



VALSTYBINĖ
MOKESČIŲ
INSPEKCIJA

VALSTYBINĖ MOKESČIŲ INSPEKCIJA PRIE LIETUVOS
RESPUBLIKOS FINANSŲ MINISTERIJOS

VMI duomenų mainų posistemis TIES

Duomenų teikimo sąsajos aprašas



VALSTYBINĖ
MOKESČIŲ
INSPEKCIJA

Versija:	2.27
Data :	2024-03-21
Būklė:	Patvirtinta
Pirmo leidimo data:	2016-05-23

Turinys

Dokumento metaduomenys	3
Dokumento keitimo chronologija.....	3
Dokumento derinimas	4
1 Įvadas	5
1.1 Dokumento paskirtis ir sudėtis	5
1.2 Susiję dokumentai ir priedai	5
2 Duomenų teikimo integracinė sąsaja	6
2.1 Duomenų teikimo schema	6
2.2 Portalo bendrieji reikalavimai	6
2.3 Duomenų teikimo, tikslinimo principai	7
2.4 Duomenų teikimo prisijungimo nuorodos	9
2.5 Duomenų teikimo failų dydžio apribojimai	9
3 Saugos reikalavimai	9
3.1 Reikalavimai skaitmeniniam sertifikatui	10
3.2 Duomenų paketo parengimo žingsniai	10
3.3 Duomenų paketo išpakavimo žingsniai	11
4 Paslaugos (WS metodai)	12
4.1 Metodas „SubmitPackage“	12
4.2 Metodas „GetStatus“	12
4.3 Metodas „GetTransmissionInfo“	13
4.4 Metodas „GetTransmissionsByDate“	14
4.5 Metodas „CancelPackage“	15
5 Pranešimai	16
5.1 Status-Sti	16
5.1.1 <i>Antraštės dalis</i>	17
5.1.2 <i>Pagrindinė dalis</i>	17
5.2 Bendrai naudojami paprastieji duomenų tipai	19
5.3 Bendrieji klasifikatoriai	20
5.3.1 <i>Paketo I lygio klaidų kodai</i>	20
5.3.2 <i>Paketo II lygio klaidų kodai</i>	21
5.3.3 <i>ISO valstybės</i>	22
5.3.4 <i>ISO valiutos</i>	22
5.4 Paketų būsenų schema	23
6 Priedai	24
6.1 Dažniausiai pasitaikančios duomenų paketo suformavimo klaidos ir jų sprendimo būdai	24
6.2 UNIX bash script'as pasirašyto ir užšifruoto duomenų paketo sukūrimui iš xml failo	26
6.3 UNIX bash script'as pasirašyto xml failo atkūrimui iš užšifruoto duomenų paketo	36
6.4 Priedas Nr. 1 „Instrukcija TIES nešifruotam paketui“	42
6.5 Priedas Nr. 2 „Instrukcija TIES paketui openssl notepad“	42

Dokumento metaduomenys

Dokumento keitimo chronologija

Data	Pakeitimas	Pakeisti skyriai
2016-05-23	Pradinė versija	visi
2016-05-27	Dokumentas papildytas MAI55-SKIS rinkinio aprašymu.	2, 5, 7
2016-06-13	Patikslinta pagal Užsakovo pastabas	1.3, 2.3
2016-06-16	Ištaisyta lentelių eilučių numeracija, patikslintas TIES pranešimų tipų sąrašas	4.3, 5
2016-10-04	Pakeitimai, pagal naujo tipo CRS-DAC2-LT pranešimų apdorojimą, surenkant informaciją apie užsienio šalių piliečių sąskaitas Lietuvos finansinėse institucijose.	visi
2017-01-03	Patvirtinta dokumento versija	-
2017-01-26	Dokumentas papildytas naujais skyreliais, apie nuorodas, per kurias galima teikti duomenis, bei teikiamų duomenų failų dydžio ribojimais.	Nauji sk.: 2.4 sk., 2.5 sk.
2017-02-02	Ištaisyta klaida dėl supainiotų nuorodų duomenų teikimui testavimui ir realių duomenų.	2.4 sk.
2017-04-14	Papildyta metodais „GetTransmissionsByDate“, „CancelPackage“, parametrais, klaidomis.	4, 5
2017-04-14	Papildyta TIES išorinio portalo (savitarnos) galimų funkcijų išvardinimu.	2.2 sk.
2017-05-31	Patikslinta skaitmeninio parašo suformavimo procedūra	3.2 sk.
2017-06-20	Portalo bendruosiuose reikalavimuose patikslinta, kad testiniai paketai pilnai neapdorojami. StatusSti papildytas elementu Severity, ir patikslinta ką reiškia priimtas pranešimas, ir ką reiškia atmestas.	2.2 sk. 5.1.2 sk.
2017-09-25	Papildyta nauju duomenų rinkiniu „FATCA-LT“ surenkant duomenis apie JAV rezidentų sąskaitas iš FI.	visi
2017-10-12	Papildyta nauju duomenų rinkiniu „CBC-DAC4-LT“ surenkant duomenis apie TĮG (tarptautinių įmonių grupių) ataskaitas	visi
2017-10-16	Patikslinta pagal apibendrintus duomenų teikėjus.	visi
2017-10-24	Papildyta priedais „Dažniausiai pasitaikančios duomenų paketo suformavimo klaidos ir jų sprendimo būdai“, „UNIX bash script'as pasirašyto ir užšifruoto duomenų paketo sukūrimui iš XML failo“ ir „UNIX bash script'as pasirašyto XML failo atkūrimui iš užšifruoto duomenų paketo“	Nauji sk.: 6 sk., 6.1 sk., 6.2 sk, 6.3 sk.
2017-10-31	Skyrius „Dažniausiai pasitaikančios duomenų paketo suformavimo klaidos ir jų sprendimo būdai“ papildytas nauju atveju dėl 20004 klaidos.	6.1 sk.
2018-01-03	Papildyta nauju duomenų rinkiniu „PALUK-ISMOK“ surenkant duomenis apie finansinių įstaigų gyventojams išmokėtas palūkanas	visi
2018-01-30	Papildyta nauju duomenų rinkiniu „TARP-IV-APSK“ surenkant duomenis apie individualios veiklos apskaitą.	1; 2; 5.2.

2018-03-02	Papildyta nauju duomenų rinkiniu „GDR-ISMOK“ surenkant duomenis apie gyvybės draudimo išmokas. Pataisyti netikslumai dėl rinkinio pavadinimo „PALUK-ISMOK“.	1; 2; 5.2.
2018-03-08	Papildyta nauju duomenų rinkiniu „FIN-PR-PERL“ surenkant duomenis apie finansinių priemonių perleidimus gyventojams.	1; 2; 5.2.
2018-09-03	Patikslintos 20004 klaidos dažniausiai pasitaikančios priežastys	6.1
2019-03-20	Papildyta nauju duomenų rinkiniu „TARP-PASK“, kuriame tarpusavio skolinimo platformų operatoriai teikia duomenis apie paskolas.	1.3; 2.3; 5, 5.3.
2019-05-21	Papildyta nauju duomenų rinkiniu „MoQ“, kuriame MoQ teikia duomenis apie arbatpinigius	1.3; 2.3; 5, 5.3.
2019-12-31	Papildyta nauju duomenų rinkiniu „DAC6-LT“	1.3; 2.3; 5, 5.3.
2020-03-30	Papildyta nauju duomenų rinkiniu „TARP-GYV-PAJ“	1.2; 1.3; 2.3; 5; 5.3.
2020-07-01	Papildyta atsakymo pranešimo „Status-Sti“ struktūra, įterpta nauja nebūtina atšaka (StatusSti/MessageBody/DAC6_IDs/), kuri aktuali atsakymams dėl DAC6-LT rinkinio.	5.1.2
2020-08-31	Papildyta nauju duomenų rinkiniu „MMR-SASK“	1.2; 1.3; 2.3; 5
2022-06-03	SD 451278 Dėl klaidos 20005 išdalinimo į keturias klaidas	6.1, 5.3.2
2022-12-09	Papildyta nauju duomenų rinkiniu „DPI-DAC7-LT“	1.2; 1.3; 2.3; 5; 5.3.
2023-02-24	Papildyta nauju duomenų rinkiniu „CESOP“	1.2; 1.3; 2.3; 5; 5.3.
2023-03-16	Patikslinta dėl duomenų rinkinio pavadinimo pakeitimo iš „CESOP“ į „PMT“	1.2; 1.3; 2.3; 5; 5.3.
2023-03-17	Pataisyta pagal pastabas	1.2; 1.3; 2.3; 5; 5.3.
2023-08-09	Pervadintas failas pagal VMI pateiktųjų kodavimą, patikslintas viršelį.	-
2023-09-14	Papildytos ir patikslintos taisyklės, kad duomenų rinkiniams, kurie turi požymį, kad jų duomenys gali būti teikiami nešifruoti, būtų taikomi tokie žingsniai, kad leistų pateikti nešifruotą xml su duomenimis.	2.2; 3; 3.1; 3.2; 3.3; 5.3.1
2024-02-15	Patikslinta versija pagal projekcinį sprendimą – jei teikiami nešifruoti duomenys, jie teikiami ir nepasirašyti sertifikatu.	3.2; 3.3
2024-03-21	Patikslinta, padidinus kritinio paketo dydžio ribą iki 200 Mb.	2.5

Dokumento derinimas

1 Įvadas

1.1 Dokumento paskirtis ir sudėtis

Šis dokumentas skirtas aprašyti reikalavimus, keliamus kompiuterizuotai duomenų teikimo VMI integracinei sąsajai.

Dokumentas skirtas duomenų teikėjams ar duomenų teikėjų informacines sistemas vystantiems subjektams siekiantiems užtikrinti tinkamą integraciją su VMI posistemių TIES.

Dokumentas aprašo duomenų teikimo integracijos sąsajos bendruosius principus, reikalavimus saugai, duomenų mainų paslaugas (WS metodus), naudojamus pranešimus, bendruosius duomenų tipus ir klasifikatorius.

1.2 Susiję dokumentai ir priedai

Priedai:

priedas Nr1 „MAI55 pranešimų XML schemas aprašymas“.

priedas Nr2 „CRS-DAC2-LT pranešimų XML schemas aprašymas“

priedas Nr3 „FATCA-LT pranešimų XML schemas aprašymas“

priedas Nr4 „CBC-DAC4-LT pranešimų XML schemas aprašymas“

priedas Nr5 „PALUK-ISMOK pranešimų XML schemas aprašymas“

priedas Nr6 „TARP-IV-APSK pranešimų XML schemas aprašymas“

priedas Nr7 „GDR-ISMOK pranešimų XML schemas aprašymas“

priedas Nr9 „TARP-PASK pranešimų XML schemas aprašymas“

priedas Nr11 „MoQ pranešimų XML schemas aprašymas“

priedas NR12 „DAC6-LT pranešimų XML schemas aprašymas“

priedas NR13 „TARP-GYV-PAJ pranešimų XML schemas aprašymas“

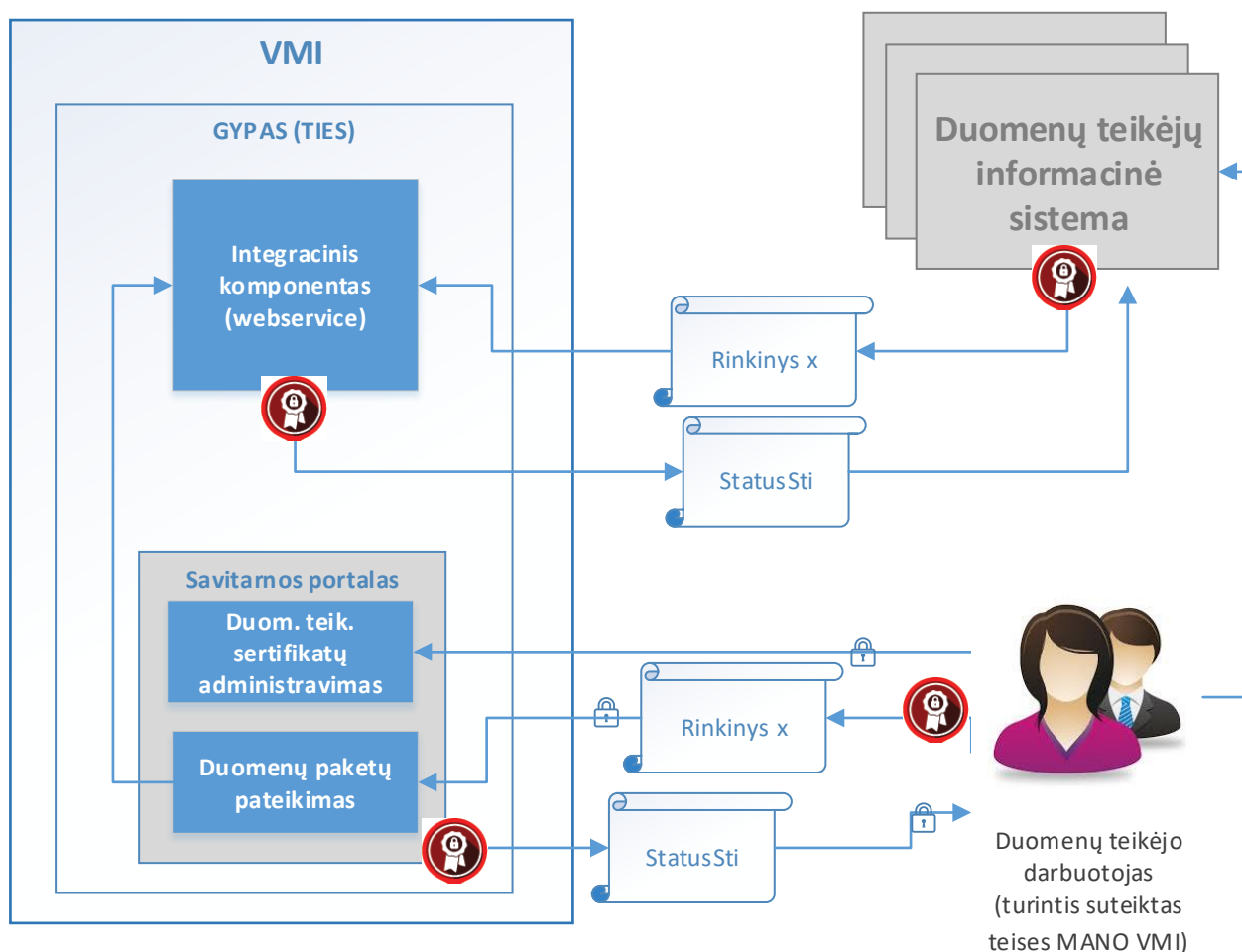
priedas NR14 „MMR-SASK pranešimų XML schemas aprašymas“

priedas Nr. 15 „DPI-DAC7-LT pranešimų XML schemas aprašymas“

priedas Nr. 16 „PMT pranešimų XML schemas aprašymas“

2 Duomenų teikimo integracinė sąsaja

2.1 Duomenų teikimo schema



Paveiksle pateikta kontekstinė duomenų pateikimo į VMI schema. Duomenų pateikimui yra kuriama GYPAS posistemė TIES, kuri užtikrina finansinių duomenų pateikimą į VMI ir nukreipia tolimesniam apdorojimui.

TIES sudaro tokio daly:

- Integracinis komponentas (WS);
- Savitarnos portalas;

2.2 Portalo bendrieji reikalavimai

TIES savitarnos portalas bus integruotas su „Mano VMI“ sprendimais autentifikavimo bei prieigos teisių valdymui. „Mano VMI“ yra numatytas teisių rinkinys („39 P.P.“), kuris yra naudotinas TIES portale ir yra skirtas teisių duomenis teikiančių subjektų atstovaujantiems asmenims suteikimui/atėmimui. Prieigos teisės, kurios bus suteikiamos TIES savitarnos portalo naudotojams, bus siejamos su duomenų rinkinių grupėmis (pvz.: MAI55, CRS /DAC2 duomenys) ir galimais portale atlikti veiksmams (pvz.: sertifikatų administravimas, duomenų rinkinio peržiūra, duomenų rinkinio teikimas ir pan.).

TIES autentifikavimo sprendimas bus integruotas su MANO VMI CAS sprendimais asmenų autentifikavimui/autorizavimui (atstovavimų nustatymas darbui portale pagal suteiktas teises ir pan.).

Duomenys teikiami XML rinkiniais, turi būti koduoti UTF-8 (bet ne UTF-8 BOM ar kitais formatais). Nekoduotus duomenis leidžiama teikti tik tiems duomenų rinkiniams, kurie turi nustatytą tokią opciją (požymį) – kad jų duomenys gali būti teikiami ir nešifruoti.

Duomenys teikiantys subjektai, kurie neturės galimybės jungtis bei duomenis teikti per integracinį komponentą, galės jungtis prie savitarnos portalo (TIES išorinis portalas). Savitarnos portale duomenis teikiančio subjekto įgaliotas atstovas, prisijungęs per „Mano VMI“ ir turintis ten suteiktas atitinkamas teises, galės atlikti tokius veiksmus TIES savitarnos portale:

- Viešieji raktai: duomenis teikiantis subjektas galės užregistruoti savo viešąjį raktą, peržiūrėti, kokie viešieji raktai buvo registruoti;
- Peržiūrėti ir atsisiųsti VMI viešuosius raktus;
- Duomenų paketai: galės peržiūrėti duomenis teikusio subjekto pateiktus duomenų paketus, jų pateikimo rezultatus, iš duomenis apdorojusios sistemos gautą atsakymo paketą, suteikiama galimybė atsisiųsti tiek pateiktą paketą, tiek gautą atsakymo paketą;
- Įkelti ir pateikti paruoštą duomenų paketą;
- Testiniai duomenų paketai: galimybė peržiūrėti bandomajam testavimui pateiktus duomenis teikusio subjekto duomenų paketus, jų pateikimo rezultatus, suteikiama galimybė atsisiųsti pateiktą paketą. Dėmesio – testiniai duomenų paketai apdorojimui ir loginiai kontrolei nesiunčiami, todėl pilna duomenų loginės kontrolės patikra jiems nevykdoma;
- Įkelti ir pateikti paruoštą testinį (bandomąjį) duomenų paketą, pagal duomenų teikimo schemas, kurių testavimas paskelbtas. Galimybė pasitikrinti ar paketas tinkamas pagal pirmines paketo lygio patikras. Dėmesio – testiniai duomenų paketai apdorojimui ir loginiai kontrolei nesiunčiami, todėl pilna duomenų loginės kontrolės patikra jiems nevykdoma;
- Duomenis turintis teikti subjektas, kuris neturi teiktinų duomenų už ataskaitinį laikotarpį, ir neturi galimybių tuščią ataskaitą (su tipu - nėra praneštinų duomenų) pateikti per WS, jei atitinkamam duomenų rinkiniui sukonfigūruota tokia galimybė – tuomet tuščią ataskaitą galima įvesti, sugeneruoti ir pateikti TIES savitarnos portale.

2.3 Duomenų teikimo, tikslinimo principai

Šiame etape numatyta, kad duomenis teikiantys subjektai į VMI teikia šiuos duomenų rinkinius per TIES:

- MAI55-SIPL;
- MAI55-SLIK;
- MAI55-SKIS;
- CRS-DAC2-LT;
- FATCA-LT;
- CBC-DAC4-LT;
- PALUK-ISMOK;
- TARP-IV-APSK;
- GDR-ISMOK;
- FIN-PR-PERL;
- TARP-PASK.
- MoQ;
- DAC6-LT
- TARP-GYV-PAJ

- MMR-SASK
- DPI-DAC7-LT
- PMT

Plačiau šių duomenų rinkinių struktūros aprašytos atskiruose šio dokumento prieduose.

Duomenų formatas, kuriuo teikiami duomenys į VMI, yra XML.

Duomenų struktūros ir pradinės patikros taisyklės apibrėžiamos XML schemose – XSD.

Duomenų teikimo būdas – SOAP protokolu, žiniatinklio paslauga. Duomenis teikiantis subjektas kviečia atitinkamus VMI žiniatinklio paslaugos metodus duomenų teikimui ir duomenų apdorojimo rezultatų gavimui. Naudojama duomenų rinkinių koduotė – UTF-8.

Tikslinimo/aktualizavimo principas – atskiromis dalimis („įrašais“, blokais, ataskaitomis). Kiekviena dalis yra identifikuojama unikaliu identifikatoriumi, kuris yra naudojamas duomenų dalies tikslinimui, ar anuliavimui.

Duomenų elementų pavadinimai ir struktūra, kiek įmanoma ir prasminga sutapatinama su CRS elementų pavadinimais bei struktūra, taikomos CRS tikslinimo taisyklės.

Bendrų duomenų struktūrų aprašymui yra naudojamos bendrosios visos posistemės XML schemas:

- IsoTypesSti;
- CommonTypesSti;
- StatusSti.

Specifinių konkrečios duomenų rinkinių grupės duomenų struktūrų aprašymui yra naudojamos specifinės tų rinkinių XML schemas, pvz.:

- M55TypesSti;
- CrsTypesSti;
- FtcTypesSti;
- CbcTypesSti.
- FpiTypesSti,
- IvaTypesSti;
- GdrTypesSti;
- FprTypesSti.

Kiekvieno konkretaus duomenų rinkinio duomenų struktūrų aprašymui naudojama atskira XML schema, galimai naudojanti bendruosius posistemės arba rinkinių grupės duomenų tipus. Tokių schemų pvz.:

M55Sipl;
M55Slik;
M55Skis,
CRS-DAC2-LT;
FATCA-LT;
CBC-DAC4-LT;
PALUK-ISMOK;
TARP-IV-APSK;
GDR-ISMOK;
FIN-PR-PERL,

TARP-PASK,
MoQ.
DAC6-LT
TARP-GYV-PAJ
MMR-SASK
DPI-DAC7-LT
PMT

2.4 Duomenų teikimo prisijungimo nuorodos

Testavimui skirtus duomenis galima teikti, parengus duomenų paketą ir prisijungus su VMI užregistruotu skaitmeniniu sertifikatu (žr.3 sk.), jungiantis šiuo URL:

<https://ties.vmi.lt/TIESWebServiceDemo/TIESService?wsdl>

Realius duomenis galima teikti, parengus duomenų paketą ir prisijungus su VMI užregistruotu skaitmeniniu sertifikatu (žr.3 sk.), jungiantis šiuo URL:

<https://ties.vmi.lt/TIESWebService/TIESService?wsdl>

2.5 Duomenų teikimo failų dydžio apribojimai

Duomenų teikimui taikomi tokie paruošto XML failo maksimalaus dydžio (nesuarchyvuoto failo) apribojimai: XML failas turi būti ne didesnis nei 200MB.

3 Saugos reikalavimai

Žiniatinklio paslaugų metodus gali kviesti tik tie Duomenų teikėjai, kurie registruoti VMI TIES portale kaip duomenų teikėjai, turintys teisę teikti konkrečius duomenų rinkinius.

Realizuojant žiniatinklio paslaugas bus užtikrinamas WS-Security reikalavimų atitikimas.

Duomenų gavėjui duomenys teikiami pasirašyti sertifikatu, užšifruoti ir suarchyvuoti. Duomenų pasirašymo, užšifravimo ir archyvavimo reikalavimai galioja tiek į VMI teikiams duomenims, tiek iš VMI gaunamiems duomenims (pvz., atsakymams apie priėmimą/nepriėmimą).

Kai kurie duomenų rinkiniai gali turėti požymį, kad jų duomenis leidžiama teikti ir neužšifruotus, tokiu atveju tokie duomenys gali būti teikiami tiek šifruoti (kaip aprašyta aukščiau), tiek nešifruoti – tokiu atveju jie teikiami suarchyvuoti (bet neužšifruoti), taigi tokiu atveju ir atsakymas bus teikiamas neužšifruotas.

3.1 Reikalavimai skaitmeniniam sertifikatui

Duomenų teikėjų IS autentifikavimui bei siunčiamų duomenų paketų pasirašymui bus naudojamas skaitmeninis sertifikatas, išduotas ir patvirtintas tiek patikimos (angl. trusted) sertifikavimo tarnybos (angl. certificate authority), tiek išduotas įstaigos vidinės sertifikavimo tarnybos. Prieš pradėdami duomenų teikimo procesą duomenų teikėjų atstovai VMI TIES portalo sertifikatų administravimo srityje turės užregistruoti teikėjo sistemos viešą raktą, kuris bus naudojamas autentifikuojant teikėjo sistemą VMI duomenų teikimo platformoje bei atrakinant ir patikrinant atsiųstą duomenų paketą.

VMI viešąjį raktą bus galima atsisiųsti iš VMI TIES portalo.

Palaikomas skaitmeninio sertifikato formatas - DER (angl. Distinguished Encoding Rules) binary X.509. Rakto stiprumas – 2048 bit.

Raktų generavimą rekomenduojama atlikti pasinaudojus vieša programine įranga OpenSSL

3.2 Duomenų paketo parengimo žingsniai

Duomenis teikiantis duomenų teikėjas (IS) turi parengti siunčiamą duomenų rinkinį. Parengimui atliekami šie žingsniai – jei teikiamas šifruotas paketas:

Žingsnio aprašymas	Rezultatas
1. Sukurti duomenų paketo failą	
1.1. Paruošti konkretaus duomenų rinkinio XML failą, jį validuoti pagal XML schemą (XSD) ir pasirašyti: - Sukurti SHA2-256 maišos reikšmę (hash) - Naudojant siuntėjo 2048 bitų privatųjį raktą, kuris sudaro porą su siuntėjo viešuoju raktu, pasirašyti RSA skaitmeniu parašu. 1.2. Skaitmeninis parašas turi būti įtrauktas į XML failą, naudojant „Enveloping“ parašo tipą (pats duomenų paketas įtrauktas į <Object> elemento vidų).	SenderID_Payload.xml, kur SenderID – Siuntėjo identifikatorius – (MM kodas arba kitas identifikacinis numeris iki 11 skaitmenų, esant trumpesniai papildomas nuliais iš kairės iki 11 skaitmenų). Pavyzdys: 00333333333_Payload.xml
1.3. Suarchyvuoti XML failą	00000000000_Payload.zip
1.4. Užšifruoti XML failą su AES-256 raktu - Cipher mode: CBC - Salt: No salt - Pradinis vektorius (PV): 16 byte IV - Key size: 256 bits/32 bytes - Encoding: None - Padding: PKCS#5 or PKCS#7	00000000000_Payload
2. Užšifruoti AES rakto failą	
2.1. Užšifruoti AES raktą ir pradinį vektorių (PV) (48 bytes total – 32 byte AES key and 16 byte PV) su VMI viešuoju raktu. - Padding: PKCS#1 v1.5 - Key size: 2048 bits	00000000000_Key
3. Sukurti galutinį paketą, kuris bus siunčiamas	
3.1. Suarchyvuoti failus 00000000000_Payload ir 00000000000_Key	UTC_SenderID.zip Pavyzdys: 2016011516304532Z_00000000000.zip

Duomenis teikiantis duomenų teikėjas (IS) turi parengti siunčiamą duomenų rinkinį. Parengimui atliekami šie žingsniai – jei teikiamas nešifruotas paketas:

Žingsnio aprašymas	Rezultatas
1. Sukurti duomenų paketo failą	
1.1. Paruošti konkretaus duomenų rinkinio XML failą, jį validuoti pagal XML schemą (XSD)	SenderID_Payload.xml, kur SenderID – Siuntėjo identifikatorius – (MM kodas arba kitas identifikacinis numeris iki 11 skaitmenų, esant trumpesniui papildomas nuliais iš kairės iki 11 skaitmenų). Pavyzdys: 0033333333_Payload.xml
2. Sukurti galutinį paketą, kuris bus siunčiamas	
2.1. Suarchyvuoti failą 0000000000_Payload (kur 0000000000 SenderID)	UTC_SenderID.zip Pavyzdys: 201601151630453Z_0000000000.zip

3.3 Duomenų paketo išpakavimo žingsniai

Duomenis gavusi IS turi išpakuoti gautą duomenų paketą. Išpakavimui atliekami šie žingsniai - žingsniai – jei buvo teiktas šifruotas paketas, kurio atsakymą norima išpakuoti:

Žingsnio aprašymas	Rezultatas
1. Išarchyvuoti gautą failą	
1.1. Išarchyvuoti gautą failą UTC_SenderID.zip	0000000000_Payload ir 0000000000_Key
2. Iššifruoti AES raktą	
2.1. Iššifruoti AES raktą naudojant savo (t.y. gavėjo) privatų raktą	0000000000_Key
3. Iššifruoti XML failą	
3.1. Iššifruoti XML failą 0000000000_Payload su ankstesniame žingsnyje iššifruotu AES-256 raktu	0000000000_Payload.zip
4. Išarchyvuoti iššifruotą failą	
4.1. Išarchyvuoti iššifruotą failą 0000000000_Payload.zip	0000000000_Payload.xml
5. Patikrinti parašą	
5.1. Naudojant teikėjo (VMI) viešąjį raktą patikrinti parašą įsitikinant siuntėjo ir duomenų paketo autentiškumu.	-

Duomenis gavusi IS turi išpakuoti gautą duomenų paketą. Išpakavimui atliekami šie žingsniai - žingsniai – jei buvo teiktas nešifruotas paketas, kurio atsakymą norima išpakuoti:

Žingsnio aprašymas	Rezultatas
1. Išarchyvuoti gautą failą	
1.1. Išarchyvuoti gautą failą UTC_SenderID.zip	0000000000_Payload.xml

4 Paslaugos (WS metodai)

TIESService – žiniatinklio paslauga, kurią VMI pateikia finansų įstaigoms ar kitiems duomenų teikėjams. Ši paslauga turi tokias žemiau poskyriuose įvardintas operacijas (metodus).

4.1 Metodas „SubmitPackage“

Pavadinimas: SubmitPackage

Paskirtis/ aprašymas: Metodas skirtas duomenų paketo, skirto VMI, perdavimui.

Metodo užklausos ir rezultato struktūrą apibrėžia schema „SubmitPackage“.

Užklausos struktūrą apibrėžia schemos elementas spc:Request_Type.

Eil. Nr.	Pavadinimas	Duomenų tipas	Būtinasis (T/N)	Aprašymas
1.	MessageType	cts:StringMax30_Type	T	Metodu perduodamame pakete esančio pranešimo ar kitokios duomenų rinkmenos tipas. Pavyzdžiui, MAI55-SIPL.
2.	MessageRefID	cts:StringMax200_Type	T	Unikalus pranešimo ar kitokios rinkmenos identifikavimo numeris.
3.	ReportingPeriodEnd	Date	T	Laikotarpio pabaigos data.
4.	ReportingOrgID	cts:StringMax30_Type	T	Duomenų teikėjo ID, kuriuo duomenų mainų platformoje registruotą metodą kviečia duomenų teikėjo IS.
5.	Payload	Failas, atitinkantis konkrečiam duomenų rinkiniui apibrėžtą struktūrą.	T	Paketas, kuriame yra pasirašytas, užšifruotas ir archyvuotas pranešimas (duomenų rinkmena)

MessageType ir MessageRefID kartu unikalios apibrėžia duomenų paketą laike duomenų teikėjo pusėje.

Užklausos rezultatą apibrėžia schemos elementas spc: Response_Type (sėkmingo užklausos apdorojimo atveju), nesėkmingo užklausos apdorojimo atveju grąžinamas Fault.

Eil. Nr.	Pavadinimas	Duomenų tipas	Būtinasis (T/N)	Aprašymas
1.	ResultCode	cts:StringMax10_Type	T	Paketo apdorojimo rezultato kodas: 0 – Gerai. Kiti kodai reiškia klaidas. Galimos klaidos apibrėžtos skyriuose „5.3.1“ ir „5.3.2“.
2.	ResultDetails	cts:StringMax4000_Type	N	Paketo apdorojimo rezultato aprašymas. Privalomas klaidų atveju (ResultCode<>0).
3.	TransmissionID	cts:StringMax30_Type	N	Duomenų pateikimo fakto VMI įrašo identifikatorius, pagal kurį gaunama tolimesnio apdorojimo būsena bei rezultatas. Kritinių klaidų atveju (ResultCode<>0), kai duomenų pateikimo VMI fakto nepavyko užfiksuoti - negrąžinamas.

4.2 Metodas „GetStatus“

Pavadinimas: GetStatus

Paskirtis/ aprašymas: Metodas skirtas duomenų apdorojimo rezultato gavimui iš VMI.

Metodo užklauskos ir rezultato struktūrą apibrėžia schema „GetStatus“.

Užklauskos struktūrą apibrėžia schemos elementas sst:Request_Type.

Eil. Nr.	Pavadinimas	Duomenų tipas	Būtinas (T/N)	Aprašymas
1.	TransmissionID	cts:StringMax30_Type	T	Duomenų apdorojimo įrašo identifikatorius.

Užklauskos rezultatą apibrėžia schemos elementas sst:Response_Type (sėkmingo užklauskos apdorojimo atveju), nesėkmingo užklauskos apdorojimo atveju grąžinamas Fault:

Eil. Nr.	Pavadinimas	Duomenų tipas	Būtinas (T/N)	Aprašymas
1.	TransmissionDate	DateTime	T	Duomenų pateikimo fakto VMI data ir laikas.
2.	TransmissionID	cts:StringMax30_Type	T	Duomenų pateikimo fakto VMI įrašo identifikatorius.
3.	ResultCode	cts:StringMax10_Type	T	Paketo apdorojimo rezultato kodas: 0 – Gerai. Kiti kodai reiškia klaidas. Galimos klaidos apibrėžtos skyriuose „5.3.1“ ir „5.3.2“.
4.	ResultDetails	cts:StringMax4000_Type	N	Paketo apdorojimo rezultato aprašymas. Privalomas klaidų atveju (ResultCode<>0). Į grąžinamą rezultatą prie klaidos traukiamas ir konkrečios klaidos detalizacija (jei ji užpildyta): TI_FILE_ERRORS.DETAILS.
5.	MessageType	cts:StringMax30_Type	T	Pakete esančio pranešimo ar kitokios duomenų rinkmenos tipas. Pavyzdžiui, MAI55-SIPL.
6.	MessageRefID	cts:StringMax200_Type	T	Pakete esančio pranešimo ar kitokios rinkmenos unikalus identifikavimo numeris.
7.	Status	cts:StringMax30_Type	T	Duomenų apdorojimo būseną.
8.	StatusDate	DateTime	T	Duomenų apdorojimo būsenos nustatymo data ir laikas.
9.	Payload	Failas, atitinkantis struktūrą sst:StatusSti	N	Duomenų apdorojimo rezultatas.

4.3 Metodas „GetTransmissionInfo“

Pavadinimas: GetTransmissionInfo

Paskirtis/ aprašymas: Metodas skirtas duomenų perdavimo į VMI fakto duomenų gavimui iš VMI. Naudotina tais atvejais, kai SubmitPackage vykdymo metu perdavimo faktas VMI sistemoje užfiksuotas, tačiau dėl sisteminių priežasčių („time out“ ar kitos klaidos) duomenų teikėjas negavo TransmissionID.

Užklauskos parametrai:

Eil. Nr.	Pavadinimas	Duomenų tipas	Būtinas (T/N)	Aprašymas
1.	MessageType	cts:StringMax30_Type	T	Metodu perduodamame pakete esančio pranešimo ar kitokios duomenų rinkmenos tipas. Pavyzdžiui, MAI55-SIPL.
2.	MessageRefID	cts:StringMax200_Type	T	Unikalus pranešimo ar kitokios rinkmenos identifikavimo numeris.

Rezultato parametrai (sėkmingo užklauskos apdorojimo atveju), nesėkmingo užklauskos apdorojimo atveju grąžinamas Fault:

Eil. Nr.	Pavadinimas	Duomenų tipas	Būtinas (T/N)	Aprašymas
1.	TransmissionDate	DateTime	T	Duomenų pateikimo fakto VMI data ir laikas.
2.	TransmissionID	cts:StringMax30_Type	T	Duomenų pateikimo fakto VMI įrašo identifikatorius.
3.	ResultCode	cts:StringMax10_Type	T	Paketo apdorojimo rezultato kodas: 0 – Gerai. Kiti kodai reiškia klaidas. Galimos klaidos apibrėžtos skyriuose „5.3.1“ ir „5.3.2“.
4.	ResultDetails	cts:StringMax4000_Type	N	Paketo apdorojimo rezultato aprašymas. Privalomas klaidų atveju (ResultCode<>0). Į grąžinamą rezultatą prie klaidos traukiamas ir konkrečios klaidos detalizacija (jei ji užpildyta): TI_FILE_ERRORS.DETAILS.
5.	MessageType	cts:StringMax30_Type	T	Pakete esančio pranešimo ar kitokios duomenų rinkmenos tipas. Pavyzdžiui, MAI55-SIPL.
6.	MessageRefID	cts:StringMax200_Type	T	Pakete esančio pranešimo ar kitokios rinkmenos unikalus identifikavimo numeris.
7.	Status	cts:StringMax30_Type	T	Duomenų apdorojimo būseną.
8.	StatusDate	DateTime	T	Duomenų apdorojimo būsenos nustatymo data ir laikas.
9.	Payload	Failas, atitinkantis struktūrą sst:StatusSti	N	Duomenų apdorojimo rezultatas.

4.4 Metodas „GetTransmissionsByDate“

Pavadinimas: GetTransmissionsByDate

Paskirtis/ aprašymas: Metodas skirtas duomenų perdavimo į VMI faktų už laikotarpį duomenų gavimui iš VMI.

Užklauskos parametrai:

Eil. Nr.	Pavadinimas	Duomenų tipas	Būtinas (T/N)	Aprašymas
1.	TransmissionDateFrom	DateTime	T	Duomenų pateikimo fakto VMI laikotarpio pradžios data ir laikas.

2.	TransmissionDateTo	DateTime	N	Duomenų pateikimo fakto VMI laikotarpio pabaigos data ir laikas.
3.	MessageType	cts:StringMax30_Type	N	Pranešimo ar kitokios duomenų rinkmenos tipas. Pavyzdžiui, MAI55-SIPL. Nenurodžius atrenkami visų tipų pranešimų teikimai.

Rezultato (sąrašo) parametrai (sėkmingo užklausos apdorojimo atveju), nesėkmingo užklausos apdorojimo atveju grąžinamas Fault:

Eil. Nr.	Pavadinimas	Duomenų tipas	Būtinasis (T/N)	Aprašymas
1.	TransmissionDate	DateTime	T	Duomenų pateikimo fakto VMI data ir laikas.
2.	TransmissionID	cts:StringMax30_Type	T	Duomenų pateikimo fakto VMI įrašo identifikatorius.
3.	ResultCode	cts:StringMax10_Type	T	Paketo apdorojimo rezultato kodas: 0 – Gerai. Kiti kodai reiškia klaidas. Galimos klaidos apibrėžtos skyriuose „5.3.1“ ir „5.3.2“.
4.	ResultDetails	cts:StringMax4000_Type	N	Paketo apdorojimo rezultato aprašymas. Privalomas klaidų atveju (ResultCode<>0). Į grąžinamą rezultatą prie klaidos traukiamas ir konkretios klaidos detalizacija (jei ji užpildyta): TI_FILE_ERRORS.DETAILS.
5.	MessageType	cts:StringMax30_Type	T	Pakete esančio pranešimo ar kitokios duomenų rinkmenos tipas. Pavyzdžiui, MAI55-SIPL.
6.	MessageRefID	cts:StringMax200_Type	T	Pakete esančio pranešimo ar kitokios rinkmenos unikalus identifikavimo numeris.
7.	Status	cts:StringMax30_Type	T	Duomenų apdorojimo būseną.
8.	StatusDate	DateTime	T	Duomenų apdorojimo būsenos nustatymo data ir laikas.

4.5 Metodas „CancelPackage“

Pavadinimas: CancelPackage

Paskirtis/ aprašymas: Metodas skirtas perduoti į VMI duomenų paketo atšaukimui. Galima atšaukti tik tokį paketą, kurio būsena (Status) yra „Pateiktas“, o kiti jo apdorojimo veiksmai dar neatlikti. Sėkmingai atšaukus paketą, jo būsena (Status) nustatoma į „Atšauktas“, kiti jo apdorojimo veiksmai nebus atliekami.

Užklausos parametrai:

Eil. Nr.	Pavadinimas	Duomenų tipas	Būtinasis (T/N)	Aprašymas
1.	TransmissionID	cts:StringMax30_Type	T	Duomenų pateikimo fakto VMI įrašo identifikatorius.
2.	MessageType	cts:StringMax30_Type	T	Pakete esančio pranešimo ar kitokios duomenų rinkmenos tipas. Pavyzdžiui, MAI55-SIPL.

3.	MessageRefID	cts:StringMax200_Type	T	Pakete esančio pranešimo ar kitokios rinkmenos unikalus identifikavimo numeris.
----	--------------	-----------------------	---	---

Rezultato parametrai (sėkmingo užklausos apdorojimo atveju), nesėkmingo užklausos apdorojimo atveju grąžinamas Fault:

Eil. Nr.	Pavadinimas	Duomenų tipas	Būtinasis (T/N)	Aprašymas
1.	Status	cts:StringMax30_Type	T	Duomenų apdorojimo būseną.
2.	StatusDate	Date	T	Duomenų apdorojimo būsenos nustatymo data ir laikas.

5 Pranešimai

TIES palaiko šiuos pranešimų tipus:

MAI55-SIPL;

MAI55-SLIK;

MAI55-SKIS;

CRS-DAC2-LT;

FATCA-LT;

CBC-DAC4-LT;

Status-Sti (apdorojimo atsakymo pranešimas, gaunamas į TIES iš apdorojančios sistemos);

PALUK-ISMOK;

TARP-IV-APSK;

GDR-ISMOK;

FIN-PR-PERL,

TARP-PASK;

TARP-GYV-PAJ

MMR-SASK

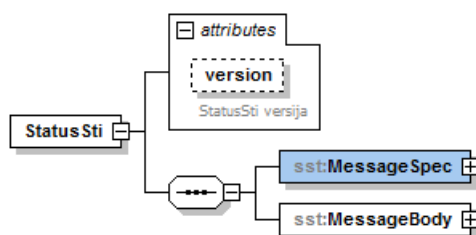
DPI-DAC7-LT

PMT

MAI55-SIPL, MAI55-SKIS ir MAI55-SLIK, CRS-DAC2-LT, FATCA-LT, CBC-DAC4-LT, PALUK-ISMOK, TARP-IV-APSK, GDR-ISMOK, TARP_PASK, MoQ, DAC6-LT, TARP-GYV-PAJ, MMR-SASK, DPI-DAC7-LT, PMT dokumentuoti atskiruose dokumento prieduose. Status-Sti apibrėžtas žemiau esančiame skyriuje.

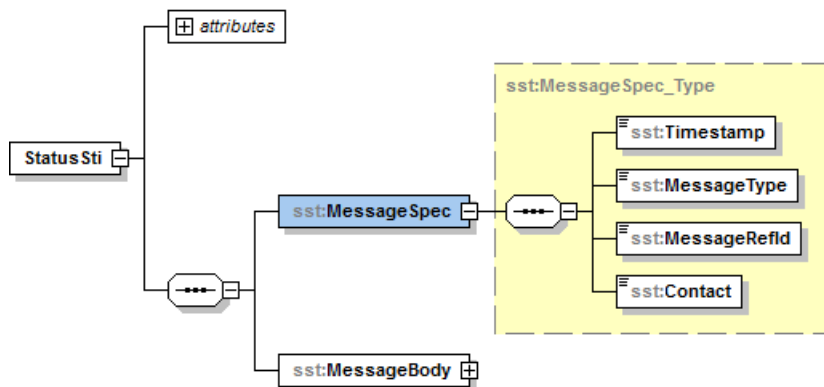
5.1 Status-Sti

Šio tipo pranešimas pateikia atsakymus apie pranešimu perduoto duomenų rinkinio priėmimą/nepriėmimą. Tai yra šis pranešimas gaunamas į TIES iš duomenis apdorojančios sistemos. Juo perduodami atitinkamo duomenų rinkinio duomenų apdorojimo rezultatai.



5.1.1 Antraštės dalis

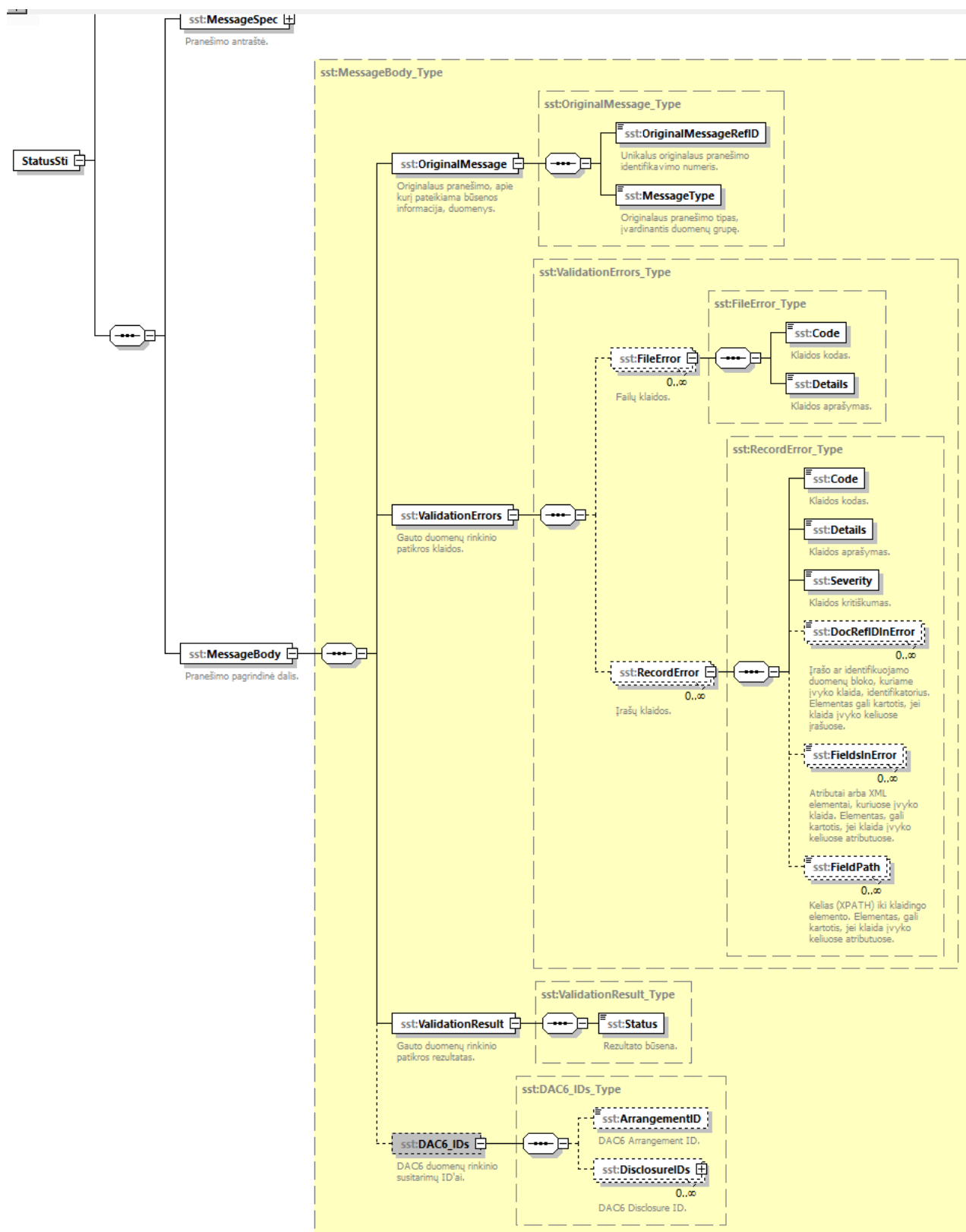
Elemento indeksas	Privalomumas	Elemento pavadinimas (anglų kalba)	Elemento trumpas aprašas	Elemento aprašas	Elemento formatas
1.1.	T	Version	Versija	Pranešimo XML struktūrų aprašo versija.	
1.2.	T	Timestamp	Suformavimo data ir laikas	Pranešimo suformavimo data ir laikas.	Data su laiku
1.3.	T	MessageType	Pranešimo tipas	Pranešimo tipas, įvardinantis duomenų grupę. Visada pildoma "Status-Sti".	30 simbolių eilutė
1.4.	T	MessageRefId	Pranešimo numeris	Unikalus pranešimo identifikavimo numeris	200 simbolių eilutė, sudaryta iš skaičių, lotyniškų raidžių bei "_ " (pabraukimo)
1.5	N	Contact	Kontakinė informacija	VMI darbuotojų kontaktinė informacija.	4000 simbolių eilutė



5.1.2 Pagrindinė dalis

Elemento indeksas	Privalomumas	Elemento pavadinimas (anglų kalba)	Elemento trumpas aprašas	Elemento aprašas	Elemento formatas
1.1.	T	OriginalMessage	Originalus pranešimas	Originalaus pranešimo, apie kurį pateikiama būsenos informacija, duomenys.	

Elemento indeksas	Privalomumas	Elemento pavadinimas (anglų kalba)	Elemento trumpas aprašas	Elemento aprašas	Elemento formatas
1.1.1	T	OriginalMessageRefID	Originalaus pranešimo identifikatorius	Unikalus originalaus pranešimo identifikavimo numeris.	200 simbolių eilutė
1.1.2	T	MessageType	Originalaus pranešimo tipas	Originalaus pranešimo tipas, įvardinantis duomenų grupę.	30 simbolių eilutė
1.2.	N	ValidationErrors	Patikros klaidos	Gauto duomenų rinkinio patikros klaidos.	
1.2.1	N	FileError	Failų klaidos	Failo lygio (viso pranešimo) klaidos.	
1.2.1.1	T	Code	Klaidos kodas	Klaidos kodas.	10 simbolių eilutė
1.2.1.2	T	Details	Klaidos aprašymas	Klaidos aprašymas.	4000 simbolių eilutė
1.2.2	N	RecordError	Įrašų klaidos	Įrašų klaidos.	
1.2.2.1	T	Code	Klaidos kodas	Klaidos kodas.	10 simbolių eilutė
1.2.2.2	T	Details	Klaidos aprašymas	Klaidos aprašymas.	4000 simbolių eilutė
1.2.2.3	T	Severity	Klaidos kritiškumas	1 – kritinė klaida dėl kurios atmetamas visas pranešimas MessageRefId su visais DocRefId; 2 – įrašo klaida, kai visas pranešimas MessageRefId priimamas, tačiau klaidingą DocRefId reikia tikslinti ir teikti kaip korekciją;	1 simbolis
1.2.2.4	N	DocRefIDInError	Klaidingų įrašų identifikatoriai	Įrašo ar identifikuojamo duomenų bloko, kuriame įvyko klaida, identifikatorius. Elementas gali kartotis, jei klaida įvyko keliuose įrašuose.	200 simbolių eilutė
1.2.2.5	N	FieldsInError	Klaidingi atributai	Atributai arba XML elementai, kuriuose įvyko klaida. Elementas, gali kartotis, jei klaida įvyko keliuose atributuose.	400 simbolių eilutė
1.2.2.6	N	FieldPath	Kelias iki klaidingo elemento	Kelias (XPATH) iki klaidingo elemento. Elementas, gali kartotis, jei klaida įvyko keliuose atributuose.	400 simbolių eilutė
1.3	T	ValidationResult	Patikros rezultatas	Gauto duomenų rinkinio patikros rezultatas.	
1.3.1	T	Status	Būsena	Rezultato būsena: Accepted – Priimtas (Gali būti priimtas pranešimas, tačiau jei yra RecordError dalyje užfiksuotų klaidų įrašams DocRefIDInError, tuomet juos reikia tikslinti generuojant naują DocRefId patikslintų duomenų teikimui, ir pradinį koreguojamą nurodant CorrDocRefId). Rejected – Atmestas. (Visas pranešimas su visais DocRefId atmestas.)	Simbolių eilutė
1.4	N	DAC6_IDs	DAC6 duomenų rinkinio susitarimų ID'ai	Rinkiniais DAC6 aktualūs susitarimų ID'ai: ArrangementID ir DisclosureID.	
1.4.1	N	ArrangementID		Susitarimo identifikatorius	17 simbolių eilutė
1.4.2	N	DisclosureIDs		Susitarimų identifikatoriai	
1.4.2.1	T	DocRefId		Ataskaitos identifikatorius	200 simbolių eilutė
1.4.2.2	T	DisclosureID		Susitarimo identifikatorius	17 simbolių eilutė



5.2 Bendrai naudojami paprastieji duomenų tipai

Bendrai naudojami duomenų tipai apibrėžti šio dokumento prieduose.

5.3 Bendrieji klasifikatoriai

Šiame skyriuje aprašyti bendrieji klasifikatoriai, kuriuos numatoma naudoti visuose ar daugelyje rinkinių, teikiamų per TIES, ar rinkinių teikimui naudojamuose WS metoduose.

Pranešimų MAI55-SLIK, MAI55-SIPL, MAI55-SKIS XSD schemų aprašymuose (pateikti šios reikalavimų specifikacijos prieduose) kaip atitinkamų laukų galimų reikšmių sąrašai yra išvardinti klasifikatoriai, naudojami MAI55 rinkiniuose.

Pranešimų CRS-DAC2-LT XSD schemų aprašymuose (pateikti šios reikalavimų specifikacijos prieduose) kaip atitinkamų laukų galimų reikšmių sąrašai yra išvardinti klasifikatoriai, naudojami CRS rinkiniuose.

Pranešimų FATCA-LT XSD schemų aprašymuose (pateikti šios reikalavimų specifikacijos prieduose) kaip atitinkamų laukų galimų reikšmių sąrašai yra išvardinti klasifikatoriai, naudojami FTC rinkiniuose.

Pranešimų CBC-DAC4-LT XSD schemų aprašymuose (pateikti šios reikalavimų specifikacijos prieduose) kaip atitinkamų laukų galimų reikšmių sąrašai yra išvardinti klasifikatoriai, naudojami CBC rinkiniuose.

Pranešimų PALUK-ISMOK XSD schemų aprašymuose (pateikti šios reikalavimų specifikacijos prieduose) kaip atitinkamų laukų galimų reikšmių sąrašai yra išvardinti klasifikatoriai, naudojami FPI rinkiniuose.

Pranešimų TARP-IV-APSK XSD schemų aprašymuose (pateikti šios reikalavimų specifikacijos prieduose) kaip atitinkamų laukų galimų reikšmių sąrašai yra išvardinti klasifikatoriai, naudojami IVA rinkiniuose.

Pranešimų GDR-ISMOK XSD schemų aprašymuose (pateikti šios reikalavimų specifikacijos prieduose) kaip atitinkamų laukų galimų reikšmių sąrašai yra išvardinti klasifikatoriai, naudojami GDR rinkiniuose.

Pranešimų FIN-PR-PERL XSD schemų aprašymuose (pateikti šios reikalavimų specifikacijos prieduose) kaip atitinkamų laukų galimų reikšmių sąrašai yra išvardinti klasifikatoriai, naudojami FPR rinkiniuose.

Pranešimų TARP_PASK XSD schemų aprašymuose (pateikti šios reikalavimų specifikacijos prieduose) kaip atitinkamų laukų galimų reikšmių sąrašai yra išvardinti klasifikatoriai, naudojami TP rinkiniuose.

Pranešimų MoQ XSD schemų aprašymuose (pateikti šios reikalavimų specifikacijos prieduose) kaip atitinkamų laukų galimų reikšmių sąrašai yra išvardinti klasifikatoriai, naudojami TP rinkiniuose.

Pranešimų DAC6-LT XSD schemų aprašymuose (pateikti šios reikalavimų specifikacijos prieduose) kaip atitinkamų laukų galimų reikšmių sąrašai yra išvardinti klasifikatoriai, naudojami TP rinkiniuose.

Pranešimų TARP-GYV-PAJ XSD schemų aprašymuose (pateikti šios reikalavimų specifikacijos prieduose) kaip atitinkamų laukų galimų reikšmių sąrašai yra išvardinti klasifikatoriai, naudojami TGP rinkiniuose.

Pranešimų DPI-DAC7-LT XSD schemų aprašymuose (pateikti šios reikalavimų specifikacijos prieduose) kaip atitinkamų laukų galimų reikšmių sąrašai yra išvardinti klasifikatoriai, naudojami DPI rinkiniuose.

Pranešimų Payment data (CESOP) XSD schemų aprašymuose (pateikti šios reikalavimų specifikacijos prieduose) kaip atitinkamų laukų galimų reikšmių sąrašai yra išvardinti klasifikatoriai, naudojami PMT rinkiniuose.

5.3.1 Paketo I lygio klaidų kodai

Kodas	Pavadinimas (Lt)	Aprašas (Lt)
10001	Trūksta teisių vykdyti veiksmui	Nepavyko autorizuoti duomenų teikėjo vykdomam veiksmui, trūksta teisių.
10002	Nekorektiška parametro MessageType reikšmė	Nepateikta ar nekorektiška parametro MessageType reikšmė
10003	Nekorektiška parametro MessageRefID reikšmė	Nepateikta ar nekorektiška parametro MessageRefID reikšmė
10004	Nekorektiška parametro ReportingPeriodEnd reikšmė	Nepateikta ar nekorektiška parametro ReportingPeriodEnd reikšmė

Kodas	Pavadinimas (Lt)	Aprašas (Lt)
10005	Viršyta failo dydžio riba	Viršyta teikiamo failo dydžio leistina riba, teikiamas per didelis failas.
10006	Toks paketas jau buvo teiktas (pagal MessageType ir MessageRefID)	Pažeistas unikalumas pagal MessageType ir MessageRefID. Toks teikėjo paketas jau buvo teiktas.
10007	Negalima parametro MessageType reikšmė ataskaitiniam laikotarpiui ReportingPeriodEnd	Negalima (negaliojanti) parametro MessageType reikšmė ataskaitiniam laikotarpiui, nurodytam parametre ReportingPeriodEnd
10008	Tokio duomenų tipo (MessageType) duomenys negali būti teikiami nešifruoti, o teikiamame pakete surastas neužšifruotas ...Payload.xml failas.	Leidžiama teikti neužšifruotus tik tuos duomenų rinkinius, kurie TIES duomenų rinkinių klasifikatoriuje turi požymį – kad leidžiama teikti ir nešifruotus. Dabar teikiamas duomenų rinkinys tokio požymio neturi, bet teikiamas duomenų paketas, kuris turi neužšifruotą failą „..._Payload.xml“, todėl pagal šio failo neužšifruotą formatą sprendžiama, kad bandoma teikti neužšifruotus duomenis.

5.3.2 Paketo II lygio klaidų kodai

Kodas	Pavadinimas (Lt)	Aprašas (Lt)
20001	Nekorektiškas paketo zip failas	Duomenų gavėjui nepavyko išpakuoti zip arba nerastas Key/Payload failas.
20002	Nepavyko iššifruoti AES rakto	Duomenų gavėjui nepavyko iššifruoti AES rakto 000000000000_Key
20003	Nepavyko iššifruoti Payload failo	Duomenų gavėjui nepavyko iššifruoti gauto failo 000000000000_Payload į 000000000000_Payload.zip
20004	Nekorektiškas Payload zip failas	Duomenų gavėjui nepavyko išpakuoti gauto failo 000000000000_Payload.zip į 000000000000_Payload.xml
20005	Nepavyko patikrinti xml pranešimo skaitmeninio parašo (iki 2022-06-14)	Duomenų gavėjui nepavyko patikrinti xml pranešimo skaitmeninio parašo su teikėjo viešuoju raktu.
20006	Nekorektiška xml pranešimo struktūra	Pranešimas neatitinka XML schemeje numatytos struktūros
20007	Nesutampa pranešimo tipas	Pranešime įrašytas pranešimo tipas (MessageType) nesutampa su nurodytu pateikiant duomenų paketą
20008	Nesutampa pranešimo identifikacinis numeris	Pranešime įrašytas pranešimo unikalus identifikavimo numeris (MessageRefID) nesutampa su nurodytu pateikiant duomenų paketą
20009	Nesutampa laikotarpio pabaigos data	Pranešime įrašyta ataskaitinio laikotarpio pabaigos data (ReportingPeriodEnd) nesutampa su nurodyta pateikiant duomenų paketą
20010	Iššifruotas failas nėra XML skaitmeniniu parašu pasirašytas XML failas	Duomenų gavėjui nepavyko patikrinti xml pranešimo skaitmeninio parašo su teikėjo viešuoju raktu. Iššifruotas failas nėra XML skaitmeniniu parašu pasirašytas XML failas
20011	XML pranešimo skaitmeninis parašas pasirašytas netinkamu algoritmu	Duomenų gavėjui nepavyko patikrinti xml pranešimo skaitmeninio parašo su teikėjo viešuoju raktu. XML pranešimo skaitmeninis parašas pasirašytas netinkamu algoritmu

Kodas	Pavadinimas (Lt)	Aprašas (Lt)
20012	XML pranešimo skaitmeninio parašo DigestValue reikšmė netinkama	Duomenų gavėjui nepavyko patikrinti xml pranešimo skaitmeninio parašo su teikėjo viešuoju raktu. XML pranešimo skaitmeninio parašo DigestValue reikšmė netinkama
20013	XML pranešimo skaitmeninio parašo SignatureValue reikšmė netinkama	Duomenų gavėjui nepavyko patikrinti xml pranešimo skaitmeninio parašo su teikėjo viešuoju raktu. XML pranešimo skaitmeninio parašo SignatureValue reikšmė netinkama

5.3.3 ISO valstybės

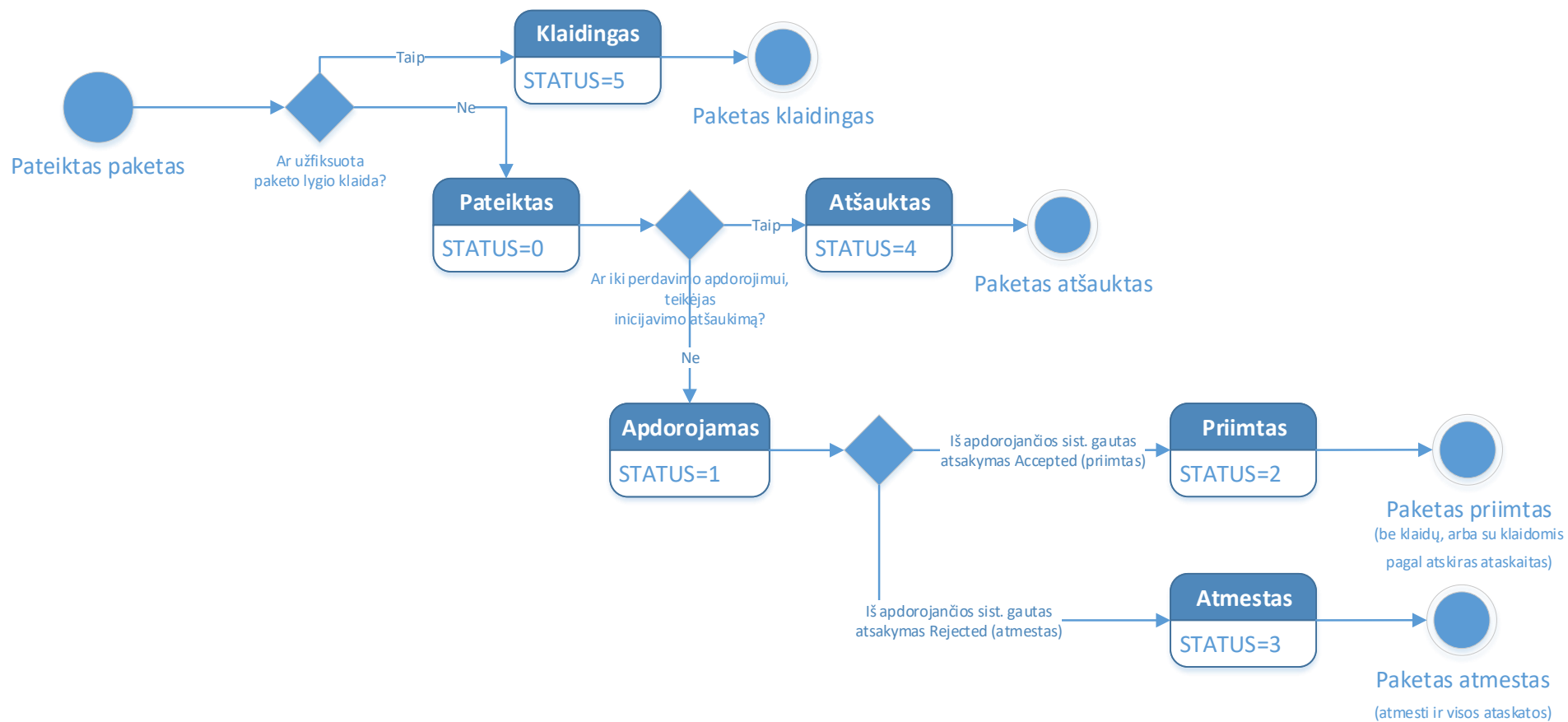
Reikšmės išvardintos XSD schemeje IsoTypesSti.

5.3.4 ISO valiutos

Reikšmės išvardintos XSD schemeje IsoTypesSti.

5.4 Paketų būsenų schema

Pateiktas paketas (tiek per duomenų teikimo integracinę sąsają, tiek įkeltas per TIES savitarnos portalą) gali įgyti žemiau schemoje pavaizduotas būsenas.



6 Priedai

6.1 Dažniausiai pasitaikančios duomenų paketo suformavimo klaidos ir jų sprendimo būdai

lentelė 6-1 – Dažniausiai pasitaikančios klaidos

Klaidos pranešimas	Galima priežastis	Sprendimo būdas
20001 - Nekorektiškas paketo zip failas	<code>{UTC}_{SenderId}.zip</code> failas negali būti išsarchyvuotas	Įsitikinti, kad zip archyvas atsidaro su populiariomis archyvavimo programomis. Patartina naudoti "Deflate" suspaudimo algoritmą.
	<code>{UTC}_{SenderId}.zip</code> archyve nerastas <code>{SenderId}_Payload</code> failas	Įsitikinti, kad galutiniame archyve yra patalpintas <code>{SenderId}_Payload</code> failas. Atkreipti dėmesį į didžiąsias/mažąsias failo pavadinimo raides.
	<code>{UTC}_{SenderId}.zip</code> archyve nerastas <code>{ReceiverID}_Key</code> failas	Įsitikinti, kad galutiniame archyve yra patalpintas <code>{ReceiverID}_Key</code> failas. Atkreipti dėmesį į didžiąsias/mažąsias failo pavadinimo raides.
20002 - Nepavyko iššifruoti AES rakto	AES raktas užšifruotas naudojant netinkamą viešąjį raktą	Įsitikinti, kad naudojamas aktualus VMI viešasis raktas , kurį atsisiųsti galima prisijungus prie TIES portalo
20003 - Nepavyko iššifruoti Payload failo	AES raktas (po sėkmingo <code>{ReceiverID}_Key</code> failo iššifravimo su VMI privačiu raktu) yra netinkamo ilgio	Įsitikinti, kad rakto faile (prieš užšifravimą) yra 48 baitų ilgio turinys . Tai yra, 32 baitų AES raktas, sujungtas su 16 baitų pradiniu vektoriumi (PV) (angl. "Initial Vector (IV)")
	<code>{SenderId}_Payload</code> failas buvo užšifruotas su AES-256 raktu, naudojant netinkamus nustatymus	Įsitikinti, kad naudojami tokie <code>{SenderId}_Payload</code> failo šifravimo su AES-256 sugeneruotu raktu nustatymai: Cipher Mode: CBC Salt: No Salt Initialization Vector: 16 byte IV Key size: 256 bits/32 bytes Encoding: None Padding: PKCS#5 or PKCS#7
20004 - Nekorektiškas Payload zip failas	<code>{SenderId}_Payload.zip</code> failas negali būti išsarchyvuotas	Įsitikinti, kad zip archyvas atsidaro su populiariomis archyvavimo programomis. Patartina naudoti "Deflate" suspaudimo algoritmą.
	<code>{SenderId}_Payload</code> failas buvo užšifruotas naudojant kitą pradinį vektorių (IV), nei pateiktą <code>{ReceiverID}_Key</code> faile	Tokiu atveju, kai <code>{SenderId}_Payload</code> failas buvo užšifruotas naudojant kitą pradinį vektorių (IV), nei pateiktą <code>{ReceiverID}_Key</code> faile, bet AES raktas pateiktas teisingas, tai <code>{SenderId}_Payload</code> failo iššifravimas įvyksta sėkmingai, tačiau gauto <code>{SenderId}_Payload.zip</code> failo pirmi 16 baitų (zip failo header dalis) būna

		neteisingi, todėl jo išarchyvuoti TIES sistemai nepavyksta.
	Simetrinio iššifravimo su pateiktu AES raktu (kai AES raktas tinkamo ilgio bei užšifruota naudojant tinkamus šifravimo nustatymus) metu 20003 klaida gali būti neaptikta, bet iššifruotas turinys neturi prasmės (pvz., pateikti AES raktas arba IV neatitinka naudotų užšifravimo metu). Tokiu atveju fiksuojama 20004 klaida.	Įsitikinti, kad pateiktame 48 baitų {ReceiverID}_Key faile yra pateiktos tos AES-256 rakto ir IV reikšmės, kurios buvo naudotos užšifravimo metu.
20005 - Nepavyko patikrinti xml pranešimo skaitmeninio parašo (iki 2022-06-22)	{SenderID}_Payload.zip faile rastas skaitmeniniu parašu pasirašytas dokumentas nėra xml failas	{SenderID}_Payload.zip archyvo faile turi būti patalpintas skaitmeniniu parašu pasirašytas xml dokumentas. Failas turi būti xml formatu, papildomai neužrakintas, nešifruotas, nepaverstas į BASE64 formatą ir pan.
	XML duomenų failas pasirašytas netinkamu XML pasirašymo algoritmu	XML skaitmeninis parašas turi būti suformuotas naudojant "Enveloping" pasirašymo algoritmą. "Enveloped" ir "Detached" algoritmais pasirašytų XML dokumentų TIES sistema nepriima. Įsitikinti, kad pasirašytame XML faile duomenų XML dalis yra <Object> elemento viduje.
	Netinkama XML skaitmeninio parašo <DigestValue> reikšmė	<DigestValue> reikšmė turi būti gauta paėmus <Object> elementą su visu duomenų XML, kuris yra <Object> elemento viduje, ir pavertus tokį XML į kanoninę formą xml-exc-c14n algoritmu. Apskaičiuota kanoninės formos XML teksto SHA256 maišos reikšmė turi būti paversta į BASE64 tekstą.
	Netinkama XML skaitmeninio parašo <SignatureValue> reikšmė	<SignatureValue> reikšmė turi būti gauta paėmus <SignedInfo> bloką su jo viduje esančiu apskaičiuotu <DigestValue> ir kitais elementais pagal aprašymą https://www.w3.org/TR/xmlsig-core/#sec-SignedInfo <SignedInfo> blokas turi būti paverstas į kanoninę formą xml-exc-c14n algoritmu. Gauta kanoninė forma turi būti užšifruota su siuntėjo privačiu raktu RAS-SHA256 algoritmu. Svarbu įsitikinti, kad privatų raktą atitinkantis viešasis raktas (sertifikatas) yra galiojantis, patalpintas į TIES portalą ir nebuvo TIES portale atšauktas.
20006 - Nekorektiška xml pranešimo struktūra	XML failas praėjo visus iššifravimo ir parašo patikros žingsnius, bet duomenys XML formatu neatitinka skelbiamų XSD schemų	Naudojant įvairias XML validavimo su XSD schemomis programas įsitikinti, kad XML failas atitinka XSD schemas. Įsitikinti, kad naudojamos naujausios xsd schemų versijos , kurias galima atsisiųsti iš TIES portalo.

20010 - Nekorektiška xml pranešimo struktūra	{SenderID}_Payload.zip faile rastas skaitmeniniu parašu pasirašytas dokumentas nėra xml failas	{SenderID}_Payload.zip archyvo faile turi būti patalpintas skaitmeniniu parašu pasirašytas xml dokumentas. Failas turi būti xml formatu, papildomai neužrakintas, nešifruotas, nepaverstas į BASE64 formatą ir pan.
20011 - XML pranešimo skaitmeninis parašas pasirašytas netinkamu algoritmu	XML duomenų failas pasirašytas netinkamu XML pasirašymo algoritmu	XML skaitmeninis parašas turi būti suformuotas naudojant "Enveloping" pasirašymo algoritmą. "Enveloped" ir "Detached" algoritmais pasirašytų XML dokumentų TIES sistema nepriima. Įsitikinti, kad pasirašytame XML faile duomenų XML dalis yra <Object> elemento viduje.
20012 - XML pranešimo skaitmeninio parašo DigestValue reikšmė netinkama	Netinkama XML skaitmeninio parašo <DigestValue> reikšmė	<DigestValue> reikšmė turi būti gauta paėmus <Object> elementą su visu duomenų XML, kuris yra <Object> elemento viduje, ir pavertus tokį XML į kanoninę formą xml-exc-c14n algoritmu. Apskaičiuota kanoninės formos XML teksto SHA256 maišos reikšmė turi būti paversta į BASE64 tekstą.
20013 - XML pranešimo skaitmeninio parašo SignatureValue reikšmė netinkama	Netinkama XML skaitmeninio parašo <SignatureValue> reikšmė	<SignatureValue> reikšmė turi būti gauta paėmus <SignedInfo> bloką su jo viduje esančiu apskaičiuotu <DigestValue> ir kitais elementais pagal aprašymą https://www.w3.org/TR/xmlsig-core/#sec-SignedInfo <SignedInfo> blokas turi būti paverstas į kanoninę formą xml-exc-c14n algoritmu. Gauta kanoninė forma turi būti užšifruota su siuntėjo privačiu raktu RAS-SHA256 algoritmu. Svarbu įsitikinti, kad privatų raktą atitinkantis viešasis raktas (sertifikatas) yra galiojantis, patalpintas į TIES portalą ir nebuvo TIES portale atšauktas.

6.2 UNIX bash script'as pasirašyto ir užšifruoto duomenų paketo sukūrimui iš xml failo

Lentelė 6-2 - test_package.sh (parametrų užpildymas)

```

1  #!/bin/bash
3
4  UNSIGNED_XML_IN=unsigned_Payload.xml
5  RECEIVER_PUBLIC_CERT_IN=tiesback.cer
6  MY_PRIVATE_KEYSTORE_PKCS12_IN=keystore.p12
7  MY_PRIVATE_KEYSTORE_PWD_IN=changeit
8  MY_PRIVATE_KEY_ALIAS=algoritmusistemas

```

```

9
10     SenderId=000000000000
11     ReceiverId=00188659752
12
13     export UNSIGNED_XML_IN RECEIVER_PUBLIC_CERT_IN MY_PRIVATE_KEYSTORE_PKCS12_IN
14     MY_PRIVATE_KEYSTORE_PWD_IN MY_PRIVATE_KEY_ALIAS SenderId ReceiverId
15     ./ties_package.sh

```

Lentelė 6-3 – ties_package.sh (pasirašyto ir užšifruoto duomenų paketo sukūrimas iš xml failo)

```

1     #!/bin/bash
2
3     #####
4     # 'openssl', 'zip' and 'xmlsec1' should be in the path.
5     # for 'xmlsec1' see https://www.aleksey.com/xmlsec
6     #####
7
8     echo "*****"
9     echo "DEFINING VARIABLES"
10    echo "*****"
11
12    echo UNSIGNED_XML_IN=$UNSIGNED_XML_IN
13    echo RECEIVER_PUBLIC_CERT_IN=$RECEIVER_PUBLIC_CERT_IN
14    echo MY_PRIVATE_KEYSTORE_PKCS12_IN=$MY_PRIVATE_KEYSTORE_PKCS12_IN
15    echo MY_PRIVATE_KEYSTORE_PWD_IN=$MY_PRIVATE_KEYSTORE_PWD_IN
16    echo MY_PRIVATE_KEY_ALIAS=$MY_PRIVATE_KEY_ALIAS
17    echo
18    echo SenderId=$SenderId
19    echo ReceiverId=$ReceiverId
20
21    echo "*****"
22
23    if [[ -z $UNSIGNED_XML_IN || -z $RECEIVER_PUBLIC_CERT_IN || -z
24    $MY_PRIVATE_KEYSTORE_PKCS12_IN || -z $MY_PRIVATE_KEYSTORE_PWD_IN || -z
25    $SenderId || -z $ReceiverId ]]; then

```

```

26     echo "please see test_package.sh....set these variables: SenderId,
ReceiverId"
27     exit 1
28 fi
29
30 if [[ ! -f $UNSIGNED_XML_IN || ! -f $RECEIVER_PUBLIC_CERT_IN || ! -f
31 $MY_PRIVATE_KEYSTORE_PKCS12_IN ]]; then
32     echo "ERROR: either $UNSIGNED_XML_IN or $RECEIVER_PUBLIC_CERT_IN or
33 $MY_PRIVATE_KEYSTORE_PKCS12_IN does not exist"
34     exit 1
35 fi
36
37 #####
38 # Define file names. DO NOT EDIT
39 #####
40
41 SenderFileId=`date -u +%Y%m%dT%H%M%S000Z`
42 FileCreateTs=`date -u +%Y-%m-%dT%H:%M:%SZ`
43
44 payload_file="${SenderId}_Payload
45 key_file="${ReceiverId}_Key
46 pkg_file="${SenderFileId}"_"${SenderId}".zip
47
48 signed_xml=`echo "${payload_file}".xml`
49 pre_sign_tmplt=`echo "${signed_xml}".tmplt`
50 compressed_signed_xml=`echo "${UNSIGNED_XML_IN}".signed.zip`
51
52 if [[ -f $signed_xml ]]; then
53     echo "ERROR: ${signed_xml} already exists"
54     exit 1
55 fi
56
57 #####
58 # GYPAS_TIES_SA 3.2      DUOMENŲ PAKETO PARENGIMO ŽINGSNIAI
59 #      1.1 - PASIRAŠYTI PARUOŠTĄ XML FAILĄ

```

```

60  #
61  #      sign xml using xmlsec1. http://www.aleksey.com/xmlsec/
62  #      - embed $UNSIGNED_XML_IN within $tmplt_prefix and $tmplt_suffix
63  #      - Resulting file $signed_xml would have structure <Object
64  #      Id="TIES">[XML]</Object>.
65  #      - Use $signed_xml and sign using 'xmlsec1'
66  #####
67
68  echo;echo "creating signature template file '$pre_sign_tmplt' for xmlsec
69  signing...."
70
71  # create signature template file after embedding xml
72  if [[ -f $pre_sign_tmplt ]]; then
73      rm -f $pre_sign_tmplt
74  fi
75
76  tmplt_prefix='<?xml version="1.0" encoding="UTF-8"
77  standalone="no"?><Signature xmlns="http://www.w3.org/2000/09/xmldsig#"
78  Id="SignatureId"><SignedInfo><CanonicalizationMethod
79  Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" /><SignatureMethod
80  Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" /><Reference
81  URI="#TIES"><Transforms><Transform Algorithm="http://www.w3.org/2001/10/xml-
82  exc-c14n#" /></Transforms><DigestMethod
83  Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" /><DigestValue/></Referen
84  ce></SignedInfo><SignatureValue/><KeyInfo><X509Data><X509Certificate/></X509
85  Data></KeyInfo><Object Id="TIES">'
86
87  tmplt_suffix='</Object></Signature>'
88
89  echo -n "$tmplt_prefix" >> $pre_sign_tmplt
90
91  is_newline_needed=0
92  xml_decl_checked=0
93  line=
94  while IFS= read -r line
95  do
96      if [[ $xml_decl_checked -eq 0 ]]; then
97          xml_decl_checked=1

```

```

90     line=`echo ${line#<?xml*>}`
91     if [[ ! -z "$line" ]]; then
92         echo -n "$line" >> $pre_sign_tmplt
93         is_newline_needed=1
94     fi
95 else
96     if [[ is_newline_needed -eq 1 ]]; then echo >> $pre_sign_tmplt; fi
97     echo -n "$line" >> $pre_sign_tmplt
98     is_newline_needed=1
99 fi
100 done < $UNSIGNED_XML_IN
101
102 #last line
103 line=`echo -n "$line"|xargs`
104 if [[ ! -z "$line" ]]; then
105     if [[ is_newline_needed -eq 1 ]]; then echo >> $pre_sign_tmplt; fi
106     echo -n "$line" >> $pre_sign_tmplt
107 fi
108
109 if [[ "$?" -ne 0 ]]; then echo "ERROR: last command failed"; exit $?; fi
110
111 echo -n "$tmplt_suffix" >> $pre_sign_tmplt
112
113 echo;echo "creating signature template file '$pre_sign_tmplt' for xmlsec
114 signing....done"
115
116 #####
117
118 echo;echo "signing '$pre_sign_tmplt' to create signed xml '$signed_xml'...."
119
120 # sign with xmlsec
121 if [[ $MY_PRIVATE_KEY_ALIAS -eq "" ]]; then
122     CMD="xmlsec1 --sign --pkcs12 $MY_PRIVATE_KEYSTORE_PKCS12_IN --pwd
123     $MY_PRIVATE_KEYSTORE_PWD_IN --output $signed_xml $pre_sign_tmplt"
124 else

```

```

124     CMD="xmlsec1 --sign --pkcs12:$MY_PRIVATE_KEY_ALIAS
125     $MY_PRIVATE_KEYSTORE_PKCS12_IN --pwd $MY_PRIVATE_KEYSTORE_PWD_IN --output
126     $signed_xml $pre_sign_tmplt"
127
128     echo;echo $CMD;$CMD
129
130
131     if [[ "$?" -ne 0 ]]; then
132         echo "!!!! please fix the error !!!!";echo $CMD;echo
133         rm -f $pre_sign_tmplt $signed_xml
134         exit 1
135     fi
136
137     echo; echo "signing '$pre_sign_tmplt' to create signed xml
138     '$signed_xml'....done"; echo
139
140     #####
141     # GYPAS_TIES_SA 3.2      DUOMENŲ PAKETO PARENGIMO ŽINGSNIAI
142     #      1.2 - SUARCHYVUOTI XML FAILĄ
143     #
144     # compress $signed_xml to $compressed_signed_xml
145     #####
146
147     echo "compressing '$signed_xml' to create '$compressed_signed_xml'...."
148
149     CMD="zip -q $compressed_signed_xml $signed_xml"
150
151     echo;echo $CMD;$CMD
152
153     if [[ "$?" -ne 0 ]]; then
154         echo "!!!! please fix the error !!!!";echo $CMD;echo
155         rm -f $pre_sign_tmplt $signed_xml $compressed_signed_xml
156         exit 1
157     fi

```

```

158
159 echo; echo "compressing '$signed_xml' to create
160 '$compressed_signed_xml'....done"; echo
161
162 #####
163 # GYPAS_TIES_SA 3.2      DUOMENŲ PAKETO PARENGIMO ŽINGSNIAI
164 #      1.3 - UŽŠIFRUOTI XML FAILĄ SU AES-256 RAKTU
165 #
166 # encrypt $compressed_signed_xml
167 #      - create 32 bytes AES key, AESKEY
168 #      - create 16 bytes Initialization Vector, IV, used for CBC encryption
169 #      - encrypt $compressed_signed_xml using CBC with $AESKEY, $IV. encrypted
170 #      - append $IV to $AESKEY and encrypt resulting $AESKEYIVBIN with
171 #      receiver's PKI public key, $RECEIVER_PUBLIC_CERT_IN. output file is
172 #      $key_file
173 #####
174
175 echo "encrypting '$compressed_signed_xml'...."
176
177 # Create 32 bytes random AES key
178 TMP=`openssl rand 32 -hex`
179 AESKEY=`echo ${TMP:0:64}`
180
181 # Create 16 bytes random Initialization Vector (IV)
182 TMP=`openssl rand 16 -hex`
183 IV=`echo ${TMP:0:32}`
184
185 echo; echo "AESKEY=$AESKEY"; echo "IV=$IV";
186
187 # Encrypt payload with key AESKEY and iv IV
188 CMD="openssl enc -e -aes-256-cbc -in $compressed_signed_xml -out
189 $payload_file -K $AESKEY -iv $IV"
190
191 echo;echo $CMD;$CMD

```



```

192  if [[ "$?" -ne 0 ]]; then
193      echo "!!!! please fix the error !!!!";echo $CMD;echo
194      rm -f $pre_sign_tmplt $signed_xml $compressed_signed_xml $payload_file
195      exit 1
196  fi
197
198  # Concatenate 32 bytes AESKEY and 16 bytes IV
199  AESKEYIV=`echo -n "$AESKEY$IV"`
200
201  # Convert AESKEY+IV hex to binary
202  AESKEYIVBIN=`echo ${key_file}.aeskeyivbin`
203
204  #echo;echo "echo -n $AESKEYIV|perl -pe '\$_=pack(\"H*\",\$_)' >
205  $AESKEYIVBIN"
206  #echo -n $AESKEYIV|perl -pe '\$_=pack("H*",\$_)' > $AESKEYIVBIN
207  echo;echo "echo -n $AESKEYIV|xxd -r -p > $AESKEYIVBIN"
208  echo -n $AESKEYIV|xxd -r -p > $AESKEYIVBIN
209
210  #####
211  # GYPAS_TIES_SA 3.2      DUOMENŲ PAKETO PARENGIMO ŽINGSNIAI
212  #      2.1 - UŽŠIFRUOTI AES RAKTĄ IR PRADINĮ VEKTORIŲ SU VMI VIEŠUOJU
213  #      RAKTU.
214  #
215  # Encrypt aeskey_iv.bin with receiver's RSA PKI public key
216  #####
217  CMD="openssl rsautl -encrypt -out $key_file -certin -inkey
218  $RECEIVER_PUBLIC_CERT_IN -keyform DER -in $AESKEYIVBIN"
219  echo;echo $CMD;$CMD
220
221  if [[ "$?" -ne 0 ]]; then
222      echo "!!!! please fix the error !!!!";echo $CMD;echo
223      rm -f $pre_sign_tmplt $signed_xml $compressed_signed_xml $payload_file
224      $AESKEYIVBIN $key_file
225      exit 1

```

```

226  fi
227
228  echo; echo "encrypting '$compressed_signed_xml'....done"; echo
229
230  #####
231  # GYPAS_TIES_SA 3.2      DUOMENŲ PAKETO PARENGIMO ŽINGSNIAI
232  #      3.1 - SUKURTI GALUTINĮ PAKETĄ, KURIS BUS SIUNČIAMAS
233  #
234  # create TIES $pkg_file which contains following files compressed
235  #      - $payload_file
236  #      - $key_file
237  #####
238
239  echo "creating pkg '$pkg_file'....."
240
241  CMD="zip -q $pkg_file $payload_file $key_file"
242
243  echo;echo $CMD;$CMD
244
245  if [[ "$?" -ne 0 ]]; then
246      echo "!!!! please fix the error !!!!";echo $CMD;echo
247      rm -f $pre_sign_tmplt $signed_xml $compressed_signed_xml $payload_file
248      $AESKEYIVBIN $key_file $pkg_file
249      exit 1
250  fi
251
252  echo; echo "creating pkg '$pkg_file'.....done"; echo
253
254  #####
255  # remove all temporary files (comment for debugging/verification)
256  #####
257
258  rm -f $pre_sign_tmplt $signed_xml $compressed_signed_xml $payload_file
259  $AESKEYIVBIN $key_file

```


6.3 UNIX bash script'as pasirašyto xml failo atkūrimui iš užšifruoto duomenų paketo

Lentelė 6-4 – test_unpack.sh (parametrų užpildymas)

```
1
2 #!/bin/bash
3
4 TIES_PKG_IN=EncryptedTIESDataPackage.zip
5 MY_PRIVATE_KEYSTORE_PKCS12_IN=server-keystore.p12
6 MY_PRIVATE_KEYSTORE_PWD_IN=changeit
7 SENDER_PUBLIC_CERT_IN=algoritmusistemas.lt.der
8
9 export TIES_PKG_IN MY_PRIVATE_KEYSTORE_PKCS12_IN MY_PRIVATE_KEYSTORE_PWD_IN
  SENDER_PUBLIC_CERT_IN
10
11 ./ties_unpack.sh
```

Lentelė 6-5 – ties_unpack.sh (duomenų paketo iššifravimas ir xml skaitmeninio parašo validavimas)

```
1 #!/bin/bash
2
3 #####
4 # 'openssl', 'unzip' and 'xmlsec1' should be in the path.
5 # for 'xmlsec1' see https://www.aleksey.com/xmlsec
6 #####
7
8 echo "*****"
9 echo "DEFINING VARIABLES"
10 echo "*****"
11
12 echo TIES_PKG_IN=$TIES_PKG_IN
13 echo MY_PRIVATE_KEYSTORE_PKCS12_IN=$MY_PRIVATE_KEYSTORE_PKCS12_IN
14 echo MY_PRIVATE_KEYSTORE_PWD_IN=$MY_PRIVATE_KEYSTORE_PWD_IN
15 echo SENDER_PUBLIC_CERT_IN=$SENDER_PUBLIC_CERT_IN
16
```

```

17 echo "*****"
18
19 if [[ -z $TIES_PKG_IN || -z $MY_PRIVATE_KEYSTORE_PKCS12_IN || -z
20 MY_PRIVATE_KEYSTORE_PWD_IN ]]; then
21     echo "please see test_unpack.sh....set at least these variables
22     TIES_PKG_IN, MY_PRIVATE_KEYSTORE_PKCS12_IN, MY_PRIVATE_KEYSTORE_PWD_IN) "
23     exit 1
24 fi
25
26 #####
27 # GYPAS_TIES_SA 3.3      DUOMENŲ PAKETO IŠPAKAVIMO ŽINGSNIAI
28 #      1.1 - IŠARCHYVUOTI GAUTĄ FAILĄ
29 #
30 # unzip TIES_PKG_IN
31 #####
32
33 if [[ ! -f $TIES_PKG_IN || ! -f $MY_PRIVATE_KEYSTORE_PKCS12_IN ]]; then
34     echo "ERROR: either $TIES_PKG_IN or $MY_PRIVATE_KEYSTORE_PKCS12_IN does
35 not exit"
36     exit 1
37 fi
38
39 echo "unzipping '$TIES_PKG_IN'...."
40
41 declare -a arr=(`unzip -Z2 ${TIES_PKG_IN}`)
42
43 i=0
44 while true; do
45     tmp=${arr[$i]#*_}
46     tmp="${tmp//${'\r'}}"
47     # Equality Comparison
48     if [[ ${tmp} = Payload ]]; then
49         payload_file=${arr[$i]}
50         payload_file="${payload_file//${'\r'}}"
51     elif [[ ${tmp} = Key ]]; then

```

```

48     key_file=${arr[$i]}
49     key_file="${key_file//$\r/}"
50 fi
51 i=$((i+1))
52 if [[ $i -eq ${#arr[@]} ]]; then
53     break;
54 fi
55 done
56
57 if [[ -z $payload_file || -z $key_file ]]; then
58     echo "invalid $TIES_PKG_IN - one or more file missing"
59     exit 1
60 fi
61
62 CMD="unzip -oq $TIES_PKG_IN"
63
64 echo;echo $CMD;$CMD
65
66 if [[ "$?" -ne 0 ]]; then
67     echo "!!!! please fix the error !!!!!";echo $CMD;echo
68     rm -f $key_file $payload_file
69     exit 1
70 fi
71
72 echo;echo "unzipping '$TIES_PKG_IN'....done"
73 echo;echo "extracting private key from keystore
74 '$MY_PRIVATE_KEYSTORE_PKCS12_IN'...."
75
76 #####
77 # GYPAS_TIES_SA 3.3      DUOMENŲ PAKETO IŠPAKAVIMO ŽINGSNIAI
78 #
79 #      2.1 - IŠŠIFRUOTI AES RAKTĄ NAUDOJANT PRIVATŲ RAKTĄ
80 #
81 # Decrypt encrypted AESKEY+IV using receiver's RSA PKI private key
82 #####

```

```

81
82 private_key_pem_file=`echo ${key_file}.pem`
83
84
85
86 CMD="openssl pkcs12 -in $MY_PRIVATE_KEYSTORE_PKCS12_IN -nocerts -passin
pass:$MY_PRIVATE_KEYSTORE_PWD_IN -nodes" > $private_key_pem_file
87
88 echo;echo "$CMD > $private_key_pem_file";$CMD > $private_key_pem_file
89
90 if [[ "$?" -ne 0 ]]; then
91     echo "!!!! please fix the error !!!!!";
92     echo;echo "$CMD > $private_key_pem_file";$CMD > $private_key_pem_file
93     rm -f $key_file $payload_file $private_key_pem_file
94     exit 1
95 fi
96
97 echo;echo "extracting private key from keystore
'$MY_PRIVATE_KEYSTORE_PKCS12_IN'....done"
98 echo;echo "decrypting '$key_file' using private key from
'$private_key_pem_file'...."
99
100 CMD="TMP=`openssl rsautl -decrypt -in $key_file -inkey $private_key_pem_file
| perl -pe '\$_=unpack("H*",\$_)'\`"
101
102 echo;echo $CMD;
103
104 TMP=`openssl rsautl -decrypt -in $key_file -inkey $private_key_pem_file|perl -
pe '\$_=unpack("H*", \$_)'\`
105
106 if [[ "$?" -ne 0 ]]; then
107     echo "!!!! please fix the error !!!!!";echo $CMD;echo
108     rm -f $key_file $payload_file $private_key_pem_file
109     exit 1
110 fi
111

```

```

108 # Extract 32 bytes AESKEY and 16 bytes IV
109 AESKEY2DECRYPT=`echo ${TMP:0:64}`
110 IV2DECRYPT=`echo ${TMP:64:96}`
111
112 #####
113 # GYPAS_TIES_SA 3.3      DUOMENŲ PAKETO IŠPAKAVIMO ŽINGSNIAI
114 #      3.1 - IŠŠIFRUOTI ARCHYVUOTĄ XML FAILĄ SU ANKSTESNIAME ŽINGSNYJE
115 IŠŠIFRUOTU AES-256 RAKTU
116 #
117 # Decrypt payload using D_AESKEY and D_IV
118 #####
119
120 payload_zip_file=`echo ${payload_file}.zip`
121 CMD="openssl enc -d -aes-256-cbc -in $payload_file -out $payload_zip_file -K
122 $AESKEY2DECRYPT -iv $IV2DECRYPT"
123
124 if [[ "$?" -ne 0 ]]; then
125     echo "!!!! please fix the error !!!!!";echo $CMD;echo
126     #rm -f $key_file $payload_file $private_key_pem_file
127     exit 1
128 fi
129 # Check if payload_zip_file are created
130 if [[ ! -f $payload_zip_file ]]; then
131     echo "!!!! please fix the error !!!!!";echo $CMD;echo
132     rm -f $key_file $payload_file $private_key_pem_file
133     exit 1
134 fi
135
136 echo;echo "decrypting '$key_file' using private key from
137 '$private_key_pem_file'....done"
138
139 #####

```



```

140 # GYPAS_TIES_SA 3.3      DUOMENŲ PAKETO IŠPAKAVIMO ŽINGSNIAI
141 #      4.1 - IŠARCHYVUOTI IŠŠIFRUOTĄ FAILĄ 000000000000_PAYLOAD.ZIP
      #
142 #####
143
144 echo;echo "unzipping '$payload_zip_file'...."
145
146 CMD="unzip -oq $payload_zip_file"
147
148 echo;echo $CMD;$CMD
149
150 payload_xml_file=${payload_file}.xml
151
152 # Check if $payload_xml_file is created
153 if [[ "$?" -ne 0 || ! -f $payload_xml_file ]]; then
154     echo "!!!! please fix the error !!!!";echo $CMD;echo
155     rm -f $key_file $payload_file $private_key_pem_file
156     exit 1
157 fi
158
159 echo;echo "unzipping '$payload_zip_file'....done"
160
161 #####
162 # GYPAS_TIES_SA 3.3      DUOMENŲ PAKETO IŠPAKAVIMO ŽINGSNIAI
163 #      5.1 - Naudojant teikėjo (VMI) viešąjį rakta patikrinti parašą
164     įsitikinant siuntėjo ir duomenų paketo autentiškumu.
165 #
166 #####
167
168 error_flag=0
169
170 if [[ ! -z $SENDER_PUBLIC_CERT_IN && -f $SENDER_PUBLIC_CERT_IN ]]; then
171     echo;echo "verifying signature of '$payload_xml_file'...."

```

```

172     CMD="xmlsec1 --verify --pubkey-cert-der $SENDER_PUBLIC_CERT_IN
173     $payload_xml_file"
174
175     echo;echo $CMD;$CMD 2>&1
176
177     if [[ "$?" -eq 0 ]]; then
178         echo;echo "'$payload_xml_file' signature verification succeed"
179     else
180         echo;echo "ERROR: '$payload_xml_file' signature verification failed"
181         error_flag=1
182     fi
183
184     echo;echo "verifying signature of '$payload_xml_file'....done"
185 fi
186
187 if [[ error_flag -eq 0 ]]; then
188     echo;echo "success!!!! unpacked $payload_xml_file"
189 fi
190
191 rm -f $key_file $payload_file $private_key_pem_file $payload_zip_file
192
193
194
195

```

6.4 Priedas Nr. 1 „Instrukcija TIES nešifruotam paketui“



R31_GYPAS_V2_TIES
_IS_priedas1_v0.2.dc

6.5 Priedas Nr. 2 „Instrukcija TIES paketui openssl notepad“



R31_GYPAS_V2_TIES
_IS_priedas2_v0.6.pc