VALSTYBINĖ MOKESČIŲ INSPEKCIJA PRIE LIETUVOS RESPUBLIKOS FINANSŲ MINISTERIJOS

TIES VMI duomenų mainų posistemis

Duomenų teikimo sąsajos aprašas

Versija: 2.15

VILNIUS
2018-09-06

KEITIMŲ CHRONOLOGIJA

Versija	Data	Pakeitimas	Pakeisti skyriai
0.1	2016-05-23	Pradinė versija	visi
0.2	2016-05-27	Dokumentas papildytas MAI55-SKIS rinkinio aprašymu.	2, 5, 7
0.3	2016-06-13	Patikslinta pagal Užsakovo pastabas	1.3, 2.3
0.4	2016-06-16	Ištaisyta lentelių eilučių numeracija, patikslintas TIES pranešimų tipų sąrašas	4.3, 5
0.5	2016-10-04	Pakeitimai, pagal naujo tipo CRS-DAC2-LT pranešimų apdorojimą, surenkant informaciją apie užsienio šalių piliečių sąskaitas Lietuvos finansinėse institucijose.	visi
1.0	2017-01-03	Patvirtinta dokumento versija	-
2.0	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.
2.1	2017-02-02	Ištaisyta klaida dėl supainiotų nuorodų duomenų teikimui testavimui ir realių duomenų.	2.4 sk.
2.2	2017-04-14	Papildyta metodais „GetTransmitionsByDate“, „CancelPackage“, parametrais, klaidomis.	4, 5
2.3	2017-04-14	Papildyta TIES išorinio portalo (savitarnos) galimų funkcijų išvardinimu.	2.2 sk.
2.4	2017-05-31	Patikslinta skaitmeninio parašo suformavimo procedūra	3.2 sk.
2.5	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.
2.6	2017-09-25	Papildyta nauju duomenų rinkiniu „FATCA-LT“ surenkant duomenis apie JAV rezidentų sąskaitas iš FĮ.	visi
2.7	2017-10-12	Papildyta nauju duomenų rinkiniu „CBC-DAC4-LT“ surenkant duomenis apie TĮG (tarptautinių įmonių grupių) ataskaitas	visi
2.8	2017-10-16	Patikslinta pagal apibendrintus duomenų teikėjus.	visi
2.9	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.
2.10	2017-10-31	Skyrius „Dažniausiai pasitaikančios duomenų paketo suformavimo klaidos ir jų sprendimo būdai“ papildytas nauju atveju dėl 20004 klaidos.	6.1 sk.
2.11	2018-01-03	Papildyta nauju duomenų rinkiniu „PALUK-ISMOK“ surenkant duomenis apie finansinių įstaigų gyventojams išmokėtas palūkanas	visi
2.12	2018-01-30	Papildyta nauju duomenų rinkiniu „TARP-IV-APSK“ surenkant duomenis apie individualios veiklos apskaitą.	1; 2; 5.2.
2.13	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.
2.14	2018-03-08	Papildyta nauju duomenų rinkiniu „FIN-PR-PERL“ surenkant duomenis apie finansinių priemonių perleidimus gyventojams.	1; 2; 5.2.
2.15	2018-09-03	Patikslintos 20004 klaidos dažniausiai pasitaikančios priežastys	6.1

TURINYS

1 Įvadas

1.1 Dokumento paskirtis ir sudėtis

Šio 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 posistemiu 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:

„MAI55 pranešimų XML schemos aprašymas“.

„CRS-DAC2-LT pranešimų XML schemos aprašymas“

„FATCA-LT pranešimų XML schemos aprašymas“

„CBC-DAC4-LT pranešimų XML schemos aprašymas“

„PALUK-ISMOK pranešimų XML schemos aprašymas“

„TARP-IV-APSK pranešimų XML schemos aprašymas“

„GDR-ISMOK pranešimų XML schemos aprašymas“

„FIN-PR-PERL pranešimų XML schemos aprašymas“

1.3 Vartojamos sąvokos

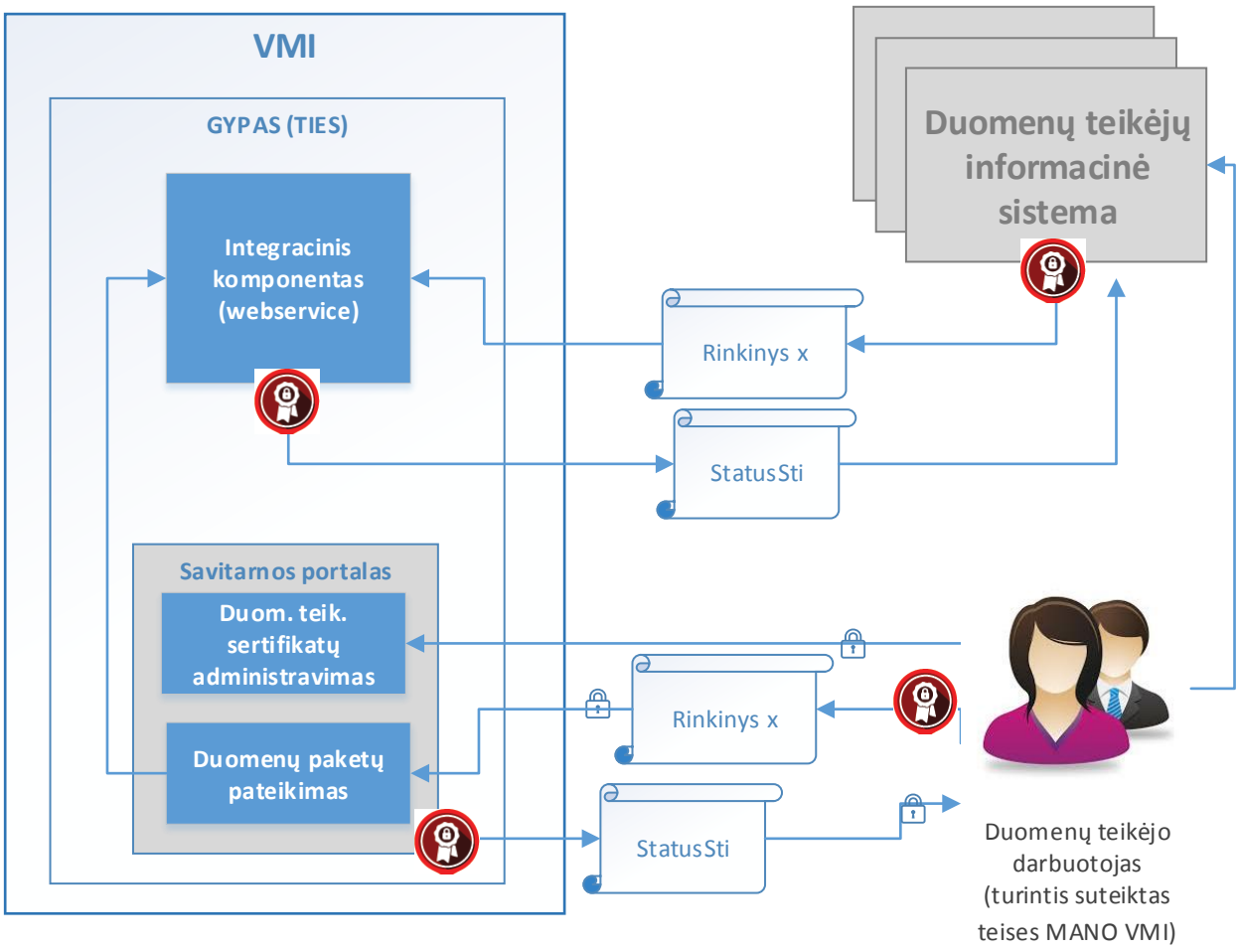
Šiame dokumente vartojamos sąvokos ir santrumpos:

Sąvoka, santrumpa	Reikšmė/Paaiškinimas
CbC	TĮG ataskaitinių finansinių metų ataskaita pagal valstybes (Angl. ‘country-by-country reporting’
CBC-DAC4-LT	XML formato pranešimas, kuriame CbC ataskaitas turintis teikti subjektas, teikia duomenų rinkinio duomenis LT mokesčių administratoriui (VMI). Vieno subjekto rinkinio duomenys gali būti teikiami keliais pranešimais.
CBC-DAC4-LT XSD	CBC-DAC4-LT pranešimo XML struktūros aprašas (angl. XML Schema Definition).
CRS-DAC2-LT	Duomenų rinkinys, gaunamas iš Lietuvos FĮ, apie praneštinus asmenis ir su jais susijusių finansinių sąskaitų duomenis. Duomenys renkami pagal informacijos, būtinos tarptautiniams bendradarbiavimo įsipareigojimams dėl automatinių informacijos apie finansines sąskaitas mainų įgyvendinti, pateikimo taisykles, patvirtintas 2015 m. lapkričio 25 d. Valstybinės mokesčių inspekcijos prie Lietuvos Respublikos finansų ministerijos viršininko įsakymu Nr. VA-102
DAC	Administravimo bendradarbiavimo direktyva
DAC4	2016 m. gegužės 25 d. Europos Tarybos direktyva (ES) 2016/881, kuria iš dalies keičiamos Direktyvos 2011/16/ES nuostatos dėl privalomų automatinių apmokestinimo srities informacijos mainų DAC4 – angl. The 4th Directive on Administrative Cooperation
FATCA	Angl. Foreign Account Tax Compliance Act – duomenų rinkinys apie užsienio valstybėse turimų sąskaitų Finansinėse institucijose duomenis

Sąvoka, santrumpa	Reikšmė/Paaiškinimas
FATCA-LT	XML formato pranešimas, kuriame FĮ teikia FATCA duomenų rinkinio duomenis LT mokesčių administratoriui (VMI). Vieno FĮ rinkinio duomenys gali būti teikiami keliais pranešimais.
FATCA-LT XSD	FATCA-LT pranešimo XML struktūros aprašas (angl. XML Schema Definition).
FĮ, FI	Finansų įstaiga, finansų rinkos dalyvis. Prižiūrimas finansų rinkos dalyvis, kaip jis apibrėžtas Lietuvos Respublikos Lietuvos banko įstatyme, privalo pateikti VMI MAI55-SIPL, MAI55-SKIS ir(arba) MAI55-SLIK duomenų rinkinius. Taip pat finansų rinkos dalyvis, kuris privalo pateikti DAC2_LT duomenų rinkinius.
FIN-PR-PERL	XML formato pranešimas, kuriame teikiami duomenys apie finansinių priemonių perleidimą gyventojams.
FIN-PR-PERL XSD	FIN-PR-PERL pranešimo XML struktūros aprašas (angl. XML Schema Definition).
GDR-ISMOK	XML formato pranešimas, kuriame gyvybės draudimo išmokų mokėtojai teikia duomenis apie gyventojams išmokėtas gyvybės draudimo išmokas.
GDR-ISMOK XSD	GDR-ISMOK pranešimo XML struktūros aprašas (angl. XML Schema Definition).
GYPAS	Gyventojų pajamų mokesčio informacinė sistema
IS	Informacinė sistema.
MAĮ	Mokesčių administravimo įstatymas
MAI55 duomenų rinkinys	MAI55-SIPL, MAI55-SKIS ar MAI55-SLIK duomenų rinkinys
MAI55-SIPL duomenų rinkinys	Visuma duomenų apie sąskaitų per kalendorinius metus gautų įplaukų dydžius, kuriuos FĮ turi pateikti VMI pagal MAĮ 55 straipsnį.
MAI55-SIPL pranešimas	XML formato pranešimas, kuriame FĮ teikia MAI55_SIPL duomenų rinkinio duomenis. Vieno rinkinio duomenys gali būti teikiami keliais pranešimais.
MAI55-SIPL XSD	MAI55-SIPL pranešimo XML struktūros aprašas (angl. XML Schema Definition).
MAI55-SLIK duomenų rinkinys	Visuma duomenų apie sąskaitų kalendorinių metų gruodžio 31 d. likučius, kuriuos FĮ turi pateikti VMI pagal MAĮ 55 straipsnį.
MAI55-SLIK pranešimas	XML formato pranešimas, kuriame FĮ teikia MAI55-SLIK duomenų rinkinio duomenis. Vieno rinkinio duomenys gali būti teikiami keliais pranešimais.
MAI55_SLIK XSD	MAI55-SLIK pranešimo XML struktūros aprašas (angl. XML Schema Definition).
MAI55-SKIS duomenų rinkinys	Visuma duomenų apie skolinius įsipareigojimus, kuriuos FĮ turi pateikti VMI pagal MAĮ 55 straipsnį.
MAI55-SKIS pranešimas	XML formato pranešimas, kuriame FĮ teikia MAI55-SKIS duomenų rinkinio duomenis. Vieno rinkinio duomenys gali būti teikiami keliais pranešimais.
MAI55_SKIS XSD	MAI55-SKIS pranešimo XML struktūros aprašas (angl. XML Schema Definition).
PALUK-ISMOK	XML formato pranešimas, kuriame FĮ teikia duomenis apie visų rūšių finansų įstaigų gyventojams išmokamas palūkanas (šiuo metu tokios išmokos žymimos pajamų rūšių kodais: 56, 58, 59, 64, 65, 66, 67, 68, 69). Vieno FĮ rinkinio duomenys gali būti teikiami keliais pranešimais.
PALUK-ISMOK XSD	PALUK-ISMOK pranešimo XML struktūros aprašas (angl. XML Schema Definition).
SOAP	Protokolas, skirtas struktūrizuotos informacijos mainams teikiant žiniatinklio paslaugas (angl. web service) kompiuterių tinklais (angl. Simple Object Access Protocol)
TARP-IV-APSK	Tarpininkų teikiami individualios veiklos apskaitos duomenys (tokių duomenų rinkinys už ataskaitinį laikotarpį)
TIES	Mokesčių ir susijusių duomenų apsikeitimo posistemė (angl. Tax Information Exchange SubSystem).
TĮG	Tarptautinė įmonių grupė
UTF	Simbolių užkodavimo formatas (angl. Unicode Transformation Format)
UTF8	8 bitų simbolių užkodavimo formatas (žr. UTF)
VMI, VMI prie FM	Valstybinė mokesčių inspekcija prie Lietuvos Respublikos finansų ministerijos.
Žiniatinklio paslauga	Programinės įrangos sistema, suprojektuota įvairių kompiuterių sąveikai tinkle užtikrinti (angl. web service)
WS-Security	Žiniatinklio paslaugų saugos standarto ir specifikacijos pavadinimas (angl. Web Services Security)
XML	Bendrosios paskirties duomenų struktūrų bei jų turinio aprašomoji kalba (angl. Extensible Markup Language).
XSD	XML struktūros aprašas (angl. XML Schema Definition).

2 Duomenų teikimo integracinė sąsaja

2.1 Duomenų teikimo schema



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

TIES sudaro tokio dalys:

- 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 veiksmais (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).

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 atilikti 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.

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 schemos:

- IsoTypesSti;
- CommonTypesSti;
- StatusSti.

Specifinių konkrečios duomenų rinkinių grupės duomenų struktūrų aprašymui yra naudojamos specifinės tų rinkinių XML schemos, 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.

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 50MB.

Pagal CRS-DAC2-LT schemą, tai sudaro apytiksliai apie 10 000 įrašų.(duomenų rinkinių). Duomenų rinkinys – tai susijusių duomenų rinkinys, kuris identifikuojamas vienu ir tuo pačiu DocRefId.

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 teikiamiems duomenims, tiek iš VMI gaunamiems duomenims (pvz., atsakymams apie priėmimą/nepriėmimą).

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:

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. Skaitmeninis parašas turi būt 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 trumpesniam papildomas nuliais iš kairės iki 11 skaitmenų). Pavyzdys: 00333333333_Payload.xml
1.2. Suarchyvuoti XML failą	00000000000_Payload.zip
1.3. 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: 20160115163045 32Z_00000000000.zip

3.3 Duomenų paketo išpakavimo žingsniai

Duomenis gavusi IS turi išpakuoti gautą duomenų paketą. Išpakavimui atliekami šie žingsniai:

Žingsnio aprašymas	Rezultatas
1. Išarchyvuoti gautą failą	
1.1. Išarchyvuoti gautą failą UTC_SenderID.zip	00000000000_Payload ir 00000000000_Key
2. Iššifruoti AES raktą	
2.1. Iššifruoti AES raktą naudojant savo (t.y. gavėjo) privatų raktą	00000000000_Key
3. Iššifruoti XML failą	
3.1. Iššifruoti XML failą 00000000000_Payload su ankstesniame žingsnyje iššifruotu AES-256 raktu	00000000000_Payload.zip

4. Išarchyvuoti iššifruotą failą	
4.1. Išarchyvuoti iššifruotą failą 00000000000_Payload.zip	00000000000_Payload.xml
5. Patikrinti parašą	
5.1. Naudojant teikėjo (VMI) viešąjį raktą patikrinti parašą įsitikinant siuntėjo ir duomenų paketo autentiškumu.	-

4 Paslaugos (WS metodai)

TIESService – žiniatinklio paslauga, kurią VMI pateikia finansų įstaigoms. 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	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.
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 unikaliai 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	Būtinas (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 užklausos ir rezultato struktūrą apibrėžia schema „GetStatus“.

Užklausos 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.

Užklausos rezultatą apibrėžia schemos elementas sst:Response_Type (sėkmingo užklausos apdorojimo atveju), nesėkmingo užklausos 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).
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 būsena.
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.

Užklausos 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 užklausos apdorojimo atveju), nesėkmingo užklausos 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).
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 būsena.
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 „GetTransmitionsByDate“

Pavadinimas: GetTransmitionsByDate

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

Užklausos 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	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).
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 būsena.
8.	StatusDate	DateTime	T	Duomenų apdorojimo būsenos nustatymo data ir laikas.

4.5 Metodas „CancelPackage“

Pavadinimas: CancelPackage

Paskirtis/ aprašymas: Metodas skirtas perduoto 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	Būtinas (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	Būtinas (T/N)	Aprašymas
1.	Status	cts:StringMax30_Type	T	Duomenų apdorojimo būsena.
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;

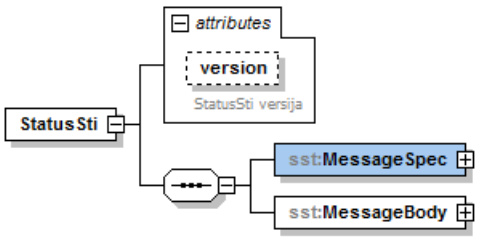
FIN-PR-PERL.

MAI55-SIPL, MAI55-SKIS ir MAI55-SLIK, CRS-DAC2-LT, FATCA-LT, CBC-DAC4-LT, PALUK-ISMOK, TARP-IV-APSK, GDR-ISMOK dokumentuoti atskiruose dokumento prieduose. Status-Sti apibrėžtas žemiau esančiame skyriuje.

5.1 Status-Sti

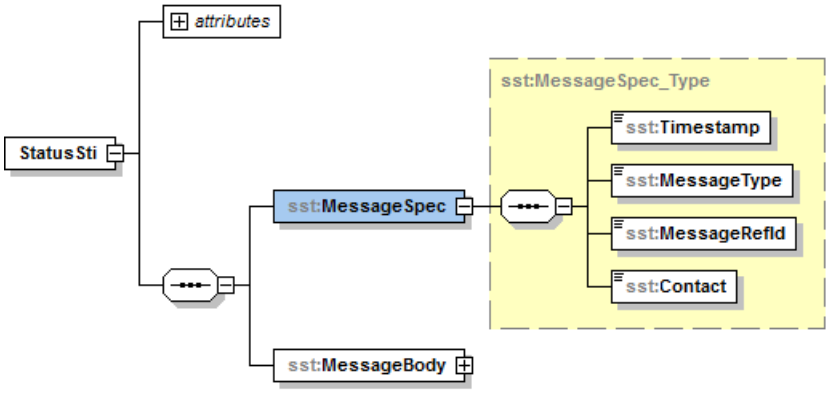
Šio tipo pranešimas pateikia atsakymus apie pranešimu perduoto duomenų rinkinio priėmimą/nepriėmimą. Tai yra šis pranešimas gaunamas į TIES iš duomenis apdorojančios sistemos.

Juo perduodami atitinkamo duomenų rinkinio duomenų apdorojimo rezultatai.



5.1.1 Antraštės dalis

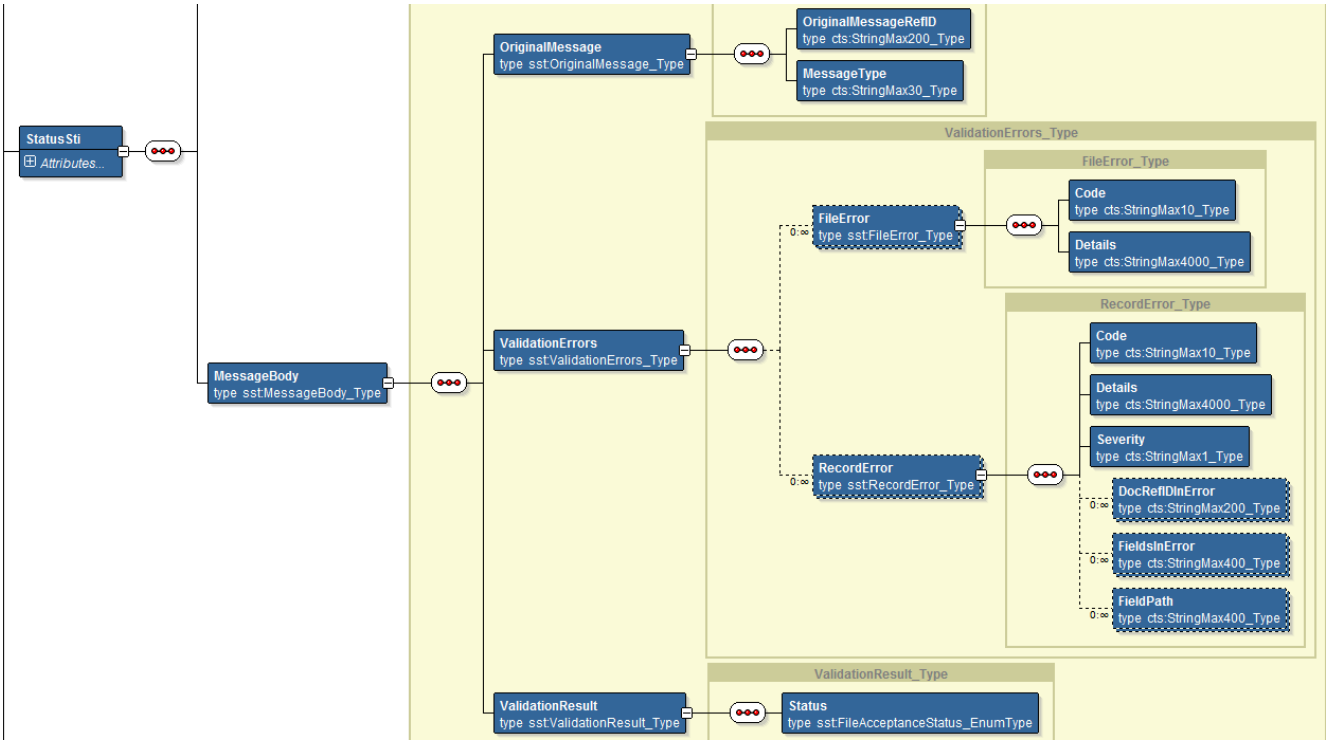
Elemento indeksas	Privalomumas	Elemento pavadinimas (anglų kalba)	Elemento trumpas aprašas	Elemento aprašas	Elemento formatas
1.1.	T	Version	Versija	Pranešimo XML struktūrų aprašo versija.	
1.2.	T	Timestamp	Suformavimo data ir laikas	Pranešimo suformavimo data ir laikas.	Data su laiku
1.3.	T	MessageType	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	Kontaktinė 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.	
1.1.1	T	OriginalMessageRefID	Originalaus pranešimo identifikatorius	Unikalus originalaus pranešimo identifikavimo numeris.	200 simbolių eilutė
1.1.2	T	MessageType	Originalaus	Originalaus pranešimo tipas, įvardinantis	30 simbolių eilutė

Elemento indeksas	Privalomumas	Elemento pavadinimas (anglų kalba)	Elemento trumpas aprašas	Elemento aprašas	Elemento formatas
			pranešimo tipas	duomenų grupę.	
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



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.

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
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

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 00000000000_Key
20003	Nepavyko iššifruoti Payload failo	Duomenų gavėjui nepavyko iššifruoti gauto failo 00000000000_Payload į 00000000000_Payload.zip
20004	Nekorektiškas Payload zip failas	Duomenų gavėjui nepavyko išpakuoti gauto failo 00000000000_Payload.zip į 00000000000_Payload.xml
20005	Nepavyko patikrinti xml pranešimo skaitmeninio parašo	Duomenų gavėjui nepavyko patikrinti xml pranešimo skaitmeninio parašo su teikėjo viešuoju raktu.
20006	Nekorektiška xml pranešimo struktūra	Pranešimas neatitinka XML schemoje numatytos struktūros
20007	Nesutampa pranešimo tipas	Pranešime įrašytas pranešimo tipas (MessageType) nesutampa su nurodytu pateikiant duomenų paketą

Kodas	Pavadinimas (Lt)	Aprašas (Lt)
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

5.3.3 ISO valstybės

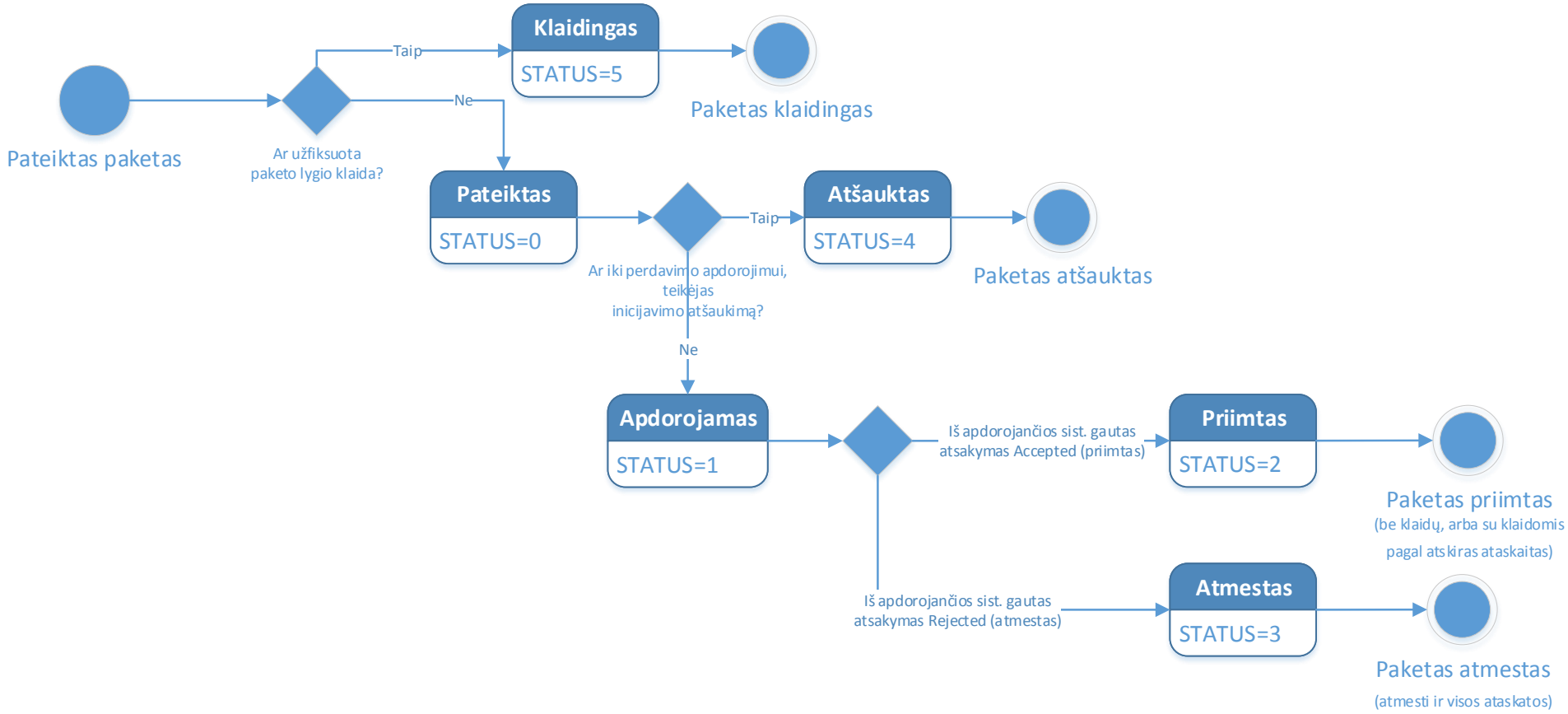
Reikšmės išvardintos XSD schemoje IsoTypesSti.

5.3.4 ISO valiutos

Reikšmės išvardintos XSD schemoje 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	*{UTC}_{SenderID}.zip* failas negali būti išarchyvuotas	Įsitikinti, kad zip archyvas atsidaro su populiariomis archyvavimo programomis. Patartina naudoti "Deflate" suspaudimo algoritmą.
	{UTC}_{SenderID}.zip archyve nerastas *{SenderID}_Payload* failas	Įsitikinti, kad galutiniame archyve yra patalpintas *{SenderID}_Payload* failas. Atkreipti dėmesį į didžiąsias/mažąsias failo pavadinimo raides.
	{UTC}_{SenderID}.zip archyve nerastas *{ReceiverID}_Key* failas	Įsitikinti, kad galutiniame archyve yra patalpintas *{ReceiverID}_Key* 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 *{ReceiverID}_Key* 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 vaktoriumi (PV) (angl. "Initial Vector (IV)"
	{SenderID}_Payload failas buvo užšifruotas su AES-256 raktu, naudojant netinkamus nustatymus	Įsitikinti, kad naudojami tokie *{SenderID}_Payload* 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	*{SenderID}_Payload.zip* failas negali būti išarchyvuotas	Įsitikinti, kad zip archyvas atsidaro su populiariomis archyvavimo programomis. Patartina naudoti "Deflate" suspaudimo algoritmą.
	{SenderID}_Payload failas buvo užšifruotas naudojant kitą pradinį vektorių (IV), nei pateiktą *{ReceiverID}_Key* faile	Tokiu atveju, kai *{SenderID}_Payload* failas buvo užšifruotas naudojant kitą pradinį vektorių (IV), nei pateiktą *{ReceiverID}_Key* faile, bet AES raktas pateiktas teisingas, tai *{SenderID}_Payload* failo iššifravimas įvyksta sėkmingai, tačiau gauto *{SenderID}_Payload.zip* failo pirmi 16

		baitų (zip failo header dalis) būna neteisingi, todėl jo išarchyvuoti TIES sistemai nepavyksta.
	Simetrinio iššifravmo 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	*{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 elementai pagal aprašymą https://www.w3.org/TR/xmldsig-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.

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
2   # @author Julius Žaldokas (Algoritmų sistemos) (IT:ES:SE:PE)
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=algoritmusistemos
9
10  SenderId=00000000000
11  ReceiverId=00188659752
12
13  export UNSIGNED_XML_IN RECEIVER_PUBLIC_CERT_IN MY_PRIVATE_KEYSTORE_PKCS12_IN
    MY_PRIVATE_KEYSTORE_PWD_IN MY_PRIVATE_KEY_ALIAS SenderId ReceiverId
14  ./ties_package.sh
```

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

```
1   #!/bin/bash
2   # @author Julius Žaldokas (Algoritmų sistemos) (IT:ES:SE:PE)
3
```

```
4   ############################################################
5   # 'openssl', 'zip' and 'xmlsec1' should be in the path.
6   # for 'xmlsec1' see https://www.aleksey.com/xmlsec
7   ############################################################
8
9   echo "****************************************************"
10  echo "DEFINING VARIABLES"
11  echo "****************************************************"
12
13  echo UNSIGNED_XML_IN=$UNSIGNED_XML_IN
14  echo RECEIVER_PUBLIC_CERT_IN=$RECEIVER_PUBLIC_CERT_IN
15  echo MY_PRIVATE_KEYSTORE_PKCS12_IN=$MY_PRIVATE_KEYSTORE_PKCS12_IN
16  echo MY_PRIVATE_KEYSTORE_PWD_IN=$MY_PRIVATE_KEYSTORE_PWD_IN
17  echo MY_PRIVATE_KEY_ALIAS=$MY_PRIVATE_KEY_ALIAS
18  echo
19  echo SenderId=$SenderId
20  echo ReceiverId=$ReceiverId
21
22  echo "****************************************************"
23
24  if [[ -z $UNSIGNED_XML_IN || -z $RECEIVER_PUBLIC_CERT_IN || -z
    $MY_PRIVATE_KEYSTORE_PKCS12_IN || -z $MY_PRIVATE_KEYSTORE_PWD_IN || -z $SenderId ||
25  -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
    $MY_PRIVATE_KEYSTORE_PKCS12_IN ]]; then
31      echo "ERROR: either $UNSIGNED_XML_IN or $RECEIVER_PUBLIC_CERT_IN or
    $MY_PRIVATE_KEYSTORE_PKCS12_IN does not exit"
32      exit 1
33  fi
34
35  ############################################################
36
37
```

```
38  # Definine 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
    Id="TIES">[XML]</Object>.
64  #    - Use $signed_xml and sign using 'xmlsec1'
65  ############################################################
66
67
68  echo;echo "creating signature template file '$pre_sign_tmplt' for xmlsec
    signing...."
69
70  # create signature template file after embedding xml
71  if [[ -f $pre_sign_tmplt ]]; then
```

```
        rm -f $pre_sign_tmplt
    fi


    tmplt_prefix='<?xml version="1.0" encoding="UTF-8" standalone="no"?><Signature
    xmlns="http://www.w3.org/2000/09/xmldsig#"
72  Id="SignatureId"><SignedInfo><CanonicalizationMethod
    Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/><SignatureMethod
73  Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/><Reference
    URI="#TIES"><Transforms><Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
74  c14n#"/></Transforms><DigestMethod
    Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/><DigestValue/></Reference></Sig
75  nedInfo><SignatureValue/><KeyInfo><X509Data><X509Certificate/></X509Data></KeyInfo><
    Object Id="TIES">'
76
77
78  tmplt_suffix='</Object></Signature>'
79
80  echo -n "$tmplt_prefix" >> $pre_sign_tmplt
81
82  is_newline_needed=0
83  xml_decl_checked=0
84  line=
85  while IFS= read -r line
86  do
87  if [[ $xml_decl_checked -eq 0 ]]; then
88      xml_decl_checked=1
89      line=`echo ${line#<?xml*?>}`
90      if [[ ! -z "$line" ]]; then
91          echo -n "$line" >> $pre_sign_tmplt
92          is_newline_needed=1
93      fi
94  else
95      if [[ is_newline_needed -eq 1 ]]; then echo >> $pre_sign_tmplt; fi
96      echo -n "$line" >> $pre_sign_tmplt
97      is_newline_needed=1
98  fi
99  done < $UNSIGNED_XML_IN
100
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
        signing....done"
114
115
        ############################################################
116
117
        echo;echo "signing '$pre_sign_tmplt' to create signed xml '$signed_xml'...."
118
119
        # sign with xmlsec
120
        if [[ $MY_PRIVATE_KEY_ALIAS -eq "" ]]; then
121
            CMD="xmlsec1 --sign --pkcs12 $MY_PRIVATE_KEYSTORE_PKCS12_IN --pwd
122     $MY_PRIVATE_KEYSTORE_PWD_IN --output $signed_xml $pre_sign_tmplt"
123     else
124         CMD="xmlsec1 --sign --pkcs12:$MY_PRIVATE_KEY_ALIAS
125     $MY_PRIVATE_KEYSTORE_PKCS12_IN --pwd $MY_PRIVATE_KEYSTORE_PWD_IN --output
        $signed_xml $pre_sign_tmplt"
126     fi
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
```

```
136     fi
137
138     echo; echo "signing '$pre_sign_tmplt' to create signed xml '$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 '$compressed_signed_xml'....done";
160     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
```

```
170     #    - encrypt $compressed_signed_xml using CBC with $AESKEY, $IV. encrypted file
        output is $payload_file
171
        #    - append $IV to $AESKEY and encrypt resulting $AESKEYIVBIN with receiver's PKI
172     public key, $RECEIVER_PUBLIC_CERT_IN. output file is $key_file
173     ############################################################
174
175     echo "encrypting '$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 $payload_file -K
189     $AESKEY -iv $IV"
190
191     echo;echo $CMD;$CMD
192
193     if [[ "$?" -ne 0 ]]; then
194         echo "!!!! please fix the error !!!!";echo $CMD;echo
195         rm -f $pre_sign_tmplt $signed_xml $compressed_signed_xml $payload_file
196         exit 1
197     fi
198
199     # Concatenate 32 bytes AESKEY and 16 bytes IV
200     AESKEYIV=`echo -n "$AESKEY$IV"`
201
202     # Convert AESKEY+IV hex to binary
203     AESKEYIVBIN=`echo ${key_file}.aeskeyivbin`
```

```
204
205     #echo;echo "echo -n $AESKEYIV|perl -pe '\$_=pack(\"H*\",\$_)' > $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 RAKTU.
213     #
214     # Encrypt aeskey_iv.bin with receiver's RSA PKI public key
215     ############################################################
216     CMD="openssl rsautl -encrypt -out $key_file -certin -inkey $RECEIVER_PUBLIC_CERT_IN
        -keyform DER -in $AESKEYIVBIN"
217
218
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
        $AESKEYIVBIN $key_file
224         exit 1
225     fi
226
227     echo; echo "encrypting '$compressed_signed_xml'....done"; echo
228
229     ############################################################
230     # GYPAS_TIES_SA 3.2       DUOMENŲ PAKETO PARENGIMO ŽINGSNIAI
231     #        3.1 - SUKURTI GALUTINĮ PAKETĄ, KURIS BUS SIUNČIAMAS
232     #
233     # create TIES $pkg_file which contains following files compressed
234     #     - $payload_file
235     #     - $key_file
236     ############################################################
237
```

```
238     echo "creating pkg '$pkg_file'......."
239
240     CMD="zip -q $pkg_file $payload_file $key_file"
241
242     echo;echo $CMD;$CMD


        if [[ "$?" -ne 0 ]]; then

            echo "!!!! please fix the error !!!!";echo $CMD;echo

            rm -f $pre_sign_tmplt $signed_xml $compressed_signed_xml $payload_file
        $AESKEYIVBIN $key_file $pkg_file

            exit 1

        fi


        echo; echo "creating pkg '$pkg_file'.......done"; echo


        ############################################################

        # remove all temporary files (comment for  debugging/verification)

        ############################################################


        rm -f $pre_sign_tmplt $signed_xml $compressed_signed_xml $payload_file $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  #!/bin/bash
2  # @author Julius Žaldokas (Algoritmų sistemos) (IT:ES:SE:PE)
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=algoritmusistemos.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 # @author Julius Žaldokas (Algoritmų sistemos) (IT:ES:SE:PE))
 3
 4 ############################################################
 5 # 'openssl', 'unzip' and 'xmlsec1' should be in the path.
 6 # for 'xmlsec1' see https://www.aleksey.com/xmlsec
 7 ############################################################
 8
 9 echo "**********************"
10 echo "DEFINING VARIABLES"
11 echo "**********************"
12
13 echo TIES_PKG_IN=$TIES_PKG_IN
14 echo MY_PRIVATE_KEYSTORE_PKCS12_IN=$MY_PRIVATE_KEYSTORE_PKCS12_IN
15 echo MY_PRIVATE_KEYSTORE_PWD_IN=$MY_PRIVATE_KEYSTORE_PWD_IN
16 echo SENDER_PUBLIC_CERT_IN=$SENDER_PUBLIC_CERT_IN
```

```
17
18 echo "**********************"
19
20 if [[ -z $TIES_PKG_IN || -z $MY_PRIVATE_KEYSTORE_PKCS12_IN || -z
   MY_PRIVATE_KEYSTORE_PWD_IN ]]; then
       echo "please see test_unpack.sh....set at least these variables TIES_PKG_IN,
21 MY_PRIVATE_KEYSTORE_PKCS12_IN, MY_PRIVATE_KEYSTORE_PWD_IN)"
       exit 1
22 fi
23
24 ####################
25 # GYPAS_TIES_SA 3.3       DUOMENŲ PAKETO IŠPAKAVIMO ŽINGSNIAI
26 #        1.1 - IŠARCHYVUOTI GAUTĄ FAILĄ
27 #
28 # unzip TIES_PKG_IN
29 ####################
30
31 if [[ ! -f $TIES_PKG_IN || ! -f $MY_PRIVATE_KEYSTORE_PKCS12_IN ]]; then
32     echo "ERROR: either $TIES_PKG_IN or $MY_PRIVATE_KEYSTORE_PKCS12_IN does not exit"
33     exit 1
   fi
34
35 echo "unzipping '$TIES_PKG_IN'...."
36
37 declare -a arr=(`unzip -Z2 ${TIES_PKG_IN}`)
38
39 i=0
40 while true; do
41         tmp=${arr[$i]#*_}
42         tmp="${tmp//$'\r'/}"
43         # Equality Comparison
44     if [[ ${tmp} = Payload ]]; then
45         payload_file=${arr[$i]}
46                 payload_file="${payload_file//$'\r'/}"
47     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 '$MY_PRIVATE_KEYSTORE_PKCS12_IN'...."
74
75  ####################
    # GYPAS_TIES_SA 3.3       DUOMENŲ PAKETO IŠPAKAVIMO ŽINGSNIAI
76  #         2.1 - IŠŠIFRUOTI AES RAKTĄ NAUDOJANT PRIVATŲ RAKTĄ
77  #
78  # Decrypt encrypted AESKEY+IV using receiver's RSA PKI private key
79  ####################
80
```

```
81 private_key_pem_file=`echo ${key_file}.pem`
82
83
84
85 CMD="openssl pkcs12 -in $MY_PRIVATE_KEYSTORE_PKCS12_IN -nocerts -passin
   pass:$MY_PRIVATE_KEYSTORE_PWD_IN -nodes" > $private_key_pem_file
86 echo;echo "$CMD > $private_key_pem_file";$CMD > $private_key_pem_file
87 if [[ "$?" -ne 0 ]]; then
88     echo "!!!! please fix the error !!!!";
89     echo;echo "$CMD > $private_key_pem_file";$CMD > $private_key_pem_file
90     rm -f $key_file $payload_file $private_key_pem_file
91     exit 1
92 fi
93
94 echo;echo "extracting private key from keystore
   '$MY_PRIVATE_KEYSTORE_PKCS12_IN'....done"
95 echo;echo "decrypting '$key_file' using private key from '$private_key_pem_file'...."
96
97 CMD="TMP=\`openssl rsautl -decrypt -in $key_file -inkey $private_key_pem_file | perl -
   pe '\$_=unpack("H*",\$_)'\`"
98
99 echo;echo $CMD;
100 TMP=`openssl rsautl -decrypt -in $key_file -inkey $private_key_pem_file|perl -pe
   '$_=unpack("H*", $_)'`
101 if [[ "$?" -ne 0 ]]; then
102     echo "!!!! please fix the error !!!!";echo $CMD;echo
103     rm -f $key_file $payload_file $private_key_pem_file
104     exit 1
105 fi
106 # Extract 32 bytes AESKEY and 16 bytes IV
107
```

```
AESKEY2DECRYPT=`echo ${TMP:0:64}`
IV2DECRYPT=`echo ${TMP:64:96}`

####################
# GYPAS_TIES_SA 3.3       DUOMENŲ PAKETO IŠPAKAVIMO ŽINGSNIAI
#        3.1 - IŠŠIFRUOTI ARCHYVUOTĄ XML FAILĄ SU ANKSTESNIAME ŽINGSNYJE IŠŠIFRUOTU AES-256 RAKTU
#
# Decrypt payload using D_AESKEY and D_IV
####################

payload_zip_file=`echo ${payload_file}.zip`
CMD="openssl enc -d -aes-256-cbc -in $payload_file -out $payload_zip_file -K $AESKEY2DECRYPT -iv $IV2DECRYPT"

echo;echo $CMD;$CMD

if [[ "$?" -ne 0 ]]; then
    echo "!!!! please fix the error !!!!";echo $CMD;echo
    #rm -f $key_file $payload_file $private_key_pem_file
    exit 1
fi

# Check if payload_zip_file are created
if [[ ! -f $payload_zip_file ]]; then
    echo "!!!! please fix the error !!!!";echo $CMD;echo
    rm -f $key_file $payload_file $private_key_pem_file
    exit 1
fi

echo;echo "decrypting '$key_file' using private key from '$private_key_pem_file'....done"

####################
# GYPAS_TIES_SA 3.3       DUOMENŲ PAKETO IŠPAKAVIMO ŽINGSNIAI
```

```
140 #        4.1 - IŠARCHYVUOTI IŠŠIFRUOTĄ FAILĄ 00000000000_PAYLOAD.ZIP
141 #
    ####################
142
143 echo;echo "unzipping '$payload_zip_file'...."
144
145 CMD="unzip -oq $payload_zip_file"
146
147 echo;echo $CMD;$CMD
148
149 payload_xml_file=${payload_file}.xml
150
151 # Check if $payload_xml_file is created
152 if [[ "$?" -ne 0 || ! -f $payload_xml_file ]]; then
153     echo "!!!! please fix the error !!!!";echo $CMD;echo
154     rm -f $key_file $payload_file $private_key_pem_file
155     exit 1
156 fi
157
158 echo;echo "unzipping '$payload_zip_file'....done"
159
160 ####################
161 # GYPAS_TIES_SA 3.3       DUOMENŲ PAKETO IŠPAKAVIMO ŽINGSNIAI
162 #        5.1 - Naudojant teikėjo (VMI) viešąjį raktą patikrinti parašą įsitikinant
    siuntėjo ir duomenų paketo autentiškumu.
163 #
164 ####################
165
166
    error_flag=0
167
168
    if [[ ! -z $SENDER_PUBLIC_CERT_IN && -f $SENDER_PUBLIC_CERT_IN ]]; then
        echo;echo "verifying signature of '$payload_xml_file'...."
169
170
        CMD="xmlsec1 --verify --pubkey-cert-der $SENDER_PUBLIC_CERT_IN $payload_xml_file"
171
```

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