h2. Dokumentpakke

Integriteten til dokumenter og metadata i signeringstjenesten skal kunne valideres mange år etter mottak. Det er ivaretatt ved at informasjonen pakkes i en dokumentpakke som beskyttes med digitale signaturer som beskrevet nedenfor. I praksis er dette en zip-fil med en gitt struktur som inneholder en digital signatur over innholdet.

h3. Standarder

table(table table-striped table-condensed).
. *Standard*	. Dokument	_. Versjon
{white-space:nowrap}. ETSI, ETSI TS 102 918	"Electronic Signatures and Infrastructures (ESI); Associated Signature":etsi1	{white-space:nowrap}. ETSI, 2013-06.
ETSI, ETSI TS 103 174	"Electronic Signatures and Infrastructures (ESI); ASiC Baseline Profile":etsi2	ETSI, 2013-06.
ETSI, ETSI TS 101 903	"Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)":etsi3	ETSI, 2010-12.
ETSI, ETSI TS 103 171	"Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile":etsi4	ETSI, 2012-03.

h4. ASiC-profil for dokumentpakken

Dokumentet pakkes i en dokumentpakke sammen med noe metadata i henhold til "ASiC (ETSI TS 102 918)":etsi1, og videre begrenset i henhold til profilen definert i "Baseline Profile (ETSI TS 103 174)":etsi2. Ytterlige begrensninger følger nedenfor:

table(table table-striped table-condensed).
. *Krav*	. Felt	_. Kommentar
"krav 6.1":etsi2_9	"ASiC conformance"	Skal være "ASiC-E XAdES"
"krav 8.1":etsi2_11	"ASiC-E Media type identification"	Skal være "ASiC file extension is ".asice""
"krav 8.2":etsi2_11	"ASiC-E Signed data object"	Alle filer utenfor META-INF katalogen skal være signert.
"krav 8.3.1":etsi2_12	"ASiC-E XAdES signature"	Det skal kun være en signatur i META-INF katalogen, med navn signatures.xml. Denne signaturen skal dekke alle andre filer i beholderen, og avsenderens virksomhetssertifikat skal benyttes for signering.
{white-space:nowrap}. "krav 8.3.2":etsi2_12	"Requirements for the contents of Container" refererer til "6.2.2 punkt 4b) "META-INF/manifest.xml" if present […] i "ASiC":etsi1	Denne filen skal ikke være tilstede.

h4. Signatur i dokumentpakken

Dokumentpakken bør være signert av "Behandlingsansvarlig", men kan signeres av "Databehandler".

Signaturen skal være i henhold til "XAdES (ETSI TS 101 903)":etsi3 med basisprofilen definert i "XAdES Baseline Profile (ETSI TS 103 171)":etsi4 (B-Level Conformance). Ytterlige begrensninger følger nedenfor:

table(table table-striped table-condensed).
. *Krav*	. Felt	_. Kommentar
"krav 5.1":etsi4_8	"Algorithm requirements"	Signeringsalgoritmen skal være "http://www.w3.org/2001/04/xmldsig-more#rsa-sha256":http://www.w3.org/2001/04/xmldsig-more#rsa-sha256. Fingeravtrykksalgoritmen i referansene skal være "http://www.w3.org/2001/04/xmlenc#sha256":http://www.w3.org/2001/04/xmlenc#sha256. Fingeravtrykksalgoritmen i CertDigest skal være "http://www.w3.org/2000/09/xmldsig#sha1":http://www.w3.org/2000/09/xmldsig#sha1.
"krav 6.2.1":etsi4_10	"Placement of the signing certificate"	. Alle sertifikater fra virkomhetsertifikatet og opp til og inkludert en tiltrodd rot skal være inkludert.
"krav 6.2.2":etsi4_11	"Canonicalization of ds:SignedInfo element"	Bør være "http://www.w3.org/2006/12/xml-c14n11":http://www.w3.org/2006/12/xml-c14n11 Kan være "http://www.w3.org/TR/2001/REC-xml-c14n-20010315":http://www.w3.org/TR/2001/REC-xml-c14n-20010315
"krav 6.2.3":etsi4_11	"Profile of ds:Reference element"	Alle dokumenter skal være med, og det er ikke lov med referanser utenfor dokumentpakken.
"krav 6.2.4":etsi4_12	"Transforms within ds:Reference element"	Alle fil-referansene skal være uten transform, og referansen til SignedProperties skal være "http://www.w3.org/TR/2001/REC-xml-c14n-20010315":http://www.w3.org/TR/2001/REC-xml-c14n-20010315
"krav 6.3.1":etsi4_12	"Profile of xades:SigningCertificate element"	Ingen ytterlige begrensninger.
"krav 6.3.2":etsi4_13	"Profile of xades:SigningTime element"	Tidsangivelsen skal være korrekt innenfor +/- 5 sekunder.
{white-space:nowrap}. "krav 6.3.3":etsi4_13	"Profile of xades:DataObjectFormat element"	Kun MimeType og ObjectReference skal være med.

[etsi1]http://www.etsi.org/deliver/etsi_ts/102900_102999/102918/01.03.01_60/ts_102918v010301p.pdf
[etsi2]http://www.etsi.org/deliver/etsi_ts/103100_103199/103174/02.02.01_60/ts_103174v020201p.pdf
[etsi2_9]http://www.etsi.org/deliver/etsi_ts/103100_103199/103174/02.02.01_60/ts_103174v020201p.pdf#page=9
[etsi2_11]http://www.etsi.org/deliver/etsi_ts/103100_103199/103174/02.02.01_60/ts_103174v020201p.pdf#page=11

[etsi2_12]http://www.etsi.org/deliver/etsi_ts/103100_103199/103174/02.02.01_60/ts_103174v020201p.pdf#page=12
[etsi3]http://www.etsi.org/deliver/etsi_ts%5C101900_101999%5C101903%5C01.04.02_60%5Cts_101903v010402p.pdf
[etsi4]http://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf
[etsi4_8]http://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf#page=8
[etsi4_10]http://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf#page=10
[etsi4_11]http://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf#page=11
[etsi4_12]http://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf#page=12
[etsi4_13]http://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf#page=13