e90uHqkEJFFZF3CfdtRHx23s2wjDFJI4CEY8WHS0D90yn0yDZV/sWcu1Emi1nZ7
CBzZ+GkU04niu+jpM90Ck1JS1LU+e+lJz6ZL70ZVegTE6tLI8JwfInf7dBjSBnf
i5KipdivkTGXJCaLflFM3bXm5t0H8AzbrHc0JVVTTXhbjIvgg7JhFuiC1z1vM
89AvNttWcdSb0rQAVz0rjl+GKzM07Aw4tYB18j42P0tjMCjV5e0TCeNfLfnZ3r9
l5gXsb+YU/RP0lg+Xh5xRA==
    </X509Certificate>
  </X509Data>
</KeyInfo>
<Object>
  <QualifyingProperties xmlns="http://uri.etsi.org/01903/v1.3.2#"
    xmlns:ns2="http://www.w3.org/2000/09/xmldsig#" TargetRef="#SignedProperties"
  <SignedProperties Id="SignedProperties">
    <SignedSignatureProperties>
      <SigningTime>2015-11-25T15:45:42.115+01:00</SigningTime>
      <SigningCertificate>
        <Cert>
          <CertDigest>
            <ns2:DigestMethod Algorithm="http://www.w3.org/
            <ns2:DigestValue>6Gko40cr8upGenUAXIT6bBVCRfo=</
          </CertDigest>
          <IssuerSerial>
            <ns2:X509IssuerName>CN=Avsender, OU=Avsender, O
            <ns2:X509SerialNumber>589725471</ns2:X509Serial
          </IssuerSerial>
        </Cert>
      </SigningCertificate>
    </SignedSignatureProperties>
    <SignedDataObjectProperties>

```

```
<DataObjectFormat ObjectReference="#ID_0">
  <MimeType>application/pdf</MimeType>
</DataObjectFormat>
<DataObjectFormat ObjectReference="#ID_1">
  <MimeType>application/xml</MimeType>
</DataObjectFormat>
</SignedDataObjectProperties>
</SignedProperties>
</QualifyingProperties>
</Object>
</Signature>
</XAdESSignatures>
```

