



VALSTYBINĖ
MOKESČIŲ
INSPEKCIJA

VALSTYBINĖ MOKESČIŲ INSPEKCIJA PRIE LIETUVOS
RESPUBLIKOS FINANSŲ MINISTERIJOS

VMI duomenų apsikeitimo posistemis Duomenų teikimo sąsajos aprašas

Versija 2.10

VILNIUS

2017-10-31

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 „GetTransmissionsByDate“, „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 atmetas.	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 FJ. (dar neįdiegta)	Visi
2.7	2017-10-12	Papildyta nauju duomenų rinkiniu „CBC-DAC4-LT“ surenkant duomenis apie TĮG (tarptautinių įmonių grupių) ataskaitas (dar neįdiegta)	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.

TURINYS

1	IVADAS	4
1.1	Dokumento paskirtis ir sudėtis	4
1.2	Susiję dokumentai ir priedai	4
1.3	Vartojamos sąvokos	4
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	8
2.5	Duomenų teikimo failų dydžio apribojimai	8
3	SAUGOS REIKALAVIMAI	8
3.1	Reikalavimai skaitmeniniam sertifikatui	8
3.2	Duomenų paketo parengimo žingsniai	9
3.3	Duomenų paketo išpakavimo žingsniai	9
4	PASLAUGOS (WS METODAI)	10
4.1	Metodas „SubmitPackage“	10
4.2	Metodas „GetStatus“	10
4.3	Metodas „GetTransmissionInfo“	11
4.4	Metodas „GetTransmissionsByDate“	12
4.5	Metodas „CancelPackage“	13
5	PRANEŠIMAI	13
5.1	Status-Sti	14
5.1.1	Antraštės dalis	14
5.1.2	Pagrindinė dalis	15
5.2	Bendrai naudojami paprastieji duomenų tipai	16
5.3	Bendrieji klasifikatoriai	16
5.3.1	Paketo I lygio klaidų kodai	17
5.3.2	Paketo II lygio klaidų kodai	17
5.3.3	ISO valstybės	18
5.3.4	ISO valiutos	18
6	PRIEDAI	19
6.1	Dažniausiai pasitaikančios duomenų paketo suformavimo klaidos ir jų sprendimo būdai	19
6.2	UNIX bash script'as pasirašyto ir užšifruoto duomenų paketo sukūrimui iš xml failo	21
6.3	UNIX bash script'as pasirašyto xml failo atkūrimui iš užšifruoto duomenų paketo	30

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 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:

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

1.3 VARTOJAMOS SĄVOKOS

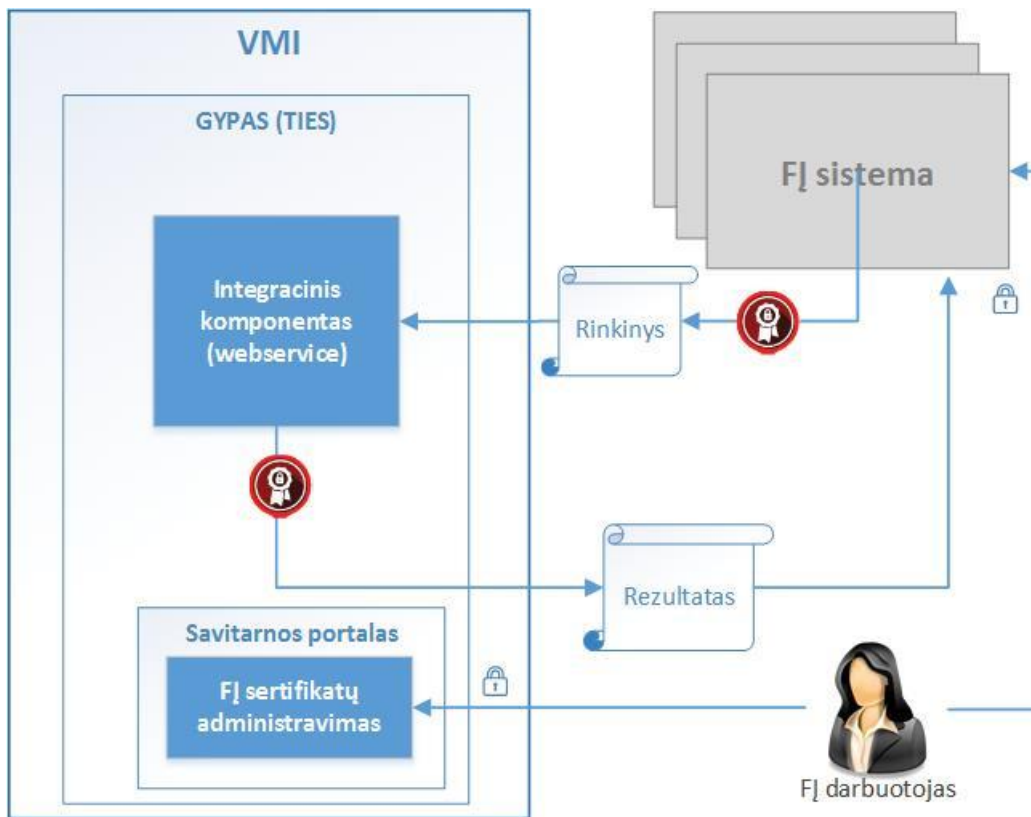
Šiame dokumente vartojamos sąvokos ir santrumpos:

Sąvoka, santrumpa	Reikšmė/Paiškinimas
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 automatinės informacijos apie finansines sąskaitas mainų įgyvendinti, pateikimo taisyklės, patvirtintos 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 automatinės 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
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).

Sąvoka, santrumpa	Reikšmė/Paiškinimas
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.
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).
SOAP	Protokolas, skirtas struktūrizuotos informacijos mainams teikiant žiniatinklio paslaugas (angl. web service) kompiuterių tinklais (angl. Simple Object Access Protocol)
TIES	Mokesčių ir susijusių duomenų apsikeitimo posistemė (angl. Tax Information Exchange SubSystem).
TJG	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 GYPAS posistemė TIES, kuri užtikrina finansinių duomenų pateikimą į VMI ir nukreipia tolimesniam apdorojimui.

TIES sudaro tokio dalys:

- Integracinis komponentas;
- Savitarnos portalas;

2.2 PORTALO BENDRIEJI REIKALAVIMAI

TIES savitarnos portalas integruotas su „Mano VMI“ sprendimais autentifikavimui bei prieigos teisių valdymui. „Mano VMI“ yra numatytas teisių rinkinys, kuris yra naudotinas TIES portale ir yra skirtas teisių duomenų teikėjui atstovaujantiems asmenims suteikimui/atėmimui. Prieigos teisės, kurios suteikiamos TIES savitarnos portalo naudotojams, siejamos su duomenų rinkinių grupėmis (pvz.: MAI55, CRS /DAC2, FATCA, CbC/DAC4 duomenys) ir galimais portale atlikti veiksmais (pvz.: sertifikatų administravimas, duomenų rinkinio peržiūra, duomenų rinkinio teikimas ir pan.). Įstaigos vadovas (ar jam prilygintas asmuo) per „Mano VMI“ turi įgaliotam atstovui suteikti teises teikti duomenų grupes ir naudotis TIES teikiama el. paslaugomis Mokesčių ir susijusių duomenų apskaitos posistemio savitarnos portale ([TIES](#)).

- Duomenų teikėjų atstovai TIES portalo sertifikatų administravimo srityje (menu punktas – Viešieji raktai) turi užregistruoti teikėjo sistemos viešą raktą, kuris bus naudojamas autentifikuojant teikėjo sistemą VMI duomenų teikimo platformoje bei apdorojant atsiųstą duomenų paketą. VMI viešąjį raktą taip pat galima atsisiųsti iš VMI TIES portalo.
- Integracijos taikymui būtina VMI viešąjį raktą atsisiųsti iš VMI TIES portalo.

Duomenys teikiami XML rinkiniais, turi būti koduoti UTF-8 (bet ne UTF-8 BOM ar kitais formatais).

FJ ir TjG, kurios neturi galimybės jungtis bei duomenis teikti per integracinį komponentą, gali jungtis prie savitarnos portalo (TIES išorinis portalas). Savitarnos portale FJ ar TjG įgaliotam atstovui, prisijungęs per „Mano VMI“ ir turintis ten suteiktas atitinkamas teises, gali atlikti tokius veiksmus TIES portale:

- Viešieji raktai: FJ galės užregistruoti savo viešąjį raktą, peržiūrėti, kokie viešieji raktai buvo registruoti;

- Peržiūrėti ir atsisiųsti VMI viešuosius raktus;
- Duomenų paketai: galės peržiūrėti FĮ 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 FĮ duomenų paketus, jų pateikimo rezultatus, suteikiama galimybė atsisiųsti pateiktą paketą.
Dėmesio – testiniai duomenų paketai apdorojimui ir loginei 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;
- FĮ, kuri 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 – tai tuščią ataskaitą galima įvesti ir sugeneruoti TIES savitarnos portale.

2.3 DUOMENŲ TEIKIMO, TIKSLINIMO PRINCIPAI

Šiame etape numatyta, kad FĮ ar TĮG į VMI teikia šiuos duomenų rinkinius:

- MAI55-SIPL;
- MAI55-SLIK;
- MAI55-SKIS;
- CRS-DAC2-LT;
- FATCA-LT;
- CBC-DAC4-LT.

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. FĮ ar TĮG 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). 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;
- SubmitPackage;
- StatusSti.

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

- M55TypesSti;
- CrsTypesSti;
- FtcTypesSti;
- CbcTypesSti.

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.

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 (nesuarchyvoto 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 tos Finansų įstaigos, kurios registruotos VMI GYPAS TIES portale kaip duomenų teikėjos, turinčios 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).

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: <ul style="list-style-type: none"> 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 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
1.2. Suarchyvuoti XML failą	00000000000_Payload.zip
1.3. Užšifruoti XML failą su AES-256 raktu <ul style="list-style-type: none"> 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. <ul style="list-style-type: none"> 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

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 užklauskos ir rezultato struktūrą apibrėžia schema „SubmitPackage“.

Užklauskos struktūrą apibrėžia schemos elementas spc:Request_Type.

Eil. Nr.	Pavadinimas	Duomenų tipas	Būtinis (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 unikalčiai apibrėžia duomenų paketą laike duomenų teikėjo pusėje.

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

Eil. Nr.	Pavadinimas	Duomenų tipas	Būtinis (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.

Užklauso rezultata apibrėžia schemas elementas sst:Response_Type (sėkmingo užklauso apdorojimo atveju), nesėkmingo užklauso 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 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.

Užklauso 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 užklauso apdorojimo atveju), nesėkmingo užklauso 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).
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 perdavimui į VMI faktų už laikotarpį duomenų gavimui iš VMI.

Užklauso parametrai:

Eil. Nr.	Pavadinimas	Duomenų tipas	Būtinasis (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 užklauso apdorojimo atveju), nesėkmingo užklauso 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).
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 būseną (Status) yra „Pateiktas“, o kiti jo apdorojimo veiksmai dar neatlikti. Sėkmingai atšaukus paketą, jo būseną (Status) nustatoma į „Atšauktas“, kiti jo apdorojimo veiksmai nebus atliekami.

Užklauso 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 užklauso apdorojimo atveju), nesėkmingo užklauso apdorojimo atveju grąžinamas Fault:

Eil. Nr.	Pavadinimas	Duomenų tipas	Būtinas (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;

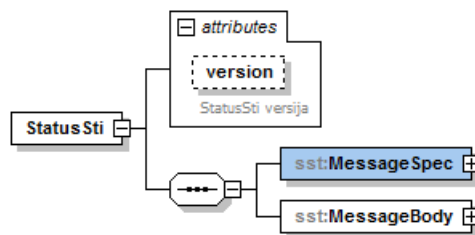
MAI55-SKIS;

CRS-DAC2-LT;
 FATCA-LT;
 CBC-DAC4-LT;
 Status-Sti.

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

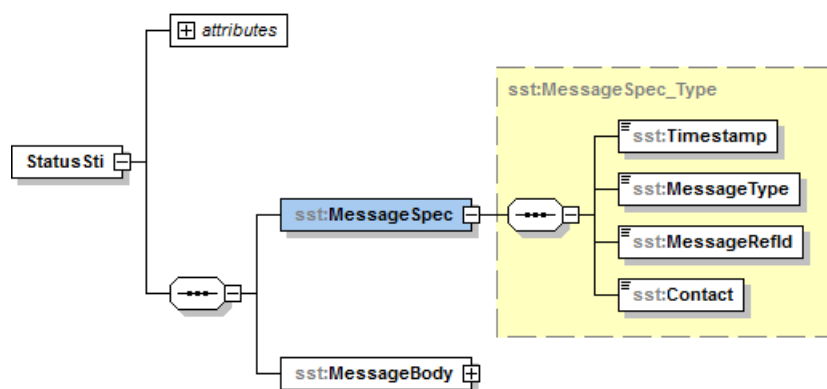
5.1 STATUS-STI

Šio tipo pranešimas pateikia atsakymus apie pranešimu perduoto duomenų rinkinio priėmimą/nepriėmimą.



5.1.1 Antraštės dalis

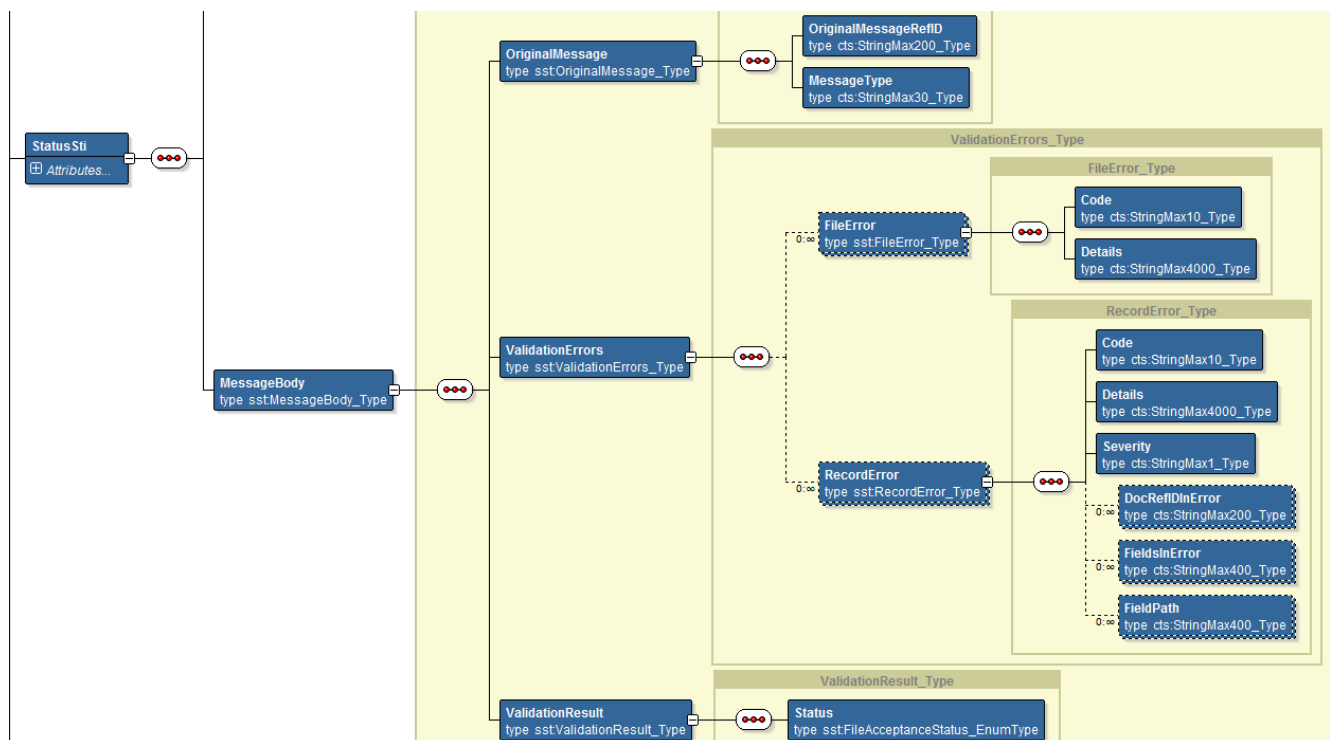
Elemento indeksas	Privalomumas	Elemento pavadinimas (anglų kalba)	Elemento trumpas aprašas	Elemento aprašas	Elemento formatas
1.1.	T	Version	Versija	Pranešimo XML struktūrų aprašo versija.	
1.2.	T	Timestamp	Suformavimo data ir laikas	Pranešimo suformavimo data ir laikas.	Data su laiku
1.3.	T	MessageType	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 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

Elemento indeksas	Privalomumas	Elemento pavadinimas (anglų kalba)	Elemento trumpas aprašas	Elemento aprašas	Elemento formatas
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	<p>Rezultato būsena:</p> <p>Accepted – Priimtas</p> <p>(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).</p> <p>Rejected – Atmestas.</p> <p>(Visas pranešimas su visais DocRefId atmestas.)</p>	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 GYPAS (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.

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
20008	Nesutampa pranešimo identifikacinis numeris	Pranešime įrašytas pranešimo unikalus identifikavimo numeris (MessageRefID) nesutampa su nurodytu pateikiant duomenų paketą

Kodas	Pavadinimas (Lt)	Aprašas (Lt)
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 schemeje IsoTypesSti.

5.3.4 ISO valiutos

Reikšmės išvardintos XSD schemeje IsoTypesSti.

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	<i>{UTC}_{SenderID}.zip</i> failas negali būti išarchyvuotas	Įsitikinti, kad zip archyvas atsidaro su populiariomis archyvavimo programomis. Patartina naudoti "Deflate" suspaudimo algoritmą.
	<i>{UTC}_{SenderID}.zip</i> archyve nerastas <i>{SenderID}_Payload</i> failas	Įsitikinti, kad galutiniame archyve yra patalpintas <i>{SenderID}_Payload</i> failas. Atkreipti dėmesį į didžiąsias/mažąsias failo pavadinimo raides.
	<i>{UTC}_{SenderID}.zip</i> archyve nerastas <i>{ReceiverID}_Key</i> failas	Įsitikinti, kad galutiniame archyve yra patalpintas <i>{ReceiverID}_Key</i> 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 <i>{ReceiverID}_Key</i> 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)")
	<i>{SenderID}_Payload</i> failas buvo užšifruotas su AES-256 raktu, naudojant netinkamus nustatymus	Įsitikinti, kad naudojami tokie <i>{SenderID}_Payload</i> 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	<i>{SenderID}_Payload.zip</i> failas negali būti išarchyvuotas	Įsitikinti, kad zip archyvas atsidaro su populiariomis archyvavimo programomis. Patartina naudoti "Deflate" suspaudimo algoritmą.

		<p>Tokiu atveju, kai <i>{SenderId}_Payload</i> failas buvo užšifruotas naudojant kitą pradinį vektorių (IV), nei pateiktą <i>{ReceiverID}_Key</i> faile, bet AES raktas pateiktas teisingas, tai <i>{SenderId}_Payload</i> failo iššifravimas įvyksta sėkmingai, tačiau gauto <i>{SenderId}_Payload.zip</i> failo pirmi 16 baitų (zip failo header dalis) būna neteisingi, todėl jo išarchyvuoti TIES sistemai nepavyksta.</p>
20005 - Nepavyko patikrinti xml pranešimo skaitmeninio parašo	<p><i>{SenderId}_Payload.zip</i> faile rastas skaitmeniniu parašu pasirašytas dokumentas nėra xml failas</p>	<p><i>{SenderId}_Payload.zip</i> archyvo faile turi būti patalpintas skaitmeniniu parašu pasirašytas xml dokumentas. Failas turi būti xml formatu, papildomai neužrakintas, nešifruotas, nepaverstas į BASE64 formatą ir pan.</p>
	<p>XML duomenų failas pasirašytas netinkamu XML pasirašymo algoritmu</p>	<p>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.</p>
	<p>Netinkama XML skaitmeninio parašo <DigestValue> reikšmė</p>	<p><DigestValue> reikšmė turi būti gauta paėmus <Object> elementą su visu duomenų XML, kuris yra <Object> elemento viduje, ir pavertus tokį XML į kanoninę formą <i>xml-exc-c14n</i> algoritmu. Apskaičiuota kanoninės formos XML teksto SHA256 maišos reikšmė turi būti paversta į BASE64 tekstą.</p>
	<p>Netinkama XML skaitmeninio parašo <SignatureValue> reikšmė</p>	<p><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</p> <p><SignedInfo> blokas turi būti paverstas į kanoninę formą <i>xml-exc-c14n</i> algoritmu. Gauta kanoninė forma turi būti užšifruota su siuntėjo privačiu raktu RAS-SHA256 algoritmu. Svarbu įsitikinti, kad privatų raktą atitinkantis viešasis raktas (sertifikatas) yra</p>

		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 (Algoritimų 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=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 # @author Julius Žaldokas (Algoritimų 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
25 $MY_PRIVATE_KEYSTORE_PKCS12_IN || -z $MY_PRIVATE_KEYSTORE_PWD_IN || -z $SenderId
26 || -z $ReceiverId ]]; then
27     echo "please see test_package.sh....set these variables: SenderId,
28 ReceiverId"
29     exit 1
30 fi
31
32 if [[ ! -f $UNSIGNED_XML_IN || ! -f $RECEIVER_PUBLIC_CERT_IN || ! -f
33 $MY_PRIVATE_KEYSTORE_PKCS12_IN ]]; then
34     echo "ERROR: either $UNSIGNED_XML_IN or $RECEIVER_PUBLIC_CERT_IN or
35 $MY_PRIVATE_KEYSTORE_PKCS12_IN does not exist"
36     exit 1
```

```

35 fi
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="${SenderId}"_"${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
    if [[ -f $pre_sign_tmplt ]]; then
        rm -f $pre_sign_tmplt
    fi

72 tmplt_prefix='<?xml version="1.0" encoding="UTF-8" standalone="no"?><Signature
73 xmlns="http://www.w3.org/2000/09/xmldsig#"
74 Id="SignatureId"><SignedInfo><CanonicalizationMethod
75 Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" /><SignatureMethod
76 Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" /><Reference
77 URI="#TIES"><Transforms><Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
78 c14n#" /></Transforms><DigestMethod
79 Algorithm="http://www.w3.org/2001/04/xmldsig-more#sha256" /><DigestValue/></Reference><
80 /SignedInfo><SignatureValue/><KeyInfo><X509Data><X509Certificate/></X509Data></K
81 eyInfo><Object Id="TIES">'
82
83 tmplt_suffix='</Object></Signature>'
84
85 echo -n "$tmplt_prefix" >> $pre_sign_tmplt
86
87 is_newline_needed=0
88 xml_decl_checked=0
89 line=
90 while IFS= read -r line
91 do
92     if [[ $xml_decl_checked -eq 0 ]]; then
93         xml_decl_checked=1
94         line="echo ${line#<?xml*?>}"
95         if [[ ! -z "$line" ]]; then
96             echo -n "$line" >> $pre_sign_tmplt
97             is_newline_needed=1
98         fi
99     else
100         if [[ is_newline_needed -eq 1 ]]; then echo >> $pre_sign_tmplt; fi
101         echo -n "$line" >> $pre_sign_tmplt
102         is_newline_needed=1
103     fi
104 fi

```



```

101 done < $UNSIGNED_XML_IN
102
103 #last line
104 line=`echo -n "$line"|xargs`
105 if [[ ! -z "$line" ]]; then
106     if [[ is_newline_needed -eq 1 ]]; then echo >> $pre_sign_tmplt; fi
107     echo -n "$line" >> $pre_sign_tmplt
108 fi
109
110 if [[ "$?" -ne 0 ]]; then echo "ERROR: last command failed"; exit $?; fi
111
112 echo -n "$tmplt_suffix" >> $pre_sign_tmplt
113
114 echo;echo "creating signature template file '$pre_sign_tmplt' for xmlsec
115 signing....done"
116
117 #####
118
119 echo;echo "signing '$pre_sign_tmplt' to create signed xml '$signed_xml'...."
120
121 # sign with xmlsec
122 if [[ $MY_PRIVATE_KEY_ALIAS -eq "" ]]; then
123     CMD="xmlsec1 --sign --pkcs12 $MY_PRIVATE_KEYSTORE_PKCS12_IN --pwd
124 $MY_PRIVATE_KEYSTORE_PWD_IN --output $signed_xml $pre_sign_tmplt"
125 else
126     CMD="xmlsec1 --sign --pkcs12:$MY_PRIVATE_KEY_ALIAS
127 $MY_PRIVATE_KEYSTORE_PKCS12_IN --pwd $MY_PRIVATE_KEYSTORE_PWD_IN --output
128 $signed_xml $pre_sign_tmplt"
129 fi
130
131 echo;echo $CMD;$CMD
132
133 if [[ "$?" -ne 0 ]]; then
134     echo "!!!! please fix the error !!!!!";echo $CMD;echo
135     rm -f $pre_sign_tmplt $signed_xml

```

```

136     exit 1
137 fi
138
139 echo; echo "signing '$pre_sign_tmplt' to create signed xml
140 '$signed_xml'....done"; echo
141
142 #####
143 # GYPAS_TIES_SA 3.2      DUOMENŲ PAKETO PARENGIMO ŽINGSNIAI
144 #      1.2 - SUARCHYVUOTI XML FAILĄ
145 #
146 # compress $signed_xml to $compressed_signed_xml
147 #####
148
149 echo "compressing '$signed_xml' to create '$compressed_signed_xml'...."
150
151 CMD="zip -q $compressed_signed_xml $signed_xml"
152
153 echo;echo $CMD;$CMD
154
155 if [[ "$?" -ne 0 ]]; then
156     echo "!!!! please fix the error !!!!";echo $CMD;echo
157     rm -f $pre_sign_tmplt $signed_xml $compressed_signed_xml
158     exit 1
159 fi
160
161 echo; echo "compressing '$signed_xml' to create
162 '$compressed_signed_xml'....done"; echo
163
164 #####
165 # GYPAS_TIES_SA 3.2      DUOMENŲ PAKETO PARENGIMO ŽINGSNIAI
166 #      1.3 - UŽŠIFRUOTI XML FAILĄ SU AES-256 RAKTU
167 #
168 # encrypt $compressed_signed_xml
169 #      - create 32 bytes AES key, AESKEY
170 #      - create 16 bytes Initialization Vector, IV, used for CBC encryption

```

```

171 # - encrypt $compressed_signed_xml using CBC with $AESKEY, $IV. encrypted
172 file output is $payload_file
173 # - append $IV to $AESKEY and encrypt resulting $AESKEYIVBIN with receiver's
174 PKI public key, $RECEIVER_PUBLIC_CERT_IN. output file is $key_file
175 #####
176
177 echo "encrypting '$compressed_signed_xml'...."
178
179 # Create 32 bytes random AES key
180 TMP=`openssl rand 32 -hex`
181 AESKEY=`echo ${TMP:0:64}`
182
183 # Create 16 bytes random Initialization Vector (IV)
184 TMP=`openssl rand 16 -hex`
185 IV=`echo ${TMP:0:32}`
186
187 echo; echo "AESKEY=$AESKEY"; echo "IV=$IV";
188
189 # Encrypt payload with key AESKEY and iv IV
190 CMD="openssl enc -e -aes-256-cbc -in $compressed_signed_xml -out $payload_file -
191 K $AESKEY -iv $IV"
192
193 echo;echo $CMD;$CMD
194
195 if [[ "$?" -ne 0 ]]; then
196     echo "!!!! please fix the error !!!!";echo $CMD;echo
197     rm -f $pre_sign_tmplt $signed_xml $compressed_signed_xml $payload_file
198     exit 1
199 fi
200
201 # Concatenate 32 bytes AESKEY and 16 bytes IV
202 AESKEYIV=`echo -n "$AESKEY$IV"`
203
204 # Convert AESKEY+IV hex to binary
205 AESKEYIVBIN=`echo ${key_file}.aeskeyivbin`

```

```

206 #echo;echo "echo -n $AESKEYIV|perl -pe '\$_=pack(\"H*\",\$_)' > $AESKEYIVBIN"
207 #echo -n $AESKEYIV|perl -pe '\$_=pack("H*",\$_)' > $AESKEYIVBIN
208 echo;echo "echo -n $AESKEYIV|xxd -r -p > $AESKEYIVBIN"
209 echo -n $AESKEYIV|xxd -r -p > $AESKEYIVBIN
210
211 #####
212 # GYPAS_TIES_SA 3.2      DUOMENŲ PAKETO PARENGIMO ŽINGSNIAI
213 #      2.1 - UŽŠIFRUOTI AES RAKTĄ IR PRADINĮ VEKTORIŲ SU VMI VIEŠUOJU 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
220 echo;echo $CMD;$CMD
221
222 if [[ "$?" -ne 0 ]]; then
223     echo "!!!! please fix the error !!!!";echo $CMD;echo
224     rm -f $pre_sign_tmplt $signed_xml $compressed_signed_xml $payload_file
225     $AESKEYIVBIN $key_file
226     exit 1
227 fi
228
229 echo; echo "encrypting '$compressed_signed_xml'....done"; echo
230
231 #####
232 # GYPAS_TIES_SA 3.2      DUOMENŲ PAKETO PARENGIMO ŽINGSNIAI
233 #      3.1 - SUKURTI GALUTINĮ PAKETĄ, KURIS BUS SIUNČIAMAS
234 #
235 # create TIES $pkg_file which contains following files compressed
236 #      - $payload_file
237 #      - $key_file
238 #####
239
240 echo "creating pkg '$pkg_file'....."

```

241

242 `CMD="zip -q $pkg_file $payload_file $key_file"`

```
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 (Algoritimų 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 (Algoritimų 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
21     echo "please see test_unpack.sh....set at least these variables
    TIES_PKG_IN, 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 $MY_PRIVATE_KEYSTORE_PKCS12_IN does
33 not exit"
    exit 1
34 fi
35
36 echo "unzipping '$TIES_PKG_IN'...."
37
38 declare -a arr=(`unzip -Z2 ${TIES_PKG_IN}`)
39
40 i=0
41 while true; do
42     tmp=${arr[$i]#*_}
43     tmp="${tmp//${'\r'}/}"
44     # Equality Comparison
45     if [[ ${tmp} = Payload ]]; then
46         payload_file=${arr[$i]}

```

```

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

```



```

81 #####
82
83 private_key_pem_file=`echo ${key_file}.pem`
84
85
86
87 CMD="openssl pkcs12 -in $MY_PRIVATE_KEYSTORE_PKCS12_IN -nocerts -passin
88 pass:$MY_PRIVATE_KEYSTORE_PWD_IN -nodes" > $private_key_pem_file
89
90 echo;echo "$CMD > $private_key_pem_file";$CMD > $private_key_pem_file
91
92 if [[ "$?" -ne 0 ]]; then
93     echo "!!!! please fix the error !!!!!";
94     echo;echo "$CMD > $private_key_pem_file";$CMD > $private_key_pem_file
95     rm -f $key_file $payload_file $private_key_pem_file
96     exit 1
97 fi
98
99 echo;echo "extracting private key from keystore
100 '$MY_PRIVATE_KEYSTORE_PKCS12_IN'....done"
101
102 echo;echo "decrypting '$key_file' using private key from
103 '$private_key_pem_file'...."
104
105 CMD="TMP=`openssl rsautl -decrypt -in $key_file -inkey $private_key_pem_file
106 | perl -pe '\$_=unpack("H*",\$_)'\`"
107
108 echo;echo $CMD;
109
110 TMP=`openssl rsautl -decrypt -in $key_file -inkey $private_key_pem_file|perl -
111 pe '\$_=unpack("H*", \$_)'\`
112
113
114 if [[ "$?" -ne 0 ]]; then
115     echo "!!!! please fix the error !!!!!";echo $CMD;echo
116     rm -f $key_file $payload_file $private_key_pem_file
117     exit 1
118 fi
119
120

```

```

109 # Extract 32 bytes AESKEY and 16 bytes IV
110 AESKEY2DECRYPT=`echo ${TMP:0:64}`
111 IV2DECRYPT=`echo ${TMP:64:96}`
112
113 #####
114 # GYPAS_TIES_SA 3.3      DUOMENŲ PAKETO IŠPAKAVIMO ŽINGSNIAI
115 #          3.1 - IŠŠIFRUOTI ARCHYVUOTĄ XML FAILĄ SU ANKSTESNIAME ŽINGSNYJE
116 IŠŠIFRUOTU AES-256 RAKTU
117 #
118 # Decrypt payload using D_AESKEY and D_IV
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 echo;echo $CMD;$CMD
125
126 if [[ "$?" -ne 0 ]]; then
127     echo "!!!! please fix the error !!!!!";echo $CMD;echo
128     #rm -f $key_file $payload_file $private_key_pem_file
129     exit 1
130 fi
131
132 # Check if payload_zip_file are created
133 if [[ ! -f $payload_zip_file ]]; then
134     echo "!!!! please fix the error !!!!!";echo $CMD;echo
135     rm -f $key_file $payload_file $private_key_pem_file
136     exit 1
137 fi
138
139 echo;echo "decrypting '$key_file' using private key from
140 '$private_key_pem_file'....done"
141
142 #####
143 # GYPAS_TIES_SA 3.3      DUOMENŲ PAKETO IŠPAKAVIMO ŽINGSNIAI

```

```

#          4.1 - IšARCHYVUOTI IšŠIFRUOTĄ FAILĄ 00000000000_PAYLOAD.ZIP
142 #
143 #####
144
145 echo;echo "unzipping '$payload_zip_file'...."
146
147 CMD="unzip -oq $payload_zip_file"
148
149 echo;echo $CMD;$CMD
150
151 payload_xml_file=${payload_file}.xml
152
153 # Check if $payload_xml_file is created
154 if [[ "$?" -ne 0 || ! -f $payload_xml_file ]]; then
155     echo "!!!! please fix the error !!!!";echo $CMD;echo
156     rm -f $key_file $payload_file $private_key_pem_file
157     exit 1
158 fi
159
160 echo;echo "unzipping '$payload_zip_file'....done"
161
162 #####
163 # GYPAS_TIES_SA 3.3      DUOMENŲ PAKETO IšPAKAVIMO ŽINGSNIAI
164 #          5.1 - Naudojant teikėjo (VMI) viešąjį rakta patikrinti parašą
165            įsitikinant siuntėjo ir duomenų paketo autentiškumu.
166 #
167 #####
168
169     error_flag=0
170
171 if [[ ! -z $SENDER_PUBLIC_CERT_IN && -f $SENDER_PUBLIC_CERT_IN ]]; then
172     echo;echo "verifying signature of '$payload_xml_file'...."
173
174     CMD="xmlsec1 --verify --pubkey-cert-der $SENDER_PUBLIC_CERT_IN
175 $payload_xml_file"

```

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