SIA "EUSO"
A.Briāna iela 9A-2
Rīga LV-1001, Latvija
tālrunis +371 67378233
e-pasts euso@euso.lv
www.euso.lv

Informācijas Tehnoloģijas

EDOC ELEKTRONISKĀ PARAKSTA FORMĀTS 2.0

Sagatavots:

VAS LVRTC
T, 26. novembris, 2014
Versija 0.95 (Public Draft v3)

Sagatavoja:

Ivars Muciņš
SIA EUSO

Izmaiņu un apstiprinājumu lapa

Izmaiņu uzskaitījums

Datums	Autors	Versija	Izmaiņu apraksts
10.10.2014	Ivars Muciņš	0.90	Sākotnēja versija
14.10.2014	Ivars Muciņš	0.92	Izmaiņas pēc komentāru izskatīšanas
21.10.2014	Ivars Muciņš	0.93	Precizējums par paraksta kriptogrāfisko algoritmu izmantošanu
03.11.2014	Ivars Muciņš	0.94	Papildinājums par gadījumiem, kad parakstā ir iekļaujami CRL dati
26.11.2014	Ivars Muciņš	0.95	Redakcionāli labojumi

Izskatītāji

Vārds, uzvārds	Amats	Apstiprinātā versija	Datums
Gatis Beikerts	Sertifikācijas pakalpojumu pārvaldnieks	0.92 (Public Draft)	14.10.2014
Gatis Beikerts	Sertifikācijas pakalpojumu pārvaldnieks	0.93 (Public Draft v2)	21.10.2014
Gatis Beikerts	Sertifikācijas pakalpojumu pārvaldnieks	0.95 (Public Draft v3)	26.11.2014

Saturs

1. Ievads

Šis dokuments apraksta elektroniskā paraksta formātu EDOC 2.0. Dokuments veidots saskaņā ar Eiropas Direktīvu "Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures".

Šajā dokumentā aprakstītais elektroniskā paraksta formāts ir veidots uz sekojošu ETSI standartu pamata:

ETSI standarts "XML Advanced Electronic Signatures (XAdES)" TS 101 903 [1] (turpmāk XAdES) apraksta uz XML pamata veidotus un platformas neatkarīgus, uzlabotā elektroniskā paraksta formātus. Šie parakstu formāti satur pietiekamu informāciju, lai būtu piemēroti lietošanai ilgtermiņā. ETSI standarts "XAdES Baseline Profile" TS 103 171[2] precizē praktiski pielietojamos XAdES profilus un nosaka tajos iekļaujamos datus.

ETSI standarts "Associated Signature Containers (ASiC)" [3]TS 102 918[3] (turpmāk ASiC) apraksta parakstīto datu, XAdES parakstu un citas nepieciešamās papildus informācijas apvienošanu vienā datnē. ETSI standarts "ASiC Baseline Profile" ETSI TS 103 174[4] precizē praktiski pielietojamos ASiC profilus un nosaka tajos iekļaujamos datus.

XAdES specifikācija ir tikusi izstrādāta un attīstījusies ilgākā laika posmā. Šajā laika posmā ir tikušas izveidotas daudzas uz šī standarta bāzētas elektroniskā paraksta izstrādes, kuras izrādījušās savstarpēji nesaderīgas. Nesaderības iemesli ir meklējami, galvenokārt, ļoti lielajā XAdES izvēles iespēju skaitā, jo praktiski neviens risinājums neatbalsta visas neobligātās iespējas. Šī iemesla dēļ ETSI standarti tika papildināti ar "XAdES Baseline Profile" un "ASiC Baseline Profile", kuri precizējot praktiski pielietojamo informāciju, nodrošina elektroniski parakstīto dokumentu savstarpējo saderību.

Gan augstākminētie standarti, gan to papildinājumi un precizējumi, ir paredzēti vispārīgam pielietojumam dažādās infrastruktūrās. Praktisku iemeslu dēļ, ir nepieciešams papildus precizēt EDOC 2.0 formātā obligāti un izvēles kārtā iekļaujamos elementus, vērtības un citus papildus datus, definējot EDOC 2.0 formāta profilus.

Šis dokuments ir veidots kā precizējums augstākminētajiem ETSI standartiem, tos neatkārtojot. EDOC 2.0 specifikācija ir pilnībā saderīga ar augstākminētajiem standartiem.

1.1. Mērķauditorija

Dokuments ir paredzēts izstrādātājiem, kuri izstrādā un ievieš risinājumus, kuros tiek nodrošināts EDOC 2.0 dokumentu formāta atbalsts.

1.2. Apzīmējumi

Specifikācijā, XAdES[1] un ASiC[2] standartu izpratnē, ir izmantotas sekojošas vārdu formas, konstrukcijas un apzīmējumi:

- vārdu "obligāti" un "nepieciešams" vai prefiksa "jā", izmantošana norāda uz to, ka funkcionalitātei ir jābūt obligāti realizētai;
- vārds "vajadzētu" un "ieteicams" apzīmē realizācijai ieteicamo funkcionalitāti;
- Ar vārdiem "var" un "pēc izvēles" tiek atzīmētas papildus iespējas.

Apzīmējums	Veidotājs	Apstrādātājs
Obligāts (O)	Obligāti jāveido šis elements.	Obligāti jāapstrādā šis elements.
Ieteicams (I)	Ieteicams veidot šo elementu.	Ja izveidots, obligāti jāapstrādā šis elements.
Pēc izvēles (P)	Pēc izvēles var veidot šo elementu.	Ja izveidots, pēc izvēles var apstrādāt šo elementu.
Nelieto (N)	Elements netiek veidots.	Elements netiek apstrādāts.

1.3. Atsauces

Dokumentā lietotās sekojošas atsauces uz citiem dokumentiem:

[1] ETSI TS 101 903 v1.4.2 (2010-12) – XML Advanced Electronic Signatures (XadES)

[2] ETSI TS 103 171 v2.1.1 (2012-03) – XAdES Baseline Profile
[3] ETSI TS 102 918 v1.3.1 (2013-06) – Associated Signature Containers (AsiC)
[4] ETSI TS 103 174 v2.2.1 (2013-06) – ASiC Baseline Profile
[5] ETSI TS 102 023 v1.2.2 (2008-10) – Policy requirements for time-stamping authorities
[6] ETSI TS 102 176-1 v2.1.1 (2011-07) – Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms
[7] ITU-T Recommendation X.509: "Information technology - Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks"
[8] IETF RFC 3161: "Internet X.509 Public Key Infrastructure Time-Stamp protocol -TSP"
[9] IETF RFC 6960: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP"
[10] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"
[11] IETF RFC 3275: "XML-Signature Syntax and Processing"
[12] OASIS "Open Document Format for Office Applications (OpenDocument) Version 1.2 Part 3: Packages"

2. Kriptogrāfiskie algoritmi

EDOC 2.0 parakstos tiek ieteikts lietot tikai SHA-256 vai labākus jaucējsummas aprēķina algoritmus. Parakstu šifrēšanai tiek ieteikts lietot RSA algoritmus ar minimālo šifrēšanas atslēgas garumu 2048 biti.

Reālajā vidē šos nosacījumus ne vienmēr ir iespējams izpildīt, jo XAdES elektroniskais paraksts, neskaitot parakstītāja pievienoto parakstu, satur daudzus citus elektroniski parakstītus elementus (sertifikātus, laika zīmogus, OCSP atbildes, CRL, u.c.), kurus ir veidojusi sertifikācijas pakalpojuma sniedzēja infrastruktūra un var saturēt vecākus algoritmus.

2.1. Jaucējfunkcijas algoritmi

Šī specifikācija nosaka, ka EDOC 2.0 parakstāmās vērtības jaucējsummas aprēķiniem ir ieteicams lietot vismaz SHA-256 (http://www.w3.org/2001/04/xmlenc#sha256) jaucējsummas aprēķina algoritms. Tikai gadījumos, ja elektroniskā paraksta radīšanas ierīce neatbalsta SHA-256 algoritma izmantošanu, EDOC 2.0 parakstāmās vērtības jaucējsummas aprēķiniem ir pieļaujams lietot SHA-1 algoritmu (http://www.w3.org/2001/04/xmlenc#sha1).

2.2. Asimetriskie šifrēšanas algoritmi

Šī specifikācija nosaka, EDOC 2.0 paraksta vērtības aprēķinam ir ieteicams lietot RSA SHA-256 algoritmu (http://www.w3.org/2001/04/xmldsigmore#rsa-sha256) ar minimālo šifrēšanas atslēgas garumu 2048 biti.

Tikai gadījumos, ja elektroniskā paraksta radīšanas ierīce neatbalsta RSA SHA-256 algoritma izmantošanu, EDOC 2.0 paraksta vērtības aprēķinam ir atļauts lietot RSA SHA-1 algoritmu (http://www.w3.org/2001/04/xmldsig#rsa-sha1) ar minimālo šifrēšanas atslēgas garumu 2048 biti.

3. EDOC paraksta profili

Lai nodrošinātu dažādus parakstīšanas un parakstu uzturēšanas scenārijus, EDOC paraksts tiek iedalīts 3 atsevišķos profilos, kuros ietvertie dati tiek loģiski paplašināti. Visi EDOC paraksta profili ir veidoti uz "XML Advanced Electronic Signatures (XadES)"[1] un XAdES Baseline Profile[2] specifikāciju pamata.

Atšķirībā no EDOC 1.0 formāta, EDOC 2.0 tiek izmantots tikai paralēlais paraksts (dokumentos ar vairākiem parakstiem iepriekš pievienotie paraksti netiek parakstīti).

3.1. EDOC pamata paraksta profils

EDOC pamata profils veidots uz XAdES-B profila pamata, kurš ir definēts XAdES Baseline Profile[2] 6. nodaļā. Pamata profila dati satur parakstāmo datu struktūras un elektronisko parakstu, kurš ir aprēķināts no šajā struktūrā norādītajiem datiem. Šī profila dati nesatur paraksta derīgumu apliecinošu informāciju - laika zīmogu, sertifikātu derīguma apliecinājumus, u.c. Šis profils veido pamatu citiem EDOC profiliem un ir izdalīts atsevišķi, lai nodrošinātu atsevišķus parakstīšanas scenārijus automatizētās datu apstrādes vidēs.

EDOC pamata profila struktūrai ir jāsatur sekojošus elementus:

- *ds:SignedInfo* elementu struktūra ar referencēm uz parakstāmajiem datu objektiem un to jaucējsummu;
- *ds:SignatureValue* elements, kurš satur elektroniskā paraksta vērtību;
- *ds:KeyInfo* elementu struktūra, kura satur parakstītāja sertifikātu;

- *xades:QualifyingProperties* elementu struktūra, kura satur neparakstītās un parakstītās paraksta īpašības.

Uz *ds:SignedInfo* elementu struktūru ir jāattiecina sekojoši ierobežojumi:

Elements		**Attribūti**	**Piezīmes**
Signature	O	*Id*	Piemēram, "S0"
SignedInfo	O		
CanonicalizationMethod	O	*Algorithm="http://www.w3.org/2006/12/xml-c14n11"*	
SignatureMethod	O	*Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"*	*Pieļaujams lietot Algorithm="http://www.w3.org/2001/04/xmldsig#rsa-sha1" tikai, elektroniskā paraksta radīšanas ierīce neatbalsta prasīto.*
Reference	O	*Id, URI, Type*	Skatīt paskaidrojumu zemāk

ds:SignedInfo elementu struktūrai ir jāsatur divi vai vairāk *ds:Reference* elementi ar referencēm uz parakstītajiem objektiem:

- viena reference uz katru parakstāmo failu. Šajā gadījumā *ds:Reference* elementam ir obligāti jāsatur parametrs URI ar referenci uz datu objektu. Piemēram, *URI="document.odt";*
- viena reference uz *SignedProperties* elementu struktūru. Šajā gadījumā *ds:Reference* elementam ir obligāti jāsatur parametrs Type ar vērtību "*http://uri.etsi.org/01903/#SignedProperties*" un parametrs *URI* ar referenci uz *SignedProperties* elementu struktūru, piemēram, *URI="#SignedProperties"*.

Uz *ds:Reference* elementu struktūru ir jāattiecina sekojoši ierobežojumi:

Elements		**Parametrs**	**Piezīmes**
DigestMethod	O	*Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"*	*Pieļaujams lietot Algorithm="http://www.w3.org/2001/04/xmlemc#sha1" tikai, ja elektroniskā paraksta radīšanas ierīce neatbalsta prasīto.*
DigestValue	O		

Saskaņā ar IETF RFC 3275: "XML-Signature Syntax and Processing" [11] 4.4 sadaļu, parakstītāja sertifikāts ir obligāti iekļaujams *ds:KeyInfo* apakšelementa *ds:X509Data* apakšelementā *ds:X509Certificate*.

ds:QualifyingProperties elementu struktūra ir jāiekļauj *ds:Object* elementā izmantojot tiešās iekļaušanas metodi, kā tas aprakstīts XAdES [1] 6.2 un 6.3 sadaļās. Netiešā iekļaušana ar *QualifyingPropertiesReference* elementa palīdzību netiek izmantota.

EDOC 2.0 tiek lietoti sekojošas *ds:QualifyingProperties* elementu struktūras:

Elements		**XAdES sadaļa**	**Piezīmes**
QualifyingProperties	O	6.2	Obligāti jālieto parametrs *Target* ar referenci uz *ds:Signature* elementu. Piemēram, *Target="#S0"*
SignedProperties	O	6.2.1	Obligāti jālieto parametrs *Id*. Piemēram, *Id="S0-SignedProperties"*
UnsignedProperties	O	6.2.2	
SignedSignatureProperties	O	6.2.3	

SignedDataObjectProperties	O	6.2.4	
UnsignedSignatureProperties	O	6.2.5	
SigningTime	O	7.2.1	Obligāti jālieto "Zulu" laika zona (GMT +0).Piemēram, *"2014-10-10T012:42:45Z"*
SigningCertificate	O	7.2.2	Obligāti jāsatur informācija tikai par parakstītāja sertifikātu. Parametrs *URI* netiek lietots.
SignaturePolicyIdentifier	N	7.2.3	Netiek lietots
CounterSignature	N	7.2.4	Netiek lietots
DataObjectFormat	O	7.2.5	Obligāti norādāms par katru parakstīto datu objektu, izņemot *SignedProperties* elementu.
MimeType	O	7.2.5	Parakstītā datu objekta MIME tips.
ObjectReference	O	7.2.5	Reference ar *Id* vērtību, kura norādīta atbilstošajā *ds:Reference* elementā.
CommitmentTypeIndication	N	7.2.6	Netiek lietots
SignatureProductionPlace	I	7.2.7	
SignerRole	I	7.2.8	Tiek lietots tikai *ClaimedRoles* elements, *CertifiedRoles* netiek lietots.
AllDataObjectsTimeStamp	N	7.2.9	Netiek lietots
IndividualDataObjectsTimeStamp	N	7.2.10	Netiek lietots

3.2. EDOC kvalificēta paraksta profils

Elektroniskā paraksta izveidošana nav tiešsaistes darbība un nav iespējams iegūt tiešu informāciju par tā izveidošanas laiku, par izveidošanas laiku tiek uzskatīts laiks, kurš ir ietverts elektroniskajam parakstam pievienotajā laika zīmogā ar nosacījumu, ka parakstītāja sertifikāts šajā brīdī ir bijis derīgs. Parakstītāja sertifikāta derīguma apliecinājums ir obligāti ietverams elektroniskajam parakstam pievienotajā informācijā.

EDOC pamata paraksta profils nesatur pārbaudāmu informāciju par paraksta izveidošanas laiku, kā arī informāciju vai parakstītāja sertifikāts paraksta izveidošanas brīdī ir bijis derīgs.

Lai EDOC pamata parakstu pēc tā izveides varētu uzskatīt par pārbaudāmu un derīgu, pārbaudes dati ir jāiegūst un jāpievieno parakstam nekavējoties, piemēram:

- darba virsmu vidēs parakstītāja aplikācija iegūst un pievieno laika zīmogu un pārbaudes datus nekavējoties pēc paraksta izveidošanas;
- tīmekļa vidēs servera puses aplikācija iegūst un pievieno laika zīmogu un pārbaudes datus, nekavējoties pēc paraksta iegūšanas no attālinātā lietotāja.

Šī specifikācija nosaka veidu, kādā pamata elektroniskajam parakstam ir pievienojama parakstītāja sertifikāta derīguma, laika zīmoga un cita nepieciešamā informācija, lai paraksts atbilstu EDOC kvalificēta paraksta profilam.

EDOC kvalificēta paraksta profils ir veidots uz XAdES-LT profila pamata, kurš ir definēts XAdES Baseline Profile[2] 8. nodaļā. EDOC kvalificēta paraksta profils pieļauj tikai IETF RFC 3161[8] saderīgu laika zīmogu lietošanu. Laika zīmoga izsniedzējam ir jābūt akreditētam Latvijas Republikā.

EDOC kvalificētā parakstā vienīgi *SignatureTimeStamp* elementā ietvertais laiks ir uzskatāms par elektroniskā paraksta izveidošanas laiku, ar nosacījumu, ka atbilst augstākminētajiem nosacījumiem.

Elements		**XAdES sadaļa**	**Piezīmes**
SignatureTimeStamp	O	7.3	Atribūts *Id* ir obligāts.

EncapsulatedTimeStamp	O	7.1.4.3	Laika zīmoga izsniedzējam ir jābūt akreditētam Latvijas Republikā, kā Uzticamam sertifikācijas pakalpojumu sniedzējam.
CompleteCertificateRefs	N	7.4.1	Netiek lietots.
CompleteRevocationRefs	N	7.4.2	Netiek lietots.
AttributeCertificateRefs	N	7.4.3	Netiek lietots.
AttributeRevocationRefs	N	7.4.4	Netiek lietots.
SigAndRefsTimeStamp	N	7.5.1	Netiek lietots.
RefsOnlyTimeStamp	N	7.5.2	Netiek lietots.
CertificateValues	O	7.6.1	Atļauta ir tikai *EncapsulatedX509Certificate* apakšelementu lietošana. Šajā elementā ir jāiekļauj visu ķēžu sertifikāti izņemot parakstītāja sertifikātu. Ja OCSP vai TSA atbildes nesatur atbildētāja sertifikātu, šie sertifikāti ir obligāti jāiekļauj šajā elementā.
RevocationValues	O	7.6.2	Ir atļauta tikai *OCSPValues* un *EncapsulatedOCSPValue* apakšelementu lietošana. Visām OCSP atbildēm ir jābūt sertifikāta derīgumu apstiprinošām. Skatīt piezīmi (*) zemāk.
AttrAuthoritiesCertValues	N	7.6.3	Netiek lietots.
AttributeRevocationValues	N	7.6.4	Netiek lietots.

* Tikai gadījumos, kad sertifikācijas pakalpojumu sniedzējs par kādu no ķēdes sertifikātiem neizsniedz OCSP atbildes, ir pieļaujama CRL iekļaušana parakstā. Iekļaujot CRL datus ir atļauta tikai *CRLValues* un *EncapsulatedCRLValue* apakšelementu lietošana. Visiem CRL datiem ir jābūt sertifikāta derīgumu apstiprinošiem. Parakstītāja sertifikāta OCSP atbildes iekļaušana ir obligāta.

3.3. EDOC arhīva paraksta profils

Kvalificēts EDOC paraksts ir uzskatāms par pietiekami drošu līdz brīdim, kamēr par pietiekoši drošiem tiek uzskatīts kriptogrāfiskais materiāls un algoritmi ar ko šis paraksts ir radīts. Straujā informācijas tehnoloģiju attīstība rada draudus, ka mūsdienās izmantotie kriptogrāfiskie algoritmi vai atslēgu garumi, jau tuvākā nākotnē var nebūt uzskatāmi par pietiekoši drošiem pret viltošanu.

Lai nākotnē aizsargātu iepriekš radītos elektroniskos parakstus, kuru radīšanai izmantotais kriptogrāfiskais materiāls vai algoritmi ir atzīti par nedrošiem, tiek izmantots papildus (arhīva) laika zīmogošanas mehānisms ar par drošām un laikam atbilstošām kriptogrāfiskajām metodēm, kas ir atbilstošas spēkā esošām Eiropas Savienības prasībām [6]. XAdES[1] specifikācija neierobežo parakstam pievienojamo arhīva laika zīmogu skaitu, kas nodrošina ilgstošu paraksta derīguma nodrošināšanu arī tālākā nākotnē.

EDOC arhīva paraksta profils ir veidots uz XAdES-LTA profila pamata un loģiski papildina EDOC kvalificēta paraksta profilu. XAdES-LTA profils ir definēts XAdES[1] 8. nodaļā un XAdES Baseline Profile[2] 9. nodaļā.

Jaucējsummas aprēķinam jāizmanto tikai XAdES[1] 8.2. nodaļā aprakstītā metodika “Not distributed case”.

Elements		**XAdES sadaļa**	**Piezīmes**
xadesv141:ArchiveTimeStamp	O	8.2	Atribūts *Id* ir obligāts.
EncapsulatedTimeStamp	O	7.1.4.3	Pieļaujama vienīgi IETF RFC 3161[8] saderīgu laika zīmogu lietošana. Laika zīmoga izsniedzējam ir jābūt akreditētam Latvijas Republikā, kā Uzticamam sertifikācijas pakalpojumu sniedzējam.
xadesv141:TimeStampValidationData	O	8.1	Elements ir obligāts, ja arhīva laika zīmoga pārbaudes dati nav jau iekļauti EDOC kvalificēta paraksta datos.

CertificateValues	O	7.6.1	Atļauta ir tikai *EncapsulatedX509Certificate* apakšelementu lietošana. Šajā elementā jāiekļauj visi ar arhīva laika zīmogu un tā pārbaudi saistītie sertifikāti ar nosacījumu, ka tiek dati netiek dublēti ar kvalificēta profila datiem.
RevocationValues	O	7.6.2	Ir atļauta tikai *OCSPValues* un *EncapsulatedOCSPValue* apakšelementu lietošana. Visām OCSP atbildēm ir jābūt sertifikāta derīgumu apstiprinošām. Skatīt piezīmi (*) zemāk.

* Tikai gadījumos, ja sertifikācijas pakalpojumu sniedzējs par kādu no ķēdes sertifikātiem neizsniedz OCSP atbildes, ir pieļaujama CRL iekļaušana. Iekļaujot CRL datus ir atļauta tikai *CRLValues* un *EncapsulatedCRLValue* apakšelementu lietošana. Visiem CRL datiem ir jābūt sertifikāta derīgumu apstiprinošiem.

4. EDOC pakotnes formāts

Šajā sadaļā ir aprakstīta parakstāmo datu un parakstu apvienošanas metodika vienotā EDOC pakotnē. EDOC pakotne ir satur parakstītos datus, pievienotos parakstus, visu nepieciešamo informāciju parakstu pārbaudei un citu papildus informāciju, kas nepieciešama šis pakotnes apstrādei.

EDOC pakotnes formāts ir balstīts uz "Associated Signature Containers (AsiC)" [3] standarta un "ASiC Baseline Profile" [4] specifikāciju pamata. EDOC pakotne atbilst "ASiC Baseline Profile" [4] 8.3. nodaļas "Requirements for ASiC-E XAdES" prasībām.

4.1. EDOC pakotnes identifikācija

EDOC datne ir ZIP pakotne. EDOC datņu nosaukumos ir jālieto paplašinājums *".edoc"*. Saskaņā "ASiC Baseline Profile" [4] 8.1. punkta noteikumiem ir EDOC pakotnēm ir obligāti jānorāda *mimetype* vērtība "*application/vnd.etsi.asic-e+zip*".

4.2. EDOC parakstīto datu glabāšana pakotnē

Parakstītās datnes ir jāglabā pakotnes saknes mapē. Pievienojot parakstītās datnes ir jāievēro *mimetype* lietošanas noteikumus saskaņā ar "Associated Signature Containers (AsiC)" [3] A.1 pielikumu.

4.3. EDOC parakstu glabāšana pakotnē

Parakstu datnes ir jāglabā *META-INF* mapē. Parakstu datņu nosaukumi ir jāveido izmantojot vedni "*edoc-signatures-[*].xml"*, kur [*] tiek aizstāts ar mapes ietvaros unikālu skaitli. Katras paraksta datnes saknes elementam ir jābūt *asic:XAdESSignatures* un tajā ir atļauts iekļaut tikai vienu parakstu (vienu *dsig:Signature* elementu). Saglabājot parakstu datnes, jāizmanto tikai "UTF-8" kodējums.

4.4. Pakotnes metadati

Saskaņā "ASiC Baseline Profile" [4] 8.3.2. punktu, metadatu glabāšanai pakotnē jāizmanto *META-INF* mapē izvietota *manifest.xml* datne, kura ir jābūt saderīgai ar OASIS "Open Document Format for Office Applications (OpenDocument) Version 1.2"[11] 3.2.sadaļas noteikumiem. Saglabājot *manifest.xml* datni jāizmanto tikai "UTF-8" kodējums.

EDOC pakotnēs uz *manifest.xml* saturu ir jāattiecina sekojoši ierobežojumi:

Elements		**Attribūti**	**Piezīmes**
manifest:manifest	O	*manifest:version="1.2"*	
manifest:file-entry	O	*manifest:full-path* *manifest:media-type*	Skat.piezīmi*
manifest:encryption-data	N		Elements netiek lietots.

* Katrai saknes mapē izvietotajai (izņemot *mimetype* datni) un parakstītajai datnei ir jāveido *manifest:file-entry* elements. Papildus *manifest:file-entry* elemets ir jāveido par pašu saknes mapi identificējot pakotnes tipu "*application/vnd.etsi.asic-e+zip*", piemēram, *"<manifest:file-entry manifest:full-path="" manifest:media-type="application/vnd.etsi.asic-e+zip">*.