

Sistema: **LT ID**  
**IDENTIFIKAVIMO IR PASIRAŠYMO PASLAUGA**

Pavadinimas: **Serviso vadovas**

Versija: **1.4**

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

### Versijų istorija

Versija	Data	Aprašymas	Autorius
1.0	2023-08-01	Pirma versija	Renatas Zinatulinas
1.1	2023-08-24	Papildyta SOAP užklausų pavyzdžiais	Zenonas Jodko
1.2	2023-11-22	Patikslintas MAC formavimo aprašymas, metodas „Status“ pakeistas į „StatusLTID“ metoda, papildyti MAC formavimo ir tikrinimo pavyzdžiai	Renatas Zinatulinas
1.3	2024-03-01	Atnaujintas žiniatinklio paslaugų serverio adresas užklausų pavyzdžiuose	Domas Inta
1.4	2024-03-25	Sukurtas naujas CancelLTID metodas, skirtas atšaukti inicijuotų SignLTID ar LoginLTID metodų vykdymą.	Valdas Žekonis

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

## Turinys

1. Įvadas .....	5
1.1. Tikslas .....	5
1.2. Apibrėžimai, akronimai, santrumpos .....	5
2. Reikalavimai Paslaugų Tiekėjui norint naudotis LT ID servisu .....	7
2.1. Integracija .....	7
2.2. Licencijos .....	7
3. Kaip pradėti naudotis LT ID servisu .....	8
4. LT ID servisas .....	9
4.1. Serviso teikiamos paslaugos .....	9
4.2. Paslaugos veiksmo atšaukimas .....	9
4.3. Serviso diagnostika .....	9
4.4. LT ID serviso specifikacija .....	9
4.4.1. Specialusis parametras MAC .....	10
4.4.2. Enumeracijos naudojamos serviso metoduose .....	12
4.4.2.1. HashType .....	12
4.4.2.2. StatusType .....	13
4.4.3. Parametrų tipai naudojami serviso metoduose .....	13
4.4.3.1. ErrorResult .....	13
4.4.3.2. SPInfo .....	14
4.4.3.3. InitResult .....	14
4.4.3.4. GetDatesResult .....	14
4.4.3.5. PersonInfoLTID .....	14
4.4.3.6. SessionResult .....	15
4.4.3.7. StatusResultLTID .....	15
4.4.3.8. CertificatesResult .....	15
4.4.4. Galimos klaidos .....	16
4.4.5. „Init“ SOAP metodas .....	17
4.4.6. „GetLicenseDates“ SOAP metodas .....	19
4.4.7. „StatusLTID“ SOAP metodas .....	21
4.4.8. „Cancel“ SOAP metodas .....	23
4.4.9. „CancelLTID“ SOAP metodas .....	24
4.4.10. „Test“ SOAP metodas .....	26
4.4.11. „LoginLTID“ SOAP metodas .....	28
4.4.12. „SignLTID“ SOAP metodas .....	31
4.4.13. „GetCertificatesLTID“ SOAP metodas .....	34
4.4.14. „Init“ REST metodas .....	36
4.4.15. „GetLicenseDates“ REST metodas .....	38
4.4.16. „StatusLTID“ REST metodas .....	39
4.4.17. „Cancel“ REST metodas .....	42
4.4.18. „CancelLTID“ REST metodas .....	43
4.4.19. „Test“ REST metodas .....	45
4.4.20. „LoginLTID“ REST metodas .....	47
4.4.21. „SignLTID“ REST metodas .....	50
4.4.22. „GetCertificatesLTID“ REST metodas .....	53

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

Priedas A. Viešųjų raktų formatai.....56

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

## 1. Įvadas

### 1.1. Tikslas

Šio dokumento tikslas – pateikti klientams (bankams, elektroninėms parduotuvėms, valstybinėms įstaigoms ir kt.) LT ID žiniatinklio paslaugų aprašymą ir paaiškinti, kaip kurti integracines sąsajas su LT ID infrastruktūra. .

### 1.2. Apibrėžimai, akronimai, santrumpos

#### Santrumpos:

<b>WS</b>	Web Service
<b>SOAP</b>	Simple Object Access Protocol
<b>REST</b>	Representational state transfer
<b>RA</b>	Registration Authority/ Registered Agreement
<b>PKCS</b>	Public Key Cryptography Standards
<b>WSDL</b>	Web Services Description Language
<b>OCSP</b>	Online Certificate Status Protocol

#### Apibrėžimai:

<b>Paslaugos Tiekėjas</b>	Šalis, kuri teikia galutiniams Naudotojams e-parašu pagrįstas paslaugas (angl. <b>Service Provider</b> ).
<b>Sertifikavimo tarnyba</b>	Aukšto saugumo lygio sistema, išduodanti skaitmeninius liudijimus apie kriptografinių raktų atitikimą fiziniams asmenims bei publikuojanti šiuos liudijimus internete (angl. <b>Certification Authority (CA)</b> ).
<b>Patikimas Paslaugų Tiekėjas</b>	Patikimų paslaugų tiekėjas, teikiantis viešojo rakto infrastruktūros paslaugas, tarpininkaujantis tarp Paslaugų Tiekėjo ir Viešojo Rakto Infrastruktūros elementų (angl. <b>Trusted Service Provider (TSP)</b> ).
<b>Naudotojas</b>	Fizinis (Juridinis) asmuo, turintis kvalifikuotą elektroninį LT ID parašą (spaudą).

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

<b>LT ID aktyvavimo įrenginys</b>	Mobiliojo ryšio telefonas ar personalinis kompiuterius, kuriame įdiegtas LT ID programinis paketas, skirtas aktyvuoti LT ID el. parašo ar spaudo duomenų kūrimą LT ID infrastruktūroje.
<b>LT ID servisas</b>	Šioje dokumentacijoje aprašytas LT ID žiniatinklio paslaugų rinkinys

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

## **2. Reikalavimai Paslaugų Tiekėjui norint naudotis LT ID servisu**

Paslaugų Tiekėjas, norintis naudotis šiuo servisu, turi turėti pastovų interneto ryšį. Paslaugų Tiekėjo informacinė sistema gali būti realizuota nepriklausomai nuo Patikimo Paslaugų Tiekėjo (TSP), bet ji privalo teisingai palaikyti sąsają su servisu, kad būtų užtikrintas saugus ir teisingas bendravimas.

### **2.1. Integracija**

LT ID servisas turi dvejetainę web service sąsają - veikiančią RESTful architektūros stiliumi ir veikiančią SOAP protokolu. Šiame serviso vadove yra pateikiami tiek RESTful tiek ir SOAP protokolu veikiančių LT ID serviso metodų aprašymai. LT ID servisas naudoja sudėtingus tipus kaip, kad bitų masyvą (`byte[]`) ir enumeraciją (`enum`), todėl verta atkreipti dėmesį, ar jūsų naudojama programavimo kalba turi atitinkamas bibliotekas.

### **2.2. Licencijos**

Licencija – tai elektroninis dokumentas, kuris yra saugomas Patikimo Paslaugų tiekėjo duomenų bazėje. Kiekvienas Paslaugų Tiekėjas, norintis naudotis LT ID serviso teikiamomis paslaugomis, privalo susitarti dėl licencijos. Prieš tai Paslaugų Tiekėjas privalo suteikti tam tikrą informaciją apie save, o kai licencija būna sukurta, jis gaus tam tikrus duomenis, kurie bus reikalingi naudojantis servisu. Kokius duomenis reikia suteikti ir kokie duomenys minimi licencijoje, skaitykite sk. [3](#).

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

### 3. Kaip pradėti naudotis LT ID servisu

Norėdamas pradėti naudotis šio serviso teikiamomis paslaugomis Paslaugų Tiekėjas turi atlikti šiuos žingsnius:

1. Susisiekti su Patikimu Paslaugų Tiekėju dėl licencijos parametrų ir sąlygų ;
2. Licencijai parengti Paslaugų Tiekėjas turės pateikti šią informaciją:
  - a. licencijos savininko pavadinimą;
  - b. (neprivaloma) Paslaugų Tiekėjo pageidaujamas licencijos galiojimo datas:
    - i. licencijos galiojimo pradžios datą;
    - ii. licencijos galiojimo pabaigos datą;
3. Patikimam Paslaugų Tiekėjui (TSP) sukūrus licenciją Paslaugų Tiekėjui, Paslaugų Tiekėjas gaus šiuos duomenis:
  - a. LT ID web serviso URL adresą;
  - b. licencijos serijinį numerį (pvz., EL-321E3-38F2E-86920);
  - c. (neprivaloma) licencijos galiojimo datas;

Taip pat Paslaugų Tiekėjas:

1. Privalo susipažinti su šia dokumentacija.
2. Ištestuoti savo informacinę sistemą kartu su sąsaja, nes Paslaugų Tiekėjas atsako už sklandų Naudotojo darbą su sistema.
3. Sukonfigūruoti savo darbinę aplinką, kad būtų galima bendrauti su LT ID servisu.

Atlikus šiuos veiksmus, kliento Naudotojai galės pradėti naudotis LT ID kvalifikuoto elektroninio parašo paslaugomis.

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

## 4. LT ID servisas

### 4.1. Serviso teikiamos paslaugos

LT ID servisą galima naudoti sekančioms paslaugoms:

1. autentifikacijai;
2. pasirašymui;
3. sertifikatų gavimui;

**Autentifikacija** – paslauga, naudojama kviečiant web serviso metodą „LoginLTID“. Ši paslauga leidžia Paslaugų Tiekėjui siųsti autentifikacijos užklausas į Naudotojo LT ID aktyvavimo įrenginį. Naudotojas pasirašo perduotus autentifikacijos duomenis ir grąžina atsakymą, tuo tarpu Patikimas Paslaugų Tiekėjas pateikia informaciją Paslaugų Tiekėjui apie įvykusių užklausa.

**Pasirašymas** – paslauga, naudojama kviečiant web serviso metodą „SignLTID“. Ši paslauga leidžia Paslaugų Tiekėjui siųsti pasirašymo užklausas į Naudotojo LT ID aktyvavimo įrenginį. Naudotojas pasirašo perduotus duomenis pasirašymui ir grąžina atsakymą, tuo tarpu Patikimas Paslaugų Tiekėjas pateikia informaciją Paslaugų Tiekėjui apie įvykusių užklausa.

**Sertifikatų gavimas** – paslauga, naudojama kviečiant web serviso metodą „GetCertificatesLTID“. Ši paslauga leidžia Paslaugų Tiekėjui gauti Naudotojo sertifikatą.

### 4.2. Paslaugos veiksmo atšaukimas

Naudotojui vykdant pasirinktą paslaugą gali iškilti įvairiausių trukdžių, todėl Naudotojas turi turėti galimybę atšaukti savo pradėta veiksmą. Šiems atšaukimo atvejams skirtas metodas „Cancel“ (aprašą žiūrėti skyriuose [4.4.8](#), [4.4.9](#), [4.4.17](#) ir [4.4.18](#)).

### 4.3. Serviso diagnostika

Naudojantis LT ID serviso paslaugomis gali iškilti įvairiausių situacijų, dėl kurių gali sutrikti autentifikacijos ar pasirašymo paslaugos naudojimas. Serviso diagnostikai buvo įgyvendintas metodas „Test“ (aprašą žiūrėti skyriuose [4.4.10](#) ir [4.4.19](#)). Šią diagnostiką galima atlikinėti reguliariai, tai pagreitins problemų identifikavimą ir sprendimą.

### 4.4. Serviso specifikacija

Web servisas turi šiuos metodus:

- Init SOAP (žr. sk. [4.4.5](#));

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

- GetLicenseDates SOAP (žr. sk. [4.4.6](#))
- StatusLTID SOAP (žr. sk. [4.4.7](#))
- Cancel SOAP (žr. sk. [4.4.8](#))
- CancelLTID SOAP metodas (žr. sk. [4.4.9](#))
- Test SOAP (žr. sk. [4.4.10](#))
- LoginLTID SOAP ( žr. sk. [4.4.11](#))
- SignLTID SOAP (žr. sk. [4.4.12](#))
- GetCertificatesLTID SOAP (žr. sk. [4.4.13](#))
- Init REST (žr. sk. [4.4.14](#));
- GetLicenseDatesLTID REST (žr. sk. [4.4.15](#))
- StatusLTID REST (žr. sk. [4.4.16](#))
- Cancel REST (žr. sk. [4.4.17](#))
- CancelLTID REST metodas (žr. sk. [4.4.18](#))
- Test REST (žr. sk. [4.4.19](#))
- LoginLTID REST (žr. sk. [4.4.20](#))
- SignLTID REST (žr. sk. [4.4.21](#))
- GetCertificatesLTID REST (žr. sk. [4.4.22](#))

#### 4.4.1. Specialusis parametras MAC

Parametras MAC (angl. *Message authentication code*) yra į visus metodus paduodamo parametro SPInfo sudedamoji dalis. SPInfo sudaro du parametrai: licencijos numeris (angl. *License number*) ir MAC. Licencijos numeris visada vienodas (tai numeris priskirtas Paslaugų Tiekėjui registruojant licenciją), o parametras MAC yra formuojamas iš naujo kiekvienai užklausiai atskirai. MAC parametras taip pat yra kiekvienos užklaustos grąžinamo atsakymo sudedamoji dalis.

MAC parametro tikslas yra užtikrinti saugų bendravimą. Panašus principas naudojamas bankiniame B2B HTTP bendravime apsaugoti nuo duomenų praradimo ar tyčinio pakeitimo. O perduodant šį parametą kartu su licencijos numeriu, įmanoma autentifikuoti ir atpažinti Paslaugų Tiekėją, kuris naudojami jam sukurta licencija.

Norint teisingai formuoti MAC, reikia atlikti šiuos veiksmus:

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

1. Gauti visus parametrus, perduodamus į vieną metodą; labai svarbi yra perduodamų parametų tvarka.

2. Toliau visus parametrus reikia paversti į duomenų eilutę (angl. *string*), gautoje duomenų eilutėje didžiosios ir mažosios raidės traktuojamos skirtingai. Tam tikrus tipus paversti reikia vadovaujantis šiomis taisyklėmis:

a. Jeigu parametro reikšmė yra tuščia, pavyzdžiui „" ar (null), jis MAC formavime nedalyvauja;

b. string → string, vertimas nebūtinai, bet eilutę reiktų saugoti UTF-8 koduotėje;

c. int → string, pavyzdžiui 2 į „2“;

d. real → string, pavyzdžiui 2,25 į „2,25“;

e. bool → string, laikomės žodinės išraiškos. Galimos reikšmės „True“, „False“;

f. byte[] → string, kadangi įvairiose koduotėse bitų masyvas gali būti verčiamas skirtingai, mes pasitelkėme Base64 šifravimą. Galutinė reikšmė būtų Base64 šifruota eilutė, pavyzdžiui „YWE=“;

g. string[] (List<string>) → string, iš eilučių masyvo padarome vieną eilutę paprasčiausiai visas masyvo eilutes sujungdami iš eilės;

h. date → string; datos gali būti atvaizduotos pagal skirtingus regioninius nustatymus, mes vaizduosime pagal Lietuvos regioną. Datą verčiame vadovaudamiesi formatu „yyyy.MM.dd HH:mm:ss“;

i. enum → string, enumeratoriuose visi pasirinkimai verčiami į žodinę išraišką, pvz.: „Asynchronous“, „SHA512“;

j. jei parametras sudarytas iš kelių sudedamųjų parametru, sudedamieji parametrai vienas paskui kita surašomi pagal aukščiau pateiktas taisykles.

3. Žinant, kaip versti skirtingus tipus, visus paverstus parametrus reikia sujungti į bendrą eilutę.

4. Jeigu gautoje eilutėje yra pabaigos simboliai, juos reikia pakeisti naudojantis XML taisyklėmis (<https://www.w3.org/TR/xml/>). Eilutės pabaigos simbolį turi atitikti simbolis `\\n`.

Keitimo taisyklės:

a. „\\r\\n“ keičiame į `\\n`;

b. `\\r` keičiame į `\\n`.

5. Šią suformuotą eilutę reikia pasirašyti. Pasirašymui naudojamas RSA šifras ir SHA1 maišos funkcija. RSA privatų raktą naudokite tą, kuris yra poroje su viešuoju raktu, perduotu licencijos sukūrimui;

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

6. Pasirašius, gaunamas baitų masyvas (byte[]). Tai ir yra MAC reikšmė, kuri bus naudojama į metodus perduodamame SPIInfo parametre.

Atsakymuose esantis MAC parametras suformuojamas LT ID serviso. Paslaugų Tiekėjas privalo jį patikrinti. Nepatikrinus, bus neįsitikinta ar atsakymas atėjo nepakeistas ir ar atsakymas yra iš tikrojo TSP serviso. Procedūra beveik tokia pati. Formuojant eilutę, imami iš eilės grįžę parametrai. O suformuota eilutė patikrinama su gautu serviso viešuoju raktu.

Parametrų eiliškumą matysite kituose skyreliuose, kuriuose aprašomi esami metodai.

#### 4.4.2. Enumeracijos naudojamos serviso methoduose

##### 4.4.2.1. HashType

Kviečiant metodus „LoginLTID“ arba „SignLTID“ galima nurodyti, kaip ir kokį maišos algoritmą taikyti. Maiša taikoma DTBS laukui. Norint sumažinti tinklo apkrovimą ir neperdavinėti didelio DTBS lauko, galima perduoti DTBS lauką su jau pritaikyta maiša. Tai patogiu ir tuomet, kai reikia pasirinkti specifinį maišos algoritmą. Galimos šio tipo reikšmės pateikiamos lentelėje:

Reikšmė	Aprašymas
HashedSHA256	DTBS lauko reikšmė yra perduota pritaikius SHA256 maišos algoritmą
HashedSHA384	DTBS lauko reikšmė yra perduota pritaikius SHA384 maišos algoritmą
HashedSHA512	DTBS lauko reikšmė yra perduota pritaikius SHA512 maišos algoritmą
HashedRIPEMD160	DTBS lauko reikšmė yra perduota pritaikius RIPEMD160 maišos algoritmą
SHA256	DTBS lauke perduodami pilni duomenys, o serveryje šiems duomenims pritaikomas SHA256 maišos algoritmas
SHA384	DTBS lauke perduodami pilni duomenys, o serveryje šiems duomenims pritaikomas SHA384 maišos algoritmas
SHA512	DTBS lauke perduodami pilni duomenys, o serveryje šiems duomenims pritaikomas SHA512 maišos algoritmas

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

Reikšmė	Aprašymas
RIPEMD160	DTBS lauke perduodami pilni duomenys, o serveryje šiems duomenims pritaikomas RIPEMD160 maišos algoritmas

#### 4.4.2.2. StatusType

Reikšmė	Aprašymas
Ok	sesija baigėsi sėkmingai.
Unknown	sesija dar nesibaigė.
Canceled	sesija buvo nutraukta.
Timeout	sesijos laikas pasibaigė.
Error	sesija baigėsi nesėkmingai.

#### 4.4.3. Parametrų tipai naudojami serviso metoduose

##### 4.4.3.1. ErrorResult

Pavadinimas	Tipas	Aprašymas
ErrorNumber	int	Įvykusios klaidos numeris. Skaičius gali svyruoti nuo -1 iki 1000. Sėkmingos užklauskos atveju skaičius bus 0.
ErrorMessage	string	Įvykusios klaidos aprašymas. Jeigu įvyko klaida, grįžta trumpas angliškas klaidos aprašymas. Sėkmingos užklauskos atveju šis parametras būna tuščias.
MAC	byte[]	LT ID serviso suformuotas MAC.

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

#### 4.4.3.2. SPInfo

Pavadinimas	Tipas	Aprašymas
LicenseNumber	string	Numeris priskirtas Paslaugų Tiekėjui registruojant licenciją.
MAC	byte[]	Metodui perduodamų atributų suformuotas ir pasirašytas MAC.

#### 4.4.3.3. InitResult

Pavadinimas	Tipas	Aprašymas
Error	<a href="#">ErrorResult</a>	Klaida vykdant metodą (jei Error.ErrorNumber = 0, metodas įvykdytas be klaidų).
PublicKey	string	Patikimo Paslaugų Tiekėjo licencijai naudojamas viešasis raktas.

#### 4.4.3.4. GetDatesResult

Pavadinimas	Tipas	Aprašymas
Error	<a href="#">ErrorResult</a>	Klaida vykdant metodą (jei Error.ErrorNumber = 0, metodas įvykdytas be klaidų).
DateFrom	DateTime	Data nuo kada galioja licencija.
DateTill	DateTime	Data iki kada galioja licencija.

#### 4.4.3.5. PersonInfoLTID

Pavadinimas	Tipas	Aprašymas
PersonCode	string	Naudotojo asmens kodas. Parametras privalomas.

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

Pavadinimas	Tipas	Aprašymas
CompanyCode	string	Įmonės kodas. Paduodamas el. spaudo kūrimo atvejais Parametras neprivalomas.

#### 4.4.3.6. SessionResult

Pavadinimas	Tipas	Aprašymas
Error	<a href="#">ErrorResult</a>	Klaida vykdant metodą (jei Error.ErrorNumber = 0, metodas įvykdytas be klaidų).
SessionNumber	int	Pasirašymo arba autentifikacijos sesijos numeris.

#### 4.4.3.7. StatusResultLTID

Pavadinimas	Tipas	Aprašymas
Error	<a href="#">ErrorResult</a>	Klaida vykdant metodą (jei Error.ErrorNumber = 0, metodas įvykdytas be klaidų).
Status	<a href="#">StatusType</a>	Enumeratoriaus reikšmė parodanti esamą sesijos būseną.
Signature	string[][]	Kriptografinis parašas. Gražinama tiek parašų / spaudų, kiek buvo paduota dokumentų pasirašymui / spaudavimui.
Certificate	string	Naudotas sertifikatas.
OCSPResponse	byte[]	Nenaudojamas
OCSPCertificate	string	Nenaudojamas

#### 4.4.3.8. CertificatesResult

Pavadinimas	Tipas	Aprašymas
Error	<a href="#">ErrorResult</a>	Klaida vykdant metodą (jei Error.ErrorNumber = 0, metodas įvykdytas be klaidų).

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

Pavadinimas	Tipas	Aprašymas
CertificateAUT	string	Nenaudojamas
CertificateSIG	string	Sertifikatas, skirtas pasirašymui / spaudavimui.

#### 4.4.4. Galimos klaidos

Žemiau esančioje lentelėje pateikiamos galimos klaidos. Šių klaidų numeriai ir aprašymai sutampa visuose metoduose.

Numeris	Trumpinys	Aprašymas
0	OK	Užklausa baigėsi sėkmingai.
-1	INTERNAL_ERROR	Nenumatyta sisteminė klaida.
1	WRONG_PARAM	Klaidingas perduotas parametras. Klaidos tekstas gali varijuoti priklausomai nuo situacijos.
2	MISSING_PARAM	Neperduotas būtinas parametras. Klaidos tekstas gali varijuoti priklausomai nuo situacijos.
3	WRONG_DATA_LENGTH	Paduotas parametras didesnis už licencijoje numatytą maksimalų dydį. Klaidos pranešime nurodomas koks yra maksimalus dydis.
4	INAPPROPRIATE_DATA	Neteisingas perduoto parametro formatas. Klaidos tekstas gali varijuoti priklausomai nuo situacijos.
5	UNSUPPORTED	Nepalaikoma funkcija ar parametro tipas. Klaidos tekstas gali varijuoti priklausomai nuo situacijos.
11	CERTIFICATE_NOT_FOUND	Asmens sertifikatas nerastas.
12	CERTIFICATE_REVOKED	Asmens sertifikato galiojimas yra atšauktas
13	CERTIFICATE_EXPIRED	Asmens sertifikato galiojimas yra pasibaigęs

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

Numeris	Trumpinys	Aprašymas
14	CERTIFICATE_PERSONCODE_DIFFERENCES	Asmens kodas įrašytas sertifikate nesutampa su perduotuoju asmens kodu.
50	LICENSE_CHECK_MAC_FAILED	Parametro MAC patikra nepavyko, bloga MAC reikšmė arba RSA raktai.
51	LICENSE_NOT_FOUND	Licencija nerasta. Perduotas blogas numeris arba licencija dar nesukurta.
52	LICENSE_KEYS_NOT_FOUND	Licencijos raktų pora nerasta, arba trūksta vieno iš poros raktų.
53	LICENSE_NOT_ACTIVE	Licencijos statusas yra neaktyvus, reiškia, kad šiuo momentu licencijos naudojimas sustabdytas.
54	LICENSE_NOT_VALID_PERIOD	Licencija šiuo laikotarpiu negalioja, reiškia, kad šiuo momentu licencijos naudojimas sustabdytas.
55	LICENSE_UNAUTHORIZED	Licencija draudžia prieigą prie veiksmų ar funkcijų. Klaidos tekstas gali varijuoti priklausomai nuo situacijos.
56	LICENSE_ALREADY_INITIALIZED	Negalima inicializuoti licencijos, nes tai jau yra atlikta.

#### 4.4.5. „Init“ SOAP metodas

„Init“ metodas skirtas automatizuoti Paslaugų Tiekėjo ir Patikimo Paslaugų Tiekėjo viešųjų raktų apsikeitimą.

„Init“ metodas yra vienetinis. Tai reiškia, kad šį metodą galima kviesti tik vieną kartą per licencijos gyvavimą. Pakartotinas jo kvietimas, pvz., pasikeitus Paslaugų Tiekėjo arba Patikimo Paslaugų Tiekėjo raktams, galimas tik susitarus su Patikimu Paslaugų Tiekėju.

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

„Init“ metodo užklauso parametrai:

Pavadinimas	Tipas	Aprašymas
SP	<a href="#">SPInfo</a>	Perduodamas licencijos numeris, kuris buvo gautas iš Patikimo Paslaugų Tiekėjo, ir MAC suformuotas iš licencijos numerio ir PublicKey parametro pasirašytos eilutės.
PublicKey	string	Paslaugų Tiekėjo viešasis raktas, kurį jis perduoda Patikimam Paslaugų Tiekėjui. Palaikomi viešojo rakto formatai pateikti <a href="#">priede A</a> .

Visi parametrai privalomi.

Užklauso pavyzdys:

```
<x:Envelope
  xmlns:x="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:tsp="http://tsp.etrionika.net/">
  <x:Header/>
  <x:Body>
    <tsp:Init>
      <tsp:SP>
        <tsp:LicenseNumber>EL-E2523-9E792-7B212</tsp:LicenseNumber>

        <tsp:MAC>JLVLnDsw3zeCxwi5GMNWKp4v8Pii4CqM+9lpw/whtUnp3nu1w6/RyheWPmLBLHaL0v/cYigLNeQilk
        UiQ/NbjgElKp8twj8DJOG+qK3umuG13+pl+bukYsbsowNTamE70DefXTXqeWkzHIN3rwzR/elvuiebTQxjCfv3P
        3r0Qf5kQZDPjcz/+4dJ/MlscwJyndXcZfQe/aUV6cwR8Ry4P/0eYqCznMQ1Cr6sACDWx2fh8o7rjXHTAgGcG7aV
        0sg2XLWjkXB6S1RX1tNKaOQf2oCjBcKfw9c8U3PZnXQfhe+fNX1M5CD9ns0Es08ae7EuOvsQMbHvwtk7V317b1
        sXQ==</tsp:MAC>

      </tsp:SP>
      <tsp:PublicKey>-----BEGIN PUBLIC KEY-----
        MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAAuCl9w+d+GZf58es/tFT3
        L83tiJ7UNshiSh6PVfjz60om/G6tuWc7KIKdEVy2IWZw5OGBIksfKSLQR6leL9Bo
        tovMyRZb3ipGMiXewaVP+8y0HtkXn8jQWshF3TddckfQ+51cLJ/fiwu/CHmLSzTp
        wiphUPAU5YKmg5cmhw1OGXctBqhUbr5ueiIKNYyMXtr+PLqWMFw+weyM54P77dAj
        bM9tY0PsvhYOMCLEyGUprFHag3Oz5jJhf6jSxkTVikw0iFA+WD/Ojv8KWX9Uo4j9
        sI5s01ocGuGyH8MUGurqe0FkFIC9JtR+ijc46M7R5bkFkdGx5ftUCBKEJGJ+mENT
        kQIDAQAB
        -----END PUBLIC KEY-----
      </tsp:PublicKey>
    </tsp:Init>
  </x:Body>
</x:Envelope>
```

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

MAC reikšmė susideda iš privačiuoju raktu pasirašytos eilutės: LicenseNumber + PublicKey.

Atsakymo pavyzdys:

```
<s:Envelope
  xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
  <s:Body>
    <InitResponse
      xmlns="http://tsp.etrionika.net/"
      <InitResult
        xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
          <Error>
            <ErrorNumber>56</ErrorNumber>
            <ErrorMessage>Public key already exists.</ErrorMessage>
            <MAC i:nil="true"/>
          </Error>
          <PublicKey i:nil="true"/>
        </InitResult>
      </InitResponse>
    </s:Body>
  </s:Envelope>
```

„Init“ metodo grąžinamas atsakymo rezultatas – [InitResult](#).

#### 4.4.6. „GetLicenseDates“ SOAP metodas

„GetLicenseDates“ metodas skirtas palengvinti Paslaugų Tiekėjo informavimą apie licencijos galiojimo periodą. Grąžinamos licencijos galiojimo pradžios ir pabaigos datos.

„GetLicenseDates“ metodo užklausos parametrai:

Pavadinimas	Tipas	Aprašymas
SP	<a href="#">SPInfo</a>	Perduodamas licencijos numeris, kuris buvo gautas iš Patikimo Paslaugų Tiekėjo, ir MAC suformuotas iš licencijos numerio parametro pasirašytos eilutės.

Visi parametrai privalomi.

Užklausos pavyzdys:

```
<x:Envelope
  xmlns:x="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:tsp="http://tsp.etrionika.net/"
  <x:Header/>
```

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

```

<x:Body>
  <tsp:GetLicenseDates>
    <tsp:SP>
      <tsp:LicenseNumber>EL-E2523-9E792-7B212</tsp:LicenseNumber>

<tsp:MAC>Twia+NEyXcs3sxVHc9Hy7JbfUD3UqiptxnN2prQpwavEdsdr8gYdxrw7Y55pbGCaVTzPGbSuAxeHFG
MeA0eVfKlJRxjiELxQ+jWUGXqtoJBjVCwASnsQNE3e0mxWTLYY7ZoeuAJMcI5eQN/Yh60keBLTBcm18j5OXtrXS
c0Y1qGQl8Tr40cjdeOm6IXZEMRjeg/9af6cbX/xb4Tv14xhK+Y4N3H82tWhEGKuXSQZ0selN1vNdSM0Rc1NepPh
WtJ17I0uryhpMFHxa30evLMRf+D8Bo5ae61RcEkiafO+XsVgEGgZuz8N/EEMk1z7UPXsJ/82Eg3aPcDqFu1LmNs
NNQ==</tsp:MAC>
    </tsp:SP>
  </tsp:GetLicenseDates>
</x:Body>
</x:Envelope>

```

MAC reikšmė susideda iš privačiuoju raktu pasirašytos eilutės: **LicenseNumber**

Atsakymo pavyzdys:

```

<s:Envelope
  xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
  <s:Body>
    <GetLicenseDatesResponse
      xmlns="http://tsp.etrionika.net/"
      <GetLicenseDatesResult
        xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
          <Error>
            <ErrorNumber>0</ErrorNumber>
            <ErrorMessage i:nil="true"/>

<MAC>XZI0p0/BeTglEetL3vAX2SnJIGG4Vsk/rCji0hbQSXf3KKcmYOMVe2WXcgVkXrr5VMht+pG+nFGITirGkn
B81RRAzw0bIMoLCPc50tjVmJ+XNoDDi+NkaFLFoAIf2g7wQDnyEjaYKo/WeFUDndGW9bdaLGQj0to2GZGZcyQWW
SnaBStH8en3oK7s2Femicktn6c3xInUNcdPdJBSpkX6DEJQsKXy5z69KBrD9A49t/oydJniGi2AF56IIiayizo
oxaiKS18m55g07KLNuVltlpufldkOclLsgQJNPWrsGIWdOKc3rbr4901HGdFn8qXhR/qYh7JnYjhJHABKys+3w=
=</MAC>

          </Error>
          <DateFrom>2023-08-03T00:00:00</DateFrom>
          <DateTill>2030-07-31T00:00:00</DateTill>
        </GetLicenseDatesResult>
      </GetLicenseDatesResponse>
    </s:Body>
  </s:Envelope>

```

„GetLicenseDates“ metodo gražinamas atsakymo rezultatas – [GetDatesResult](#).

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

#### 4.4.7. „StatusLTID“ SOAP metodas

„StatusLTID“ metodas skirtas stebėti autentifikacijos ir pasirašymo paslaugų statusus, o taip pat gauti parašus ar papildomus laukus. Paslaugų Tiekėjas, reguliariai kviesdamas šį metodą, gali sužinoti, koks yra užklauskos statusas.

Paprastai šis metodas reguliariai kviečiamas tada, kai pasirenkamas asinchroninis kliento-serverio režimas. Tačiau jį galima naudoti ir asinchroniniame serverio-serverio režime. Pvz., jei atsakymas neateina Paslaugų Tiekėjo sukurto puslapio URL adresu, pravartu pasinaudoti „StatusLTID“ metodu.

„StatusLTID“ metodo užklauskos parametrai:

Pavadinimas	Tipas	Aprašymas
SP	<a href="#">SPInfo</a>	Perduodamas licencijos numeris, kuris buvo gautas iš Patikimo Paslaugų Tiekėjo, ir MAC suformuotas iš licencijos numerio ir sesijos numerio parametru pasirašytos eilutės.
SessionNumber	int	Sesijos numeris, kuris buvo gautas kviečiant „LoginLTID “ ar „SignLTID“ metodus. Einamosios paslaugos sekimo numeris.

Visi parametrai privalomi.

Užklauskos pavyzdys:

```
<x:Envelope
  xmlns:x="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:tsp="http://tsp.etrionika.net/">
  <x:Header/>
  <x:Body>
    <tsp:Status>
      <tsp:SP>
        <tsp:LicenseNumber>EL-E2523-9E792-7B212</tsp:LicenseNumber>

        <tsp:MAC>ejDh1/eJjRgIOaxRLnc7CxpR+PuTYqm9fr6c8+nTIXoObpLDdyZkReJqfs+5iMmdT+jxJ6pOevFXUa
        oyg5Lqg80eadURXivI4dY8jVFt+XD+h5p0ED25FJYAlSONAm1IEoCwwFE3EM3k74B9xoXdsoFFOzMdhLKTEUh6d
        oWuMUrAPpzzpoC1lFfn0Gk8+CcRw5w3XH+Ohus2B8HvNdN06uq5K+UbvXXBi5yrkA4Bw03EnaUzZUBsh7TVDt4F
        RpOM010AkJa9+XxKerpsetSHjAxVwGvXysJ0yU1Ljqu4MXtwPTdWZ0Jh9be1rRWlWwV8gFbkNnCuLn905AWC18S
        6iw==</tsp:MAC>

      </tsp:SP>
      <tsp:SessionNumber>1401285</tsp:SessionNumber>
    </tsp:Status>
```

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

```
</x:Body>
</x:Envelope>
```

MAC reikšmė susideda iš privačiuoju raktu pasirašytos eilutės: LicenseNumber + SessionID  
t.y. EL-E2523-9E792-7B2121401285

#### Atsakymo pavyzdys:

```
<s:Envelope
  xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
  <s:Body>
    <StatusResponse
      xmlns="http://tsp.etronika.net/">
      <StatusResult
        xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
        <Error>
          <ErrorNumber>0</ErrorNumber>
          <ErrorMessage i:nil="true"/>
          <MAC>Yu31BVoengAdR+rx7y7eGR1Ntg2j3nV71j4OWLDBRSdvZ9TwDZiN1Trtho6SwnZUueE9Ri1MisfthMd8jC
          iP3uXXqHx8YMMqZ7pv0/aYHGZ+FDlGCsaZftyl+/Xxv7PCubBA9eNMDr8qqpWF6WLQAeNYqPAdS2oN5GGP0KUEt
          bsOShzkwIOK2vzf3h1eKk7/pG0WP6w08T2TsGXxs5tBfCs/XTnD7dEOXwUjDosqPK/yx8wCV0fxj9aqEU0qyPw
          Mxj0ztz+Qmz673U6iPqMP/XZNbdIZWNrmsQ8claMCUyJZWLPX7YIZuHtJtRYa5Yb8GCBur8BBHnbh3Ioarsudg=
          =</MAC>
        </Error>
        <Status>Timeout</Status>
        <Signature i:nil="true"

xmlns:a="http://schemas.microsoft.com/2003/10/Serialization/Arrays"/>
        <Certificate i:nil="true"/>
        <OCSPResponse i:nil="true"/>
        <OCSPCertificate i:nil="true"/>
      </StatusResult>
    </StatusResponse>
  </s:Body>
</s:Envelope>
```

„StatusLTID“ metodo grąžinamas atsakymo rezultatas – [StatusResult](#).

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

#### 4.4.8. „Cancel“ SOAP metodas

„Cancel“ metodas skirtas atšaukti einamosios mobilaus parašo paslaugos, inicijuotos Sign ar Login metodais, vykdymą. Pavyzdžiui pradėjus vykdyti autentifikacijos ar pasirašymo paslaugą, yra gaunamas parametras „SessionNumber“, perduodant jį šiam metodui paslaugos vykdymas nutraukiamas. Su tuo pačiu sesijos numeriu bandant gauti paslaugos statusą, atsakymo statusas bus „Canceled“ (būseną – nutraukta).

Paslaugos vyksmą galima nutraukti, tik kai statusas yra „Unknown“ (vis dar vyksta).

PASTABA. Kai paslaugos statusas nėra „Unknown“ (vis dar vyksta) ir bandoma paslaugą nutraukti, tuomet metodas klaidos negrąžins ir būseną išliks nepakitusi.

„Cancel“ metodo užklauso parametrai:

Pavadinimas	Tipas	Aprašymas
SP	<a href="#">SPInfo</a>	Perduodamas licencijos numeris, kuris buvo gautas iš Patikimo Paslaugų Tiekėjo, ir MAC suformuotas iš licencijos numerio ir sesijos numerio parametrų pasirašytos eilutės.
SessionNumber	int	Sesijos numeris, kuris buvo gautas kviečiant „Login“ ar „Sign“ metodus. Einamosios paslaugos sekimo numeris.

Visi parametrai privalomi.

Užklauso pavyzdys:

```
<x:Envelope
  xmlns:x="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:tsp="http://tsp.etrionika.net/">
  <x:Header/>
  <x:Body>
    <tsp:Cancel>
      <tsp:SP>
        <tsp:LicenseNumber>EL-E2523-9E792-7B212</tsp:LicenseNumber>

        <tsp:MAC>ejDh1/eJjRgIOaxRLnc7CxpR+PuTYqm9fr6c8+nTIXoObpLDdyZkReJqfs+5iMmdT+jxJ6pOevFXUa
        oyg5Lqg80eadURXivI4dY8jVFt+XD+h5p0ED25FJYAlSONAm1IEoCwwFE3EM3k74B9xoXdsoFFOzMdhLKTEUh6d
        oWuMUrAPpzzpoC1lFfn0Gk8+CcRw5w3XH+Ohus2B8HvNdN06uq5K+UbvXXBi5yrkA4Bw03EnaUzZUBsh7TVDT4F
        RpOM010AkJa9+XxKerpsetSHjAxVwGvXYsJ0yU1Ljqu4MXtWPTdWZOJh9be1rRWlWwV8gFbkNnCuLn905AWC18S
        6iw==</tsp:MAC>
      </tsp:SP>
    </tsp:Cancel>
  </x:Body>
</x:Envelope>
```

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

```

        <tsp:SessionNumber>1401285</tsp:SessionNumber>
    </tsp:Cancel>
</x:Body>
</x:Envelope>

```

MAC reikšmė susideda iš privačiuoju raktu pasirašytos eilutės: LicenseNumber + SessionID

t.y.

EL-E2523-9E792-7B2121401285

Atsakymo pavyzdys:

```

<s:Envelope
  xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
  <s:Body>
    <CancelResponse
      xmlns="http://tsp.etronika.net/">
      <CancelResult
        xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
        <ErrorNumber>0</ErrorNumber>
        <ErrorMessage i:nil="true"/>
</CancelResult>
      </CancelResponse>
    </s:Body>
  </s:Envelope>

```

```

<MAC>QyY5RyOiW139Li0zPtoci6LhBwc3c3eUE7ZAJTfVh3qaSTd4zxdlL2bktCzwKzSWQ6vneH67M62P8g4P61
50mND5+yPs2Ewon42uLHMU7sXRXMxCyD0z5c6ZF+sglZe8vwAE/DU1Rmgbx2QWw5GA9reQVeTf59FrkBrB/oEt
nCGLi+Xz+leZ1XwnSS0w2unmAyd9FrX8ufrr6H0fmf6T7w88D58LQGHlwjDKehidM3zu3pHd3MUwbJNAYkX20XZ
eSypALLV4PJHxQphGoBURucNI4Z7bZ0iL27Dk0QJkryhF7+Pcg9wPu3MSTRabZJqZwyhEU5hcXkqyC3BLq9CWA=
=</MAC>

```

„Cancel“ metodo gražinamas atsakymo rezultatas – [ErrorResult](#).

#### 4.4.9. „CancelLTID“ SOAP metodas

„CancelLTID“ metodas skirtas atšaukti einamosios LTID paslaugos, inicijuotos SignLTID ar LoginLTID metodais, vykdymą.

Paslaugos vyksmą galima nutraukti, tik kai statusas yra „Unknown“ (vis dar vyksta).

PASTABA. Kai paslaugos statusas nėra „Unknown“ (vis dar vyksta) ir bandoma paslaugą nutraukti, tuomet metodas klaidos negražins ir būsena išliks nepakitusi.

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

„CancelLTID“ metodo užklauso parametrai:

Pavadinimas	Tipas	Aprašymas
SP	<a href="#">SPInfo</a>	Perduodamas licencijos numeris, kuris buvo gautas iš Patikimo Paslaugų Tiekėjo, ir MAC suformuotas iš licencijos numerio ir sesijos numerio parametru pasirašytos eilutės.
Person	<a href="#">PersonInfoLTID</a>	Fizinio asmens atveju paduodamas fizinio asmens kodas. Įmonės atveju paduodamas įmonės kodas ir fizinio asmens kodas.

Visi parametrai privalomi.

Užklauso pavyzdys:

```
<x:Envelope
  xmlns:x="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:tsp="http://tsp.etrionika.net/">
  <x:Header/>
  <x:Body>
    <tsp:CancelLTID>
      <tsp:SP>
        <tsp:LicenseNumber>EL-E2523-9E792-7B212</tsp:LicenseNumber>

        <tsp:MAC>oMuHkyl/EaH5Ocrooqmcxcp8xo/B0uBaxnewsuTH663gceZszrmOycMWyaRHiv2POvuxXrNkcw5Efo
        7X+q1AfFDbaWStNoSXTSd2Wgxfs9iu8ATF2EU09AyChF3c+6gPr+ctZ/46me/iExnXnVV6JVI59Koh8i4syWYM3
        MynEvBTQbPR3FnnOLje6capyP8zYV/TNsm3wnfB15ADzQUIAcJZFqYqSgfh/cH/To9aTM54a/H4J/gY8ijcMsoU
        5HElJAIrjpfI6Y/oFWGP30KAbsa/uAn3a9Cs5B6IF0xY5dmciDLM03d9F3M3Rdujv0bfjsckzS3NDRxsVuWEQn2
        jvg==</tsp:MAC>

      </tsp:SP>
      <tsp:Person>
        <tsp:PersonCode>10000000001</tsp:PersonCode>
        <tsp:CompanyCode></tsp:CompanyCode>
      </tsp:Person>
    </tsp:CancelLTID>
  </x:Body>
</x:Envelope>
```

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

MAC reikšmė susideda iš privačiuoju raktu pasirašytos eilutės: LicenseNumber+PersonCode + \_ + CompanyCode t.y. EL-E2523-9E792-7B21210000000001\_

CompanyCode nurodomas kai užklaustos vykdomos su el. spaudo sertifikatais.

#### Atsakymo pavyzdys:

```
<s:Envelope
  xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
  <s:Body>
    <CancelLTIDResponse
      xmlns="http://tsp.etronika.net/"
      <CancelLTIDResult
        xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
          <ErrorNumber>0</ErrorNumber>
          <ErrorMessage i:nil="true"/>
        </CancelLTIDResult>
      </CancelLTIDResponse>
    </s:Body>
  </s:Envelope>
```

<MAC>QyY5RyOiW139Li0zPtoci6LhBwC3c3eUE7ZAJTfVh3qaSTd4zxd1L2bktCZwKzSWQ6vneH67M62P8g4P6150mND5+yPs2Ewon42uLHMU7sXRXMxCyD0z5c6ZF+sg1Ze8vwAE/DU1Rmgbx2QWw5GA9reQVeTf59FrkBrB/oEt nCGLi+Xz+leZ1XwnSS0w2unmAyd9FrX8ufrr6H0fmf6T7w88D58LQGHlwjDKehidM3zu3pHd3MUwbJNAYkX20XZeSypALLV4PJHxQphGoBURucNI4Z7bZ0iL27Dk0QJkryhF7+Pcg9wPu3MSTRabZJqZwyhEU5hcXkqyC3BLq9CWA= =</MAC>

„CancelLTID“ metodo grąžinamas atsakymo rezultatas – [ErrorResult](#).

#### 4.4.10. „Test“ SOAP metodas

„Test“ metodas skirtas patikrinti LT ID serviso bei komponentų veikimą. Šį metodą galima kviesti diagnostikos, testavimo ir patikros tikslais. Pavyzdžiui Paslaugų Tiekėjo sistema, kartas nuo karto kreipiasi į šį metodą įsitikinti, ar servisas yra veiksnus. Gavus neigiamą atsakymą, galima iš karto informuoti Naudotojus apie neveikiančią paslaugą, arba gauti įspėjimą apie negaliojančią licenciją ir pan.

Metodas patikrina:

- LT ID serviso veiksnumą;
- licencijos duomenis;

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

- MAC formavimą.

PASTABOS: „Test“ metodas netikrina visos LT ID infrastruktūros veiksmo. Sėkmingos užklausos atveju grąžinamo parametro „ErrorResult“ atributo „ErrorMessage“ reikšmė nebūna tuščia – pateikiamas tekstas „SYSTEMOK“.

„Test“ metodo užklausos parametrai:

Pavadinimas	Tipas	Aprašymas
SP	<a href="#">SPInfo</a>	Perduodamas licencijos numeris, kuris buvo gautas iš Patikimo Paslaugų Tiekėjo, ir MAC suformuotas iš licencijos pasirašytos eilutės.

Visi parametrai privalomi.

Užklausos pavyzdys:

```
<x:Envelope
  xmlns:x="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:tsp="http://tsp.etrionika.net/">
  <x:Header/>
  <x:Body>
    <tsp:Test>
      <tsp:SP>
        <tsp:LicenseNumber>EL-E2523-9E792-7B212</tsp:LicenseNumber>
```

```
<tsp:MAC>Twia+NEyXcs3sxVHc9Hy7JbfUD3UqiptxnN2prQpwavEdsdr8gYdxrw7Y55pbGCaVTzPGbSuAxeHFGMe
A0eVfKljRxjiELxQ+jWUgXqtoJBjVCwASnsQNE3e0mxWTLYY7ZoeuAJMcI5eQN/Yh60kEBLTBcm18j5OXtrXS0Y1
qGQl8Tr40cjdeOm6IXZEMRjeg/9af6cbX/xb4Tv14xhK+Y4N3H82tWhEGKuXSQZ0selN1vNdSM0Rc1NepPhWtJ17I
0uryhpMFHxa30evLMRf+D8Bo5ae61RcEkiAfO+XsVgEGgZuz8N/EEMk1z7UPXsJ/82Eg3aPcDqFu1LmNsNNQ==</t
sp:MAC>
```

```
      </tsp:SP>
    </tsp:Test>
  </x:Body>
</x:Envelope>
```

MAC reikšmė susideda iš privačiuoju raktu pasirašytos eilutės: LicenseNumber

Atsakymo pavyzdys:

```
<s:Envelope
  xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
  <s:Body>
```

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

```

<TestResponse
  xmlns="http://tsp.etrionika.net/">
  <TestResult
    xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
    <ErrorNumber>0</ErrorNumber>
    <ErrorMessage>SYSTEMOK</ErrorMessage>

<MAC>fzQasIszQQJKc2D8Ty0HsH7ujybAEpfecBBakhdPq4DrY0QXDPDS2AQVyTRs0nDMZc9rEniXoOHjDbjEl7RB
gNALkASzbHNBwKPvojnN2y1yEXss77094pkSzoQhFuJusMw8TiQ1UIq/JeiyoSvUFXQHLOpGSDCBhiyEZid2RuDc
8Ys5i6T6oftoNBt9/qsohLNHZDY3+U6ERatUWD7PSI1pJ4dy71N7t1WKvPK2NM7129JGFjNIUnmaXW1Lne2sUUZx
UnWhuq7LFAJHkNbcKKHbROw/JnyI1KBnUpiWbCAI6HxcoB1/sf4eU8sI5QYCOum659WQn4PO5wJ/xkjg==</MAC>
    </TestResult>
  </TestResponse>
</s:Body>
</s:Envelope>

```

„Test“ metodo gražinamas atsakymo rezultatas – [ErrorResult](#).

#### 4.4.11. „LoginLTID“ SOAP metodas

LoginLTID metodas yra skirtas vartotojų arba duomenų autentifikacijai naudojant LTID parašą.

„LoginLTID“ metodo užklauso parametrai:

Pavadinimas	Tipas	Aprašymas
SP	<a href="#">SPIInfo</a>	Perduodamas licencijos numeris, kuris buvo gautas iš Patikimo Paslaugų Tiekėjo, ir MAC suformuotas iš licencijos numerio ir kitų parametų pasirašytos eilutės.
Person	<a href="#">PersonInfoLTID</a>	Fizinio asmens atveju paduodamas fizinio asmens kodas. Įmonės atveju paduodamas įmonės kodas ir fizinio asmens kodas.
HashUsage	<a href="#">HashType</a>	Šis parametras nurodo, koks maišos algoritmas buvo panaudotas formuojant DTBS lauką. Parametras panaudojamas DTBS turinio kontrolei.

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

Pavadinimas	Tipas	Aprašymas
DTBS	byte[]	(angl. <i>Data to be signed</i> ) – tai duomenys, kuriuos galutinis Naudotojas pasirašys LT ID elektroniniu parašu .
DTBD	string	(angl. <i>Data to be displayed</i> ) – tai tekstas, kurį galutinis Naudotojas išvys LT ID aktyvavimo įrenginyje. Jeigu šis parametras bus tuščias, bus rodomas standartinis licencijoje įvestas tekstas.  Į vieną telefono ekraną telpa apie 60 ženklų, todėl siūloma naudoti kompaktiškus tekstus, sudarytus iš Paslaugų teikėjo pavadinimo ir keturių skaičių kontrolinio kodo, kuriuos vartotojai turėtų sulyginti su kontroliniais kodais, rodomais kompiuterio ekrane. Pavyzdžiui, DTBD="Turto Bankas. Kontrolinis kodas: 2233". Atvejais, kai šio lauko ilgis didesnis nei 60 ženklų, tekstas gali būti išskaitytas į daug dialoginių langų.
Timeout	int	Laiko tarpas sekundėmis, kiek daugiausiai gali užtrukti autentifikacija.

Visi parametrai privalomi.

Užklauso pavyzdys:

```
<x:Envelope
  xmlns:x="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:tsp="http://tsp.etrionika.net/">
  <x:Header/>
  <x:Body>
    <tsp:LoginLTID>
      <tsp:SP>
        <tsp:LicenseNumber>EL-E2523-9E792-7B212</tsp:LicenseNumber>

        <tsp:MAC>CFQmJ1HHwKeVHpNL527tUZuv7QqEZgHbjre4kwa/kLxK00UmEX/MrNvs7z3d0+ULraKQR2bjHLfkqf
UwQiFhMvvp5gv6X687vQGGj4KKoVAM6QnLQeQdd3G2SgiJ2ixmudDSyHQQNxsFRbB1YC4p77mYBakcv83TwOyYc
di6RXcyNWlniYEcBwmyhKuUoE0k5bNqGV300wsylAmfBuiKgdpq0ojd3L49WJvYvbYLFnGXdG1ZcEjjWDaVyHtK
b41e99DLs900N1MGBty45V4jD0reV+IrXp70SzLv7Wbp1HRkcROv/+u2m7E3R2izpaQhSG+5h1MbaQGJDG7ATfX
elg==</tsp:MAC>

      </tsp:SP>
    <tsp:Person>
      <tsp:PersonCode>10000000001</tsp:PersonCode>
    </tsp:Person>
  </x:Body>
</x:Envelope>
```

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

```

        <tsp:CompanyCode></tsp:CompanyCode>
    </tsp:Person>
    <tsp:HashUsage>HashedSHA1</tsp:HashUsage>
    <tsp:DTBS>AQID</tsp:DTBS>
    <tsp:DTBD>prisijungimas</tsp:DTBD>
    <tsp:Timeout>100</tsp:Timeout>
</tsp:LoginLTID>
</x:Body>
</x:Envelope>

```

MAC reikšmė susideda iš privačiuoju raktu pasirašytos eilutės: LicenseNumber + PersonCode + \_ + CompanyCode + HashType + DTBS + DTBD + Timeout t.y.

EL-E2523-9E792-7B21210000000001\_HashedSHA1AQIDprisijungimas100

CompanyCode nurodomas kai užklauskos vykdomos su el. spaudo sertifikatais.

Atsakymo pavyzdys:

```

<s:Envelope
  xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
  <s:Body>
    <LoginLTIDResponse
      xmlns="http://tsp.etrionika.net/">
      <LoginLTIDResult
        xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
        <Error>
          <ErrorNumber>0</ErrorNumber>
          <ErrorMessage i:nil="true"/>

```

```

<MAC>Lx0QY/eziqXTVnQaXlwLY8zy3cC2YQiQfcWUeTaoHfe3sAcvKnoaHiW9MS/sUuLx0kEPGkx+akdCjuGdH
ctcmTfLX4cxWv2ZzH33wrE5MN+3nYs0LKktmOJR00OotQh0hbi5NUk+ONbbNN0MBYQh49kfU7ajxUN0e+QkvE1s
8V0Sxn32x0p8wr78jWYJN4k6hKqIMibBiqf6Z3hUesIPc2t1FP7K9oVNbzYkwBle1J1tAJMuU/g83sjbV6LnR8q
goEQmexnz5nq1H91jrhT+244xZqoCu2dKL7hBaSZxqZaYddvcoBAK+dtuEx9OjPF/5gmXITsWwPVWuuVgCuvdg=
=</MAC>

```

```

        </Error>
        <SessionNumber>1401375</SessionNumber>
    </LoginLTIDResult>
  </LoginLTIDResponse>
</s:Body>
</s:Envelope>

```

„LoginLTID“ metodo grąžinamas atsakymo rezultatas – [SessionResult](#).

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

#### 4.4.12. „SignLTID“ SOAP metodas

„SignLTID“ metodas skirtas pasirašymo paslaugai naudojant LTID parašą ar spaudą. El. dokumentų ar duomenų pasirašymui LT ID parašu turi būti paduodamas pasirašančio asmens kodas, LT ID spaudu – asmens, kuris užsakė ir gavo LT ID spaudą, fizinio asmens bei įmonės, kuriai buvo išduotas LT ID spaudas, kodai.

„SignLTID“ metodo užklauso parametrai:

Pavadinimas	Tipas	Aprašymas
SP	<a href="#">SPInfo</a>	Perduodamas licencijos numeris, kuris buvo gautas iš Patikimo Paslaugų Tiekėjo, ir MAC suformuotas iš licencijos numerio ir kitų parametru pasirašytos eilutės.
Person	<a href="#">PersonInfoLTID</a>	Fizinio asmens atveju paduodamas fizinio asmens kodas. (El. parašas) Įmonės atveju paduodamas fizinio asmens kodas ir įmonės kodas. (El. spaudas)
HashUsage	<a href="#">HashType</a>	Šis parametras nurodo, koks maišos algoritmas buvo panaudotas formuojant DTBS lauką. Parametras panaudojamas DTBS turinio kontrolei.
DTBS	byte[][]	(angl. <i>Data to be signed</i> ) – tai duomenys, kuriuos Galutinis Naudotojas pasirašys LT ID elektroniniu parašu ar spaudu. Galima paduoti daugiau nei vieną dokumentą pasirašymui. Kiekvienas dokumentas yra baitų masyvas. Metodas priima masyvą dokumentų.

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

Pavadinimas	Tipas	Aprašymas
DTBD	string	(angl. <i>Data to be displayed</i> ) – tai tekstas, kurį galutinis Naudotojas išvys LT ID aktyvavimo įrenginyje. Jeigu šis parametras bus tuščias, bus rodomas standartinis licencijoje įvestas tekstas. Į vieną telefono ekraną telpa apie 60 ženklų, todėl siūloma naudoti kompaktiškus tekstus, sudarytus iš Paslaugų teikėjo pavadinimo ir keturių skaičių kontrolinio kodo, kuriuos vartotojai turėtų sulyginti su kontroliniais kodais, rodomais kompiuterio ekrane. Pavyzdžiui, DTBD="Turto Bankas. Kontrolinis kodas: 2233". Atvejais, kai šio lauko ilgis didesnis nei 60 ženklų, tekstas gali būti išskaitytas į daug dialoginių langų.
Timeout	int	Laiko tarpas sekundėmis, kiek daugiausiai gali trukti pasirašymas.

Visi parametrai privalomi.

Užklauso pavyzdys:

```
<x:Envelope
  xmlns:x="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:tsp="http://tsp.etrionika.net/"
  xmlns:arr="http://schemas.microsoft.com/2003/10/Serialization/Arrays">
  <x:Header/>
  <x:Body>
    <tsp:SignLTID>
      <tsp:SP>
        <tsp:LicenseNumber>EL-E2523-9E792-7B212</tsp:LicenseNumber>

        <tsp:MAC>X6aHgNWK1N9BN7yn2vnNbAoWPHCbjm3SZs6DbChWkbq1+vb9ZEU3bCUMOwyUEsksv/86uUrkaJaZ20
        TWuctOQ01AT47oawGn1+lew1/lnBw4s8AbJGfWNxZLugJ5dHrkJ2oxaoudK1N4xGMkYAaBJoBily0biFRcPHFW
        tyQmMnb78AAeRvyNImL124/nNYvye3sxK93cLJIzkdG4R6clnHhNk5iHJHimU0aAOPGQX3JuGVBvoHX8vYdJvWV
        K3ONyIauBQQbjkH4kF+YUE6HSdbKSK7IujeY6AiIv7PiBZNfmbHNo72YUzmnU3zrAogY5zprXrz84nonWez45H8e
        dXA==</tsp:MAC>

      </tsp:SP>
    <tsp:Person>
      <tsp:PersonCode>10000000001</tsp:PersonCode>
      <tsp:CompanyCode></tsp:CompanyCode>
    </tsp:Person>
    <tsp:HashUsage>HashedSHA1</tsp:HashUsage>
  </x:Body>
</x:Envelope>
```

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

```

<tsp:DTBS>
  <arr:base64Binary>AQIDAQID</arr:base64Binary>
</tsp:DTBS>
<tsp:DTBD>prisijungimas</tsp:DTBD>
<tsp:Timeout>100</tsp:Timeout>
</tsp:SignLTID>
</x:Body>
</x:Envelope>

```

MAC reikšmė susideda iš privačiuoju raktu pasirašytos eilutės: LicenseNumber + PersonCode + \_ + CompanyCode + HashType + DTBS + DTBD + Timeout t.y.

EL-E2523-9E792-7B2121000000001\_HashedSHA1AQIDAQIDprisijungimas100  
CompanyCode nurodomas kai užklauskos vykdomos su el. spaudu sertifikatais.

#### Atsakymo pavyzdys:

```

<s:Envelope
  xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
  <s:Body>
    <SignLTIDResponse
      xmlns="http://tsp.etrionika.net/"
      <SignLTIDResult
        xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
          <Error>
            <ErrorNumber>0</ErrorNumber>
            <ErrorMessage i:nil="true"/>
          </Error>
          <SessionNumber>1401377</SessionNumber>
        </SignLTIDResult>
      </SignLTIDResponse>
    </s:Body>
  </s:Envelope>

```

```

<MAC>SjrkbmaDp+qVz1X6d8YVJnNSV0HZt4YJOUjPp70KkXiIqI8O4QxZ2cxGHd0HpwuWmoWyD1C024r7emRA8
kdJ4xSkdvpec/APTmgjTtZ02f9qIJe18mCn+W/8aYPSRtbRTaI9boRC/nAl2vLPAJJeCR8S8Btqm9NVZ6x1OjYc
WB+6KPGTsQRV/pzbCGZzrHpsHx1D9Hs3FYM3nJIwbv4b49r/v+/uf7kBBGmPEd5IbYqjnw0/AQWQBRAS4cjlw5
tbYGtL7Sh1IR2+msK8twgR9hgZjvd8jkVxV6Y2eb8a8M4trDhQEBQSreHFHYITm85noJqx3vzq6+5oaLCLPFOA=
=</MAC>

```

„SignLTID“ metodas grąžina atsakymo rezultata – [SessionResult](#). Šis atsakymas sutampa su „LoginLTID“ metodo grąžinamu atsakymu, todėl supaprastinamas paslaugų statusų stebėjimas.

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

#### 4.4.13. „GetCertificatesLTID“ SOAP metodas

„GetCertificatesLTID“ metodas skirtas grąžinti galutinio naudotojo turimus aktyvius sertifikatus.

„GetCertificatesLTID“ metodo užklauso parametrai:

Pavadinimas	Tipas	Aprašymas
SP	<a href="#">SPInfo</a>	Perduodamas licencijos numeris, kuris buvo gautas iš Patikimo Paslaugų Tiekėjo, ir MAC suformuotas iš licencijos numerio ir kitų parametų pasirašytos eilutės.
Person	<a href="#">PersonInfoLTID</a>	Fizinio asmens atveju paduodamas fizinio asmens kodas. Įmonės atveju paduodamas įmonės kodas ir fizinio asmens kodas.

Visi parametrai privalomi.

Užklauso pavyzdys:

```
<x:Envelope
  xmlns:x="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:tsp="http://tsp.etrionika.net/">
  <x:Header/>
  <x:Body>
    <tsp:GetCertificatesLTID>
      <tsp:SP>
        <tsp:LicenseNumber>EL-E2523-9E792-7B212</tsp:LicenseNumber>

        <tsp:MAC>oMuHkyl/EaH5Ocrocqmcxcp8xo/B0uBaxnewsuTH663gceZszrmOycMWyaRHiv2POvuxXrNkcw5Efo
        7X+q1AfFDbaWStNoSXTSd2Wgxfs9iu8ATF2EU09AyChF3c+6gPr+ctZ/46me/iExnXnVV6JVI59Koh8i4syWYM3
        MynEvBTQbPR3FnnOLje6capyp8zYV/TNsm3wnfB15ADzQUiAcJZFqYqSgfh/ch/To9aTM54a/H4J/gy8ijcMsoU
        5HElJAIrjpf16Y/oFWGP30KAbsa/uAn3a9Cs5B6IF0xY5dmciDLM03d9F3M3Rdujv0bfjsckzS3NDRxsVuWEQn2
        jvg==</tsp:MAC>

      </tsp:SP>
      <tsp:Person>
        <tsp:PersonCode>10000000001</tsp:PersonCode>
        <tsp:CompanyCode></tsp:CompanyCode>
      </tsp:Person>
    </tsp:GetCertificatesLTID>
  </x:Body>
```



LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

```

c2MwNgYIKwYBBQUHMAKGMh0dHA6Ly9jc3AyLnJjc2MubHQvYWlhL1JDU0NfSXNz
dWluZ0NBmNydDA9BgkrBgEEAYI3FQcEMDAuBiYrBgEEAYI3FQiCnOx7hKbACoTl
kQ6Gk5hj4LRXoFhj/MIg4bTLgIBZAIBCzATBgNVHSUEDDAKBggrBgEFBQcDAjBG
BgNVHSAEPzA9MDsGCysGAQQBgfE3AQIGMCwwKgYIKwYBBQUHAgEWHmh0dHA6Ly93
d3cucmNzYy5sdC9yZXBvc2l0b3J5LzAbBgkrBgEEAYI3FQoEDjAMMAoGCCsGAQUF
BwMCMA0GCSqGSIb3DQEBCwUAA4IBAQB55X/dh1ZqTZ4POpznfHmwW0S6CUhMLEF
EhkGF68F1AyzRe+bsZLDjOuvIPRIIEqox5h9iPUmnLK1icsdcmv+YCoB79H9cpUp
CvblA0zRrPuxYbX3CqVob7ai2G7a6dAKlHPJAp+nhKI5Eq4W0taGNmwbGY0BFX6D
0ZWxOJY/1ICg7PaiEglJV4GyIlkY+6A2bHqngkSgxGvKkgdHMKeG7jEutmhiDpGs
idZXAZm0+OLrKRWDOn+ZbDM71c937K7aahukxca/pr2X0WEZY2EvpwSukgsbHVPF
oD2s+Ct+sX2yiTCHRHwrRj0d8QXJRIVmJzipewyHqMOVkymRfBAN</CertificateSIG>
</GetCertificatesLTIDResult>
</GetCertificatesLTIDResponse>
</s:Body>
</s:Envelope>

```

„GetCertificatesLTID“ metodo grąžinamas atsakymo rezultatas – [CertificatesResult](#). CertificateSIG laukelyje yra base-64 užkoduotas sertifikatas.

#### 4.4.14. „Init“ REST metodas

„Init“ metodas skirtas automatizuoti Paslaugų Tiekėjo ir Patikimo Paslaugų Tiekėjo viešųjų raktų apsikeitimą.

„Init“ metodas yra vienetinis. Tai reiškia, kad šį metodą galima kviesti tik vieną kartą per licencijos gyvavimą. Pakartotinas jo kvietimas, pvz., pasikeitus Paslaugų Tiekėjo arba Patikimo Paslaugų Tiekėjo raktams, galimas tik susitarus su Patikimu Paslaugų Tiekėju.

„Init“ metodo užklauso parametrai:

Pavadinimas	Tipas	Aprašymas
SP	<a href="#">SPIInfo</a>	Perduodamas licencijos numeris, kuris buvo gautas iš Patikimo Paslaugų Tiekėjo, ir MAC suformuotas iš licencijos numerio ir PublicKey parametro pasirašytos eilutės.
PublicKey	string	Paslaugų Tiekėjo viešasis raktas, kurį jis perduoda Patikimam Paslaugų Tiekėjui. Palaikomi viešojo rakto formatai pateikti <a href="#">priede A</a> .

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

Visi parametrai privalomi.

„Init“ metodo grąžinamas atsakymo rezultatas – [InitResult](#).

„Init“ metodo užklauso – atsakymo pavyzdys:

POST: <https://api.ltid.lt/api/init>

Užklauso pavyzdys:

```
{
  "SPInfo": {
    "LicenseNumber": "EL-E2523-9E792-7B212",
    "MAC": [36, 181, 75, 156, 59, 48, 223, 55, 130, 199, 8, 185, 128, 195, 86, 40, 25
4, 47, 240, 248, 162, 224, 42, 140, 251, 217, 105, 195, 252, 33, 181, 73, 233, 222, 123,
181, 195, 175, 209, 202, 23, 150, 62, 98, 193, 44, 118, 139, 210, 255, 220, 98, 40, 11, 5
3, 228, 34, 150, 69, 34, 67, 243, 91, 142, 1, 53, 42, 159, 45, 194, 63, 3, 36, 232, 62, 1
68, 173, 238, 154, 225, 165, 223, 234, 101, 249, 187, 164, 98, 198, 236, 161, 99, 83, 106
, 97, 59, 208, 55, 159, 93, 53, 234, 121, 105, 51, 28, 131, 119, 175, 12, 209, 253, 233,
111, 186, 39, 155, 77, 12, 99, 9, 251, 247, 63, 122, 244, 65, 254, 100, 65, 144, 207, 141
, 204, 255, 251, 135, 73, 252, 201, 108, 115, 2, 114, 157, 213, 220, 101, 244, 30, 253, 1
65, 21, 233, 204, 17, 241, 28, 184, 63, 253, 30, 98, 160, 179, 156, 196, 53, 10, 190, 172
, 0, 32, 214, 199, 103, 225, 242, 142, 235, 141, 113, 211, 2, 1, 156, 27, 182, 149, 210,
200, 54, 92, 181, 163, 145, 112, 122, 74, 84, 87, 214, 211, 74, 104, 228, 31, 218, 128, 1
63, 5, 194, 133, 195, 215, 60, 83, 115, 217, 157, 116, 31, 132, 79, 159, 53, 121, 76, 228
, 32, 253, 242, 123, 52, 18, 205, 60, 105, 238, 196, 184, 235, 210, 64, 198, 199, 191, 11
, 100, 237, 93, 245, 237, 189, 108, 93]
  },
  "PublicKey": "-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAAuCl9w+d+GZf58es/tFT3
L83tiJ7UNshiSh6PVfjz60om/G6tuWc7KIKdEVy2IWZw5OGBIksfKSLQR6leL9Bo
tovMyRZb3ipGMiXewaVP+8y0HtkXn8jQWshF3TddckfQ+5lcLJ/fiwu/CHmLSzTp
wiphUPAU5YKmg5cmhwLOGXctBqhUbr5ueiIKNYyMXtr+PLqWMFw+weyM54P77dAj
bM9tY0PsvhYOMCLEyGUPrFHag3Oz5jJhf6jSXkTVikw0iFA+WD/Ojv8KWX9Uo4j9
sI5s0locGuGyH8MUgurqe0FkFIC9JtR+ijc46M7R5bkFkdGx5ftUCBKEJGJ+mENT
kQIDAQAB
-----END PUBLIC KEY-----"
}
```

Atsakymo pavyzdys:

```
{
  "PublicKey": null,
  "Error": {
    "ErrorNumber": 56,
  }
}
```

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

```

    "ErrorMessage": "Public key already exists.",
    "HasError": true,
    "MAC": null
  }
}

```

Error.MAC yra skaičiuojamas MAC iš grąžintų laukų pasirašant tokeną serverio privačiu raktu. Grąžinamas sėkmės atveju. Klientas **privalo** patikrinti ar gautas MAC'as ir grąžintos reikšmės sutampa.

Token'as kuri šiuo atveju reikia tikrint serverio viešuoju raktu: 0PublicKeyreikšmė

#### 4.4.15. „GetLicenseDates“ REST metodas

„GetLicenseDates“ metodas skirtas palengvinti Paslaugų Tiekėjo informavimą apie licencijos galiojimo periodą. Grąžinamos licencijos galiojimo pradžios ir pabaigos datos.

„GetLicenseDates“ metodo užklausos parametrai:

Pavadinimas	Tipas	Aprašymas
SP	<a href="#">SPInfo</a>	Perduodamas licencijos numeris, kuris buvo gautas iš Patikimo Paslaugų Tiekėjo, ir MAC suformuotas iš licencijos numerio parametro pasirašytos eilutės.

Visi parametrai privalomi.

„GetLicenseDates“ metodo grąžinamas atsakymo rezultatas – [GetDatesResult](#).

„GetLicenseDates“ metodo užklausos – atsakymo pavyzdys:

POST: <https://api.ltid.lt/api/licensedates>

Užklausos pavyzdys:

```

{
  "LicenseNumber": "EL-E2523-9E792-7B212",
  "MAC": [79, 8, 154, 248, 209, 50, 93, 203, 55, 179, 21, 71, 115, 209, 242, 236, 1
50, 223, 80, 61, 212, 170, 42, 109, 198, 115, 118, 166, 180, 41, 193, 171, 196, 118, 199,
107, 242, 6, 29, 198, 188, 59, 99, 158, 105, 108, 96, 154, 85, 60, 207, 25, 180, 174, 3,
23, 161, 20, 99, 30, 3, 71, 149, 22, 66, 227, 71, 24, 226, 16, 188, 80, 250, 53, 148, 12

```

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

```
9, 122, 173, 160, 144, 99, 84, 44, 0, 74, 123, 16, 52, 77, 222, 210, 108, 86, 76, 182, 24
, 237, 154, 30, 184, 2, 76, 112, 142, 94, 64, 223, 216, 135, 173, 36, 16, 18, 211, 5, 195
, 37, 242, 62, 78, 94, 218, 215, 73, 205, 24, 214, 161, 144, 151, 196, 235, 227, 71, 35,
117, 227, 166, 232, 133, 217, 16, 196, 99, 122, 15, 253, 105, 254, 156, 109, 127, 241, 11
1, 132, 239, 215, 140, 97, 43, 230, 56, 55, 113, 252, 218, 213, 161, 16, 98, 174, 93, 36,
25, 58, 199, 165, 55, 91, 205, 117, 35, 52, 69, 205, 77, 122, 147, 225, 90, 210, 117, 23
6, 141, 46, 175, 40, 105, 48, 81, 241, 107, 125, 30, 188, 179, 17, 127, 224, 252, 6, 142,
90, 123, 173, 81, 112, 73, 34, 105, 243, 190, 94, 197, 96, 16, 104, 25, 187, 63, 13, 252
, 65, 12, 147, 92, 251, 80, 245, 236, 39, 255, 54, 18, 13, 218, 61, 192, 234, 22, 237, 75
, 152, 219, 13, 53]
```

}

Atsakymo pavyzdys:

```
{
  "DateFrom": "2023-08-03T00:00:00",
  "DateTill": "2030-07-31T00:00:00",
  "Error": {
    "ErrorNumber": 0,
    "ErrorMessage": null,
    "HasError": false,
    "MAC": null
  }
}
```

Error.MAC yra skaičiuojamas MAC iš gražintų laukų pasirašant tokeną serverio privačiu raktu.

Klientas **privalo** patikrinti ar gautas MAC'as ir gražintos reikšmės sutampa.

Token'as kuri šiuo atveju reikia tikrint serverio viešuoju raktu: 02023.08.03 00:00:002030.07.31 00:00:00

#### 4.4.16. „StatusLTID“ REST metodas

„StatusLTID“ metodas taip pat yra pasiekiamas naudojant REST api.

„StatusLTID“ metodo užklauso parametrai:

Pavadinimas	Tipas	Aprašymas
SP	<a href="#">SPInfo</a>	Perduodamas licencijos numeris, kuris buvo gautas iš Patikimo Paslaugų Tiekėjo, ir MAC suformuotas iš licencijos numerio ir kitų parametru pasirašytos eilutės.

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

Pavadinimas	Tipas	Aprašymas
SessionID	<a href="#">string</a>	Sesijos numeris, kuris buvo gautas kviečiant „LoginLTID“ ar „SignLTID“ metodus. Einamosios paslaugos sekimo numeris.

Visi parametrai privalomi.

„StatusLTID“ metodo užklausos – atsakymo pavyzdys:

POST: <https://api.lt.id.lt/api/status>

Užklausos pavyzdys:

```
{
  "SPInfo": {
    "LicenseNumber": "EL-E2523-9E792-7B212",
    "MAC": [122, 48, 225, 215, 247, 137, 141, 24, 8, 57, 172, 81, 46, 119, 59, 11, 26,
, 81, 248, 251, 147, 98, 169, 189, 126, 190, 156, 243, 233, 211, 33, 122, 14, 110, 146, 1
95, 119, 38, 100, 69, 226, 106, 126, 207, 185, 136, 201, 157, 79, 232, 241, 39, 170, 78,
122, 241, 87, 81, 170, 50, 131, 146, 234, 131, 205, 30, 105, 213, 17, 94, 43, 200, 225, 2
14, 60, 141, 81, 109, 249, 112, 254, 135, 154, 116, 16, 61, 185, 20, 150, 0, 150, 195, 14
1, 2, 109, 72, 18, 128, 176, 192, 81, 55, 16, 205, 228, 239, 128, 125, 198, 133, 221, 178
, 129, 69, 59, 51, 29, 132, 178, 147, 17, 72, 122, 118, 133, 174, 49, 74, 192, 62, 156, 2
43, 166, 128, 181, 148, 87, 231, 208, 105, 60, 248, 39, 17, 195, 156, 55, 92, 127, 142, 1
34, 235, 54, 7, 193, 239, 53, 211, 116, 234, 234, 185, 43, 229, 27, 189, 117, 193, 139, 1
56, 171, 144, 14, 1, 195, 77, 196, 157, 165, 51, 101, 64, 108, 135, 180, 213, 13, 62, 5,
70, 147, 140, 211, 93, 0, 144, 150, 189, 249, 124, 74, 122, 186, 108, 122, 212, 135, 140,
12, 85, 192, 107, 215, 98, 194, 116, 201, 77, 75, 142, 171, 184, 49, 123, 112, 61, 55, 8
6, 100, 226, 97, 245, 183, 181, 173, 21, 165, 91, 5, 124, 128, 86, 228, 54, 112, 148, 46,
127, 116, 228, 5, 130, 151, 196, 186, 139]
  },
  "SessionID": "1401285"
}
```

MAC reikšmė susideda iš privačiuoju raktu pasirašytos eilutės: LicenseNumber + SessionID t.y. EL-E2523-9E792-7B2121401285

Atsakymo pavyzdys:

```
{
```

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

```

"Error": {

    "ErrorNumber": 0,

    "ErrorMessage": null,

    "HasError": false,

    "MAC": null

},

"Status": 0,

"Signature": ["MGUCMGS17pTdvGk0V+OUmnqN1Y7A2C2JHn9FFDIwRj..."],

"Certificate": null,

"OCSPResponse": null,

"OCSPCertificate": ""

}

```

„StatusLTID“ metodo grąžinamas atsakymo rezultatas – [StatusResult](#).

Reikšmė	Aprašymas
Ok (0)	sesija baigėsi sėkmingai.
Unknown (1)	sesija dar nesibaigė.
Canceled (2)	sesija buvo nutraukta.
Timeout (3)	sesijos laikas pasibaigė.
Error (4)	sesija baigėsi nesėkmingai.

Kviečiamas loginltid arba signltid, kuris grįžta asinchroniškai su SessionID. Tuomet užklaustos statusas tikrinamas naudojant StatusLTID metodą. Signature yra pasirašytas dokumentas.

Error.MAC yra skaičiuojamas MAC iš grąžintų laukų pasirašant tokeną serverio privačiu raktu.

Klientas **privalo** patikrinti ar gautas MAC'as ir grąžintos reikšmės sutampa.

Token'as kuri šiuo atveju reikia tikrint serverio viešuoju raktu:

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

00kSignature1Signature2..SignatureNCertificate

#### 4.4.17. „Cancel“ REST metodas

„Cancel“ metodas skirtas atšaukti einamosios paslaugos vykdymą. Pradėjus vykdyti autentifikacijos ar pasirašymo paslaugą, yra gaunamas parametras „SessionNumber“, perduodant jį šiam metodui paslaugos vykdymas nutraukiamas. Su tuo pačiu sesijos numeriu bandant gauti paslaugos statusą, atsakymo statusas bus „Canceled“ (būsena – nutraukta).

Paslaugos vyksmą galima nutraukti, tik kai statusas yra „Unknown“ (vis dar vyksta).

PASTABA. Kai paslaugos statusas nėra „Unknown“ (vis dar vyksta) ir bandoma paslaugą nutraukti, tuomet metodas klaidos negrąžins ir būsena išliks nepakitusi.

„Cancel“ metodo užklausos parametrai:

Pavadinimas	Tipas	Aprašymas
SP	<a href="#">SPInfo</a>	Perduodamas licencijos numeris, kuris buvo gautas iš Patikimo Paslaugų Tiekėjo, ir MAC suformuotas iš licencijos numerio ir sesijos numerio parametrų pasirašytos eilutės.
SessionNumber	int	Sesijos numeris, kuris buvo gautas kviečiant „Login“ ar „Sign“ metodus. Einamosios paslaugos sekimo numeris.

Visi parametrai privalomi.

„Cancel“ metodo grąžinamas atsakymo rezultatas – [ErrorResult](#).

„Cancel“ metodo užklausos – atsakymo pavyzdys:

POST: <https://api.lt.id.lt/api/cancel>

Užklausos pavyzdys:

```
{
  "SPInfo": {
    "LicenseNumber": "EL-E2523-9E792-7B212",
    "MAC": [122, 48, 225, 215, 247, 137, 141, 24, 8, 57, 172, 81, 46, 119, 59, 11, 26,
, 81, 248, 251, 147, 98, 169, 189, 126, 190, 156, 243, 233, 211, 33, 122, 14, 110, 146, 1
95, 119, 38, 100, 69, 226, 106, 126, 207, 185, 136, 201, 157, 79, 232, 241, 39, 170, 78,
122, 241, 87, 81, 170, 50, 131, 146, 234, 131, 205, 30, 105, 213, 17, 94, 43, 200, 225, 2
```

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

```
14, 60, 141, 81, 109, 249, 112, 254, 135, 154, 116, 16, 61, 185, 20, 150, 0, 150, 195, 14
1, 2, 109, 72, 18, 128, 176, 192, 81, 55, 16, 205, 228, 239, 128, 125, 198, 133, 221, 178
, 129, 69, 59, 51, 29, 132, 178, 147, 17, 72, 122, 118, 133, 174, 49, 74, 192, 62, 156, 2
43, 166, 128, 181, 148, 87, 231, 208, 105, 60, 248, 39, 17, 195, 156, 55, 92, 127, 142, 1
34, 235, 54, 7, 193, 239, 53, 211, 116, 234, 234, 185, 43, 229, 27, 189, 117, 193, 139, 1
56, 171, 144, 14, 1, 195, 77, 196, 157, 165, 51, 101, 64, 108, 135, 180, 213, 13, 62, 5,
70, 147, 140, 211, 93, 0, 144, 150, 189, 249, 124, 74, 122, 186, 108, 122, 212, 135, 140,
12, 85, 192, 107, 215, 98, 194, 116, 201, 77, 75, 142, 171, 184, 49, 123, 112, 61, 55, 8
6, 100, 226, 97, 245, 183, 181, 173, 21, 165, 91, 5, 124, 128, 86, 228, 54, 112, 148, 46,
127, 116, 228, 5, 130, 151, 196, 186, 139]
```

```
},
  "SessionID": "1401285"
}
```

MAC reikšmė susideda iš privačiuoju raktu pasirašytos eilutės: LicenseNumber + SessionID t.y. EL-E2523-9E792-7B2121401285

Atsakymo pavyzdys:

```
{
  "ErrorNumber": 0,
  "ErrorMessage": null,
  "HasError": false,
  "MAC": null
}
```

Error.MAC yra skaičiuojamas MAC iš grąžintų laukų pasirašant tokeną serverio privačiu raktu.

Klientas **privalo** patikrinti ar gautas MAC'as ir grąžintos reikšmės sutampa.

Token'as kuri šiuo atveju reikia tikrinti serverio viešuoju raktu: 0

#### 4.4.18. „CancelLTID“ REST metodas

„CancelLTID“ metodas skirtas atšaukti einamosios paslaugos vykdymą.

Paslaugos vyksmą galima nutraukti, tik kai statusas yra „Unknown“ (vis dar vyksta).

PASTABA. Kai paslaugos statusas nėra „Unknown“ (vis dar vyksta) ir bandoma paslaugą nutraukti, tuomet metodas klaidos negrąžins ir būsena išliks nepakitusi.

„CancelLTID“ metodo užklauso parametrai:

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

Pavadinimas	Tipas	Aprašymas
SP	<a href="#">SPInfo</a>	Perduodamas licencijos numeris, kuris buvo gautas iš Patikimo Paslaugų Tiekėjo, ir MAC suformuotas iš licencijos numerio ir sesijos numerio parametrų pasirašytos eilutės.
Person	<a href="#">PersonInfoLTID</a>	Fizinio asmens atveju paduodamas fizinio asmens kodas. Įmonės atveju paduodamas įmonės kodas ir fizinio asmens kodas.

Visi parametrai privalomi.

„CancelLTID“ metodo grąžinamas atsakymo rezultatas – [ErrorResult](#).

„CancelLTID“ metodo užklauso – atsakymo pavyzdys:

POST: <https://api.ltid.lt/api/cancelltid>

Užklauso pavyzdys:

```
{
  "SPInfo": {
    "LicenseNumber": "EL-E2523-9E792-7B212",
    "MAC": [5, 192, 253, 66, 210, 116, 6, 204, 75, 39, 180, 253, 167, 218, 107, 134,
137, 10, 205, 24, 46, 22, 139, 207, 143, 108, 83, 151, 5, 246, 25, 8, 120, 5, 6, 184, 56,
224, 7, 95, 8, 53, 55, 228, 78, 209, 149, 35, 119, 49, 65, 46, 178, 120, 197, 210, 175,
154, 114, 62, 55, 83, 24, 246, 176, 247, 8, 221, 36, 115, 252, 199, 109, 68, 99, 199, 22,
193, 51, 237, 56, 59, 113, 208, 137, 109, 245, 81, 255, 5, 58, 220, 243, 242, 253, 108,
235, 202, 32, 226, 34, 71, 209, 99, 191, 66, 46, 138, 128, 60, 95, 205, 218, 80, 133, 90,
235, 3, 35, 10, 159, 243, 17, 15, 63, 40, 254, 177, 80, 36, 123, 160, 69, 33, 95, 27, 13
3, 55, 51, 12, 213, 153, 222, 25, 4, 205, 178, 119, 228, 159, 103, 95, 65, 12, 170, 25, 1
68, 63, 221, 208, 182, 160, 106, 75, 250, 95, 61, 218, 216, 214, 171, 68, 139, 168, 70, 1
37, 61, 230, 8, 251, 147, 203, 16, 215, 118, 141, 193, 211, 183, 14, 100, 123, 78, 50, 20
0, 108, 17, 55, 37, 70, 96, 249, 156, 108, 134, 170, 200, 59, 8, 221, 77, 227, 246, 16, 2
39, 24, 210, 115, 113, 198, 33, 253, 219, 239, 61, 117, 110, 164, 249, 101, 108, 64, 45,
239, 176, 140, 34, 238, 156, 204, 88, 90, 189, 247, 148, 8, 70, 160, 56, 151, 243, 213, 1
09, 17, 232, 156]
  },
  "PersonInfo": {
    "PersonCode": "38507160203",
    "CompanyCode": ""
  }
}
```

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

MAC reikšmė susideda iš privačiuoju raktu pasirašytos eilutės: LicenseNumber+PersonCode + \_ + CompanyCode t.y. EL-E2523-9E792-7B21210000000001\_ CompanyCode nurodomas kai užklaustos vykdomos su el. spaudo sertifikatais.

Atsakymo pavyzdys:

```
{
  "ErrorNumber": 0,
  "ErrorMessage": null,
  "HasError": false,
  "MAC": "QyY5RyOiW139Li0zPtoci6LhBwC3c3eUE7ZAJTfVh3qaSTd4zxdlL2bktCzwKzSWQ6vneH67M62P8
g4P6150mND5+yPs2Ewon42uLHMU7sXRXMXuCyD0z5c6ZF+sglZe8vwAE/DU1Rmgbx2QWw5GA9reQVeTf59FrkBrB/
oEtnCGLi+Xz+leZ1XwnSS0w2unmAyd9FrX8ufr6H0fmf6T7w88D58LQGHLwjDKehidM3zu3pHd3MUwbJNAYkX20X
ZeSypALLV4PJHxQphGoBURucNI4Z7bZ0iL27Dk0QJkryhF7+Pcg9wPu3MSTRabZJqZwyhEU5hcXkqyC3BLq9CWA=="
}
```

Error.MAC yra skaičiuojamas MAC iš grąžintų laukų pasirašant tokeną serverio privačiu raktu. Klientas **privalo** patikrinti ar gautas MAC'as ir grąžintos reikšmės sutampa. Token'as kuri šiuo atveju reikia tikrint serverio viešuoju raktu: 0

#### 4.4.19. „Test“ REST metodas

„Test“ metodas skirtas patikrinti LT ID serviso bei komponentų veikimą. Šį metodą galima kviesti diagnostikos, testavimo ir patikros tikslais. Pavyzdžiui Paslaugų Tiekėjo sistema, kartas nuo karto kreipiasi į šį metodą įsitikinti, ar servisas yra veiksnus. Gavus neigiamą atsakymą, galima iš karto informuoti Naudotojus apie neveikiančią paslaugą, arba gauti įspėjimą apie negaliojančią licenciją ir pan.

Metodas patikrina:

- LT ID serviso veiksnumą;
- licencijos duomenis;
- MAC formavimą.

PASTABOS: „Test“ metodas netikrina visos LT ID infrastruktūros veiksnumo. Sėkmingos užklaustos atveju grąžinamo parametro „ErrorResult“ atributo „ErrorMessage“ reikšmė nebūna tuščia – pateikiamas tekstas „SYSTEMOK“.

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

„Test“ metodo užklauso parametrai:

Pavadinimas	Tipas	Aprašymas
SP	<a href="#">SPInfo</a>	Perduodamas licencijos numeris, kuris buvo gautas iš Patikimo Paslaugų Tiekėjo, ir MAC suformuotas iš licencijos pasirašytos eilutės.

Visi parametrai privalomi.

„Test“ metodo grąžinamas atsakymo rezultatas – [ErrorResult](#).

„Test“ metodo užklauso – atsakymo pavyzdys:

POST: <https://api.ltid.lt/api/test>

Užklauso pavyzdys:

```
{
  "SPInfo": {
    "LicenseNumber": "EL-E2523-9E792-7B212",
    "MAC": [79, 8, 154, 248, 209, 50, 93, 203, 55, 179, 21, 71, 115, 209, 242, 236, 1
50, 223, 80, 61, 212, 170, 42, 109, 198, 115, 118, 166, 180, 41, 193, 171, 196, 118, 199,
107, 242, 6, 29, 198, 188, 59, 99, 158, 105, 108, 96, 154, 85, 60, 207, 25, 180, 174, 3,
23, 161, 20, 99, 30, 3, 71, 149, 22, 66, 227, 71, 24, 226, 16, 188, 80, 250, 53, 148, 12
9, 122, 173, 160, 144, 99, 84, 44, 0, 74, 123, 16, 52, 77, 222, 210, 108, 86, 76, 182, 24
, 237, 154, 30, 184, 2, 76, 112, 142, 94, 64, 223, 216, 135, 173, 36, 16, 18, 211, 5, 195
, 37, 242, 62, 78, 94, 218, 215, 73, 205, 24, 214, 161, 144, 151, 196, 235, 227, 71, 35,
117, 227, 166, 232, 133, 217, 16, 196, 99, 122, 15, 253, 105, 254, 156, 109, 127, 241, 11
1, 132, 239, 215, 140, 97, 43, 230, 56, 55, 113, 252, 218, 213, 161, 16, 98, 174, 93, 36,
25, 58, 199, 165, 55, 91, 205, 117, 35, 52, 69, 205, 77, 122, 147, 225, 90, 210, 117, 23
6, 141, 46, 175, 40, 105, 48, 81, 241, 107, 125, 30, 188, 179, 17, 127, 224, 252, 6, 142,
90, 123, 173, 81, 112, 73, 34, 105, 243, 190, 94, 197, 96, 16, 104, 25, 187, 63, 13, 252
, 65, 12, 147, 92, 251, 80, 245, 236, 39, 255, 54, 18, 13, 218, 61, 192, 234, 22, 237, 75
, 152, 219, 13, 53]
  }
}
```

MAC reikšmė susideda iš privačiuoju raktu pasirašytos eilutės: LicenseNumber t.y. EL-E2523-9E792-7B212

Atsakymo pavyzdys:

```
{
  "ErrorNumber": 0,
```

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

```

"ErrorMessage": "SYSTEMOK",
"HasError": false,
"MAC": null
}

```

Error.MAC yra skaičiuojamas MAC iš grąžintų laukų pasirašant tokeną serverio privačiu raktu.

Klientas **privalo** patikrinti ar gautas MAC'as ir grąžintos reikšmės sutampa.

Token'as kuri šiuo atveju reikia tikrinti serverio viešuoju raktu: 0SYSTEMOK

#### 4.4.20. „LoginLTID“ REST metodas

LoginLTID metodas yra skirtas vartotojų arba duomenų autentifikacijai naudojant LTID parašą.

„LoginLTID“ metodo užklauso parametrai:

Pavadinimas	Tipas	Aprašymas
SP	<a href="#">SPInfo</a>	Perduodamas licencijos numeris, kuris buvo gautas iš Patikimo Paslaugų Tiekėjo, ir MAC suformuotas iš licencijos numerio ir kitų parametų pasirašytos eilutės.
Person	<a href="#">PersonInfoLTID</a>	Fizinio asmens atveju paduodamas fizinio asmens kodas. Įmonės atveju paduodamas įmonės kodas ir fizinio asmens kodas.
DTBS	byte[]	(angl. <i>Data to be signed</i> ) – tai duomenys, kuriuos galutinis Naudotojas pasirašys LT ID elektroniniu parašu.

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

Pavadinimas	Tipas	Aprašymas
DTBD	string	(angl. <i>Data to be displayed</i> ) – tai tekstas, kurį galutinis Naudotojas išvys LT ID aktyvavimo įrenginyje. Jeigu šis parametras bus tuščias, bus rodomas standartinis licencijoje įvestas tekstas.  Į vieną telefono ekraną telpa apie 60 ženklų, todėl siūloma naudoti kompaktiškus tekstus, sudarytus iš Paslaugų teikėjo pavadinimo ir keturių skaičių kontrolinio kodo, kuriuos vartotojai turėtų sulyginti su kontroliniais kodais, rodomais kompiuterio ekrane. Pavyzdžiui, DTBD="Turto Bankas. Kontrolinis kodas: 2233". Atvejais, kai šio lauko ilgis didesnis nei 60 ženklų, tekstas gali būti išskaitytas į daug dialoginių langų.
HashUsage	<a href="#">HashType</a>	Šis parametras nurodo, koks maišos algoritmas buvo panaudotas formuojant DTBS lauką. Parametras panaudojamas DTBS turinio kontrolei.
Timeout	int	Laiko tarpas sekundėmis, kiek daugiausiai gali užtrukti autentifikacija.

Visi parametrai privalomi.

„LoginLTID“ metodo grąžinamas atsakymo rezultatas – [SessionResult](#).

„LoginLTID“ metodo užklausos – atsakymo pavyzdys:

POST <https://api.lttd.lt/api/loginltid>

Užklausos pavyzdys:

```
{
  "SPInfo": {
    "LicenseNumber": "EL-E2523-9E792-7B212",
    "MAC": [8, 84, 38, 39, 81, 199, 192, 167, 149, 30, 147, 75, 231, 110, 237, 81, 15
5, 175, 237, 10, 132, 102, 1, 219, 142, 183, 184, 147, 6, 191, 144, 188, 74, 211, 69, 38,
17, 127, 204, 172, 219, 236, 239, 61, 221, 211, 229, 11, 173, 162, 144, 71, 102, 227, 28
, 183, 228, 169, 245, 48, 66, 33, 97, 50, 251, 233, 230, 11, 250, 95, 175, 59, 189, 1, 13
4, 143, 130, 138, 161, 80, 12, 233, 9, 203, 65, 228, 29, 119, 113, 182, 74, 8, 137, 218,
```

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

```

44, 102, 185, 208, 210, 200, 116, 16, 53, 123, 5, 69, 176, 117, 96, 46, 41, 239, 185, 152
, 5, 169, 28, 191, 205, 211, 192, 236, 152, 113, 216, 186, 69, 119, 50, 53, 109, 103, 137
, 129, 28, 7, 9, 178, 132, 171, 148, 160, 77, 36, 229, 179, 106, 25, 93, 206, 57, 107, 50
, 148, 9, 159, 6, 232, 138, 129, 218, 106, 210, 136, 221, 220, 190, 61, 88, 155, 216, 189
, 182, 11, 22, 113, 151, 116, 105, 89, 112, 72, 227, 88, 54, 149, 200, 123, 74, 111, 141,
94, 247, 208, 203, 179, 211, 180, 54, 83, 6, 6, 220, 184, 229, 94, 35, 12, 234, 222, 87,
226, 43, 94, 158, 206, 75, 50, 239, 237, 102, 233, 148, 116, 100, 113, 19, 175, 255, 235
, 182, 155, 177, 55, 71, 104, 179, 165, 164, 33, 72, 111, 185, 134, 83, 27, 105, 1, 137,
12, 110, 192, 77, 245, 222, 214]
},
"PersonInfo": {
  "PersonCode": "10000000001",
  "CompanyCode": ""
},
"DTBS": [1,2,3],
"DTBD": "prisijungimas",
"HashType": "HashedSHA1",
"Timeout": 100
}

```

MAC reikšmė susideda iš privačiuoju raktu pasirašytos eilutės: LicenseNumber + PersonCode + \_ + CompanyCode + HashType + DTBS + DTBD + Timeout t.y.

EL-E2523-9E792-7B21210000000001\_HashedSHA1AQIDprisijungimas100

CompanyCode nurodomas kai užklauso vykdomos su el. spaudo sertifikatais

Atsakymo pavyzdys:

```

{
  "SessionID": 1401285,
  "Error": {
    "ErrorNumber": 0,
    "ErrorMessage": null,
    "HasError": false,
    "MAC": null
  }
}

```

Sesijos ID naudojamas StatusLTID metode užklauso statusui tikrinti.

Error.MAC yra skaičiuojamas MAC iš grąžintų laukų pasirašant tokeną serverio privačiu raktu.

Klientas **privalo** patikrinti ar gautas MAC'as ir grąžintos reikšmės sutampa.

Token'as kuri šiuo atveju reikia tikrint serverio viešuoju raktu: 0SessionId

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

#### 4.4.21. „SignLTID“ REST metodas

„SignLTID“ metodas skirtas pasirašymo paslaugai naudojant LTID parašą ar spaudą. El. dokumentų ar duomenų pasirašymui LT ID parašu turi būti paduodamas pasirašančio asmens kodas, LT ID spaudu – asmens, kuris užsakė ir gavo LT ID spaudą, fizinio asmens bei įmonės, kuriai buvo išduotas LT ID spaudas, kodai.

„SignLTID“ metodo užklausos parametrai:

Pavadinimas	Tipas	Aprašymas
SP	<a href="#">SPInfo</a>	Perduodamas licencijos numeris, kuris buvo gautas iš Patikimo Paslaugų Tiekėjo, ir MAC suformuotas iš licencijos numerio ir kitų parametru pasirašytos eilutės.
Person	<a href="#">PersonInfoLTID</a>	Fizinio asmens atveju paduodamas fizinio asmens kodas. (El. parašas) Įmonės atveju paduodamas įmonės kodas ir fizinio asmens kodas. (El. spaudas)
DTBS	byte[][]	(angl. <i>Data to be signed</i> ) – tai duomenys, kuriuos Galutinis Naudotojas pasirašys LT ID elektroniniu parašu ar spaudu. Galima paduoti daugiau nei vieną dokumentą. Kiekvienas dokumentas yra baitų masyvas. Metodas priima masyvą dokumentų.

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

Pavadinimas	Tipas	Aprašymas
DTBD	String	(angl. <i>Data to be displayed</i> ) – tai tekstas, kurį galutinis Naudotojas išvys LT ID aktyvavimo įrenginyje. Jeigu šis parametras bus tuščias, bus rodomas standartinis licencijoje įvestas tekstas.  Į vieną telefono ekraną telpa apie 60 ženklų, todėl siūloma naudoti kompaktiškus tekstus, sudarytus iš Paslaugų teikėjo pavadinimo ir keturių skaičių kontrolinio kodo, kuriuos vartotojai turėtų sulyginti su kontroliniais kodais, rodomais kompiuterio ekrane. Pavyzdžiui, DTBD="Turto Bankas. Kontrolinis kodas: 2233". Atvejais, kai šio lauko ilgis didesnis nei 60 ženklų, tekstas gali būti išskaitytas į daug dialoginių langų.
HashUsage	<a href="#">HashType</a>	Šis parametras nurodo, koks maišos algoritmas buvo panaudotas formuojant DTBS lauką. Parametras panaudojamas DTBS turinio kontrolei.
Timeout	int	Laiko tarpas sekundėmis, kiek daugiausiai gali trukti pasirašymas.

Visi parametrai privalomi.

„SignLTID“ metodo grąžinamas atsakymo rezultatas – [SessionResult](#).

„SignLTID“ metodo užklausa – atsakymo pavyzdys:

POST: <https://api.ltid.lt/api/signltid>

Body pavyzdys:

```
{
  "SPInfo": {
    "LicenseNumber": "EL-E2523-9E792-7B212",
    "MAC": [95, 166, 135, 128, 213, 138, 148, 223, 65, 55, 188, 167, 218, 249, 205, 1
08, 10, 22, 60, 112, 155, 142, 109, 210, 102, 206, 131, 108, 40, 86, 41, 186, 181, 250, 2
46, 253, 100, 69, 55, 108, 37, 12, 59, 12, 148, 18, 201, 44, 87, 255, 58, 185, 74, 228, 1
```

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

```

06, 54, 153, 216, 228, 214, 185, 203, 78, 67, 73, 64, 79, 142, 232, 107, 1, 167, 215, 233
, 94, 195, 95, 229, 156, 28, 56, 179, 192, 27, 36, 103, 214, 55, 22, 75, 186, 2, 121, 116
, 122, 228, 39, 106, 49, 106, 135, 174, 116, 173, 77, 227, 17, 140, 145, 128, 26, 4, 154,
1, 138, 92, 180, 110, 33, 81, 112, 241, 197, 90, 220, 144, 152, 201, 219, 239, 192, 0, 1
21, 27, 242, 52, 137, 139, 215, 110, 63, 156, 214, 47, 201, 237, 236, 196, 175, 119, 112,
178, 72, 206, 64, 198, 225, 30, 156, 150, 113, 225, 54, 78, 98, 28, 145, 226, 153, 77, 2
6, 0, 227, 198, 65, 125, 201, 184, 101, 65, 190, 129, 215, 242, 246, 29, 38, 245, 149, 43
, 115, 141, 200, 134, 174, 5, 4, 27, 142, 65, 248, 144, 95, 152, 80, 78, 135, 73, 214, 20
2, 74, 78, 200, 186, 55, 152, 232, 8, 136, 191, 179, 226, 5, 147, 95, 154, 19, 104, 239,
102, 20, 206, 105, 212, 223, 58, 192, 162, 6, 57, 206, 148, 87, 175, 63, 56, 158, 137, 21
4, 123, 62, 57, 31, 199, 157, 92]
},
"PersonInfo": {
  "PersonCode": "10000000001",
  "CompanyCode": ""
},
"DTBS": [[1,2,3],[1,2,3]],
"DTBD": "prisijungimas",
"HashType": "HashedSHA1",
"Timeout": 100
}

```

MAC reikšmė susideda iš privačiuoju raktu pasirašytos eilutės: LicenseNumber + PersonCode + \_  
+ CompanyCode + HashType + DTBS + DTBD + Timeout t.y.

EL-E2523-9E792-7B2121000000001\_HashedSHA1AQIDAQIDprisijungimas100

CompanyCode nurodomas kai užklauso vykdomos su el. spaudo sertifikatais.

Atsakymo pavyzdys:

```

{
  "SessionID": 1401289,
  "Error": {
    "ErrorNumber": 0,
    "ErrorMessage": null,
    "HasError": false,
    "MAC": null
  }
}

```

Sesijos ID naudojamas StatusLTID metode užklauso statusui tikrinti.

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

Error.MAC yra skaičiuojamas MAC iš grąžintų laukų pasirašant tokeną serverio privačiu raktu.

Klientas **privalo** patikrinti ar gautas MAC'as ir grąžintos reikšmės sutampa.

Token'as kuri šiuo atveju reikia tikrint serverio viešuoju raktu: 0SessionId

#### 4.4.22. „GetCertificatesLTID“ REST metodas

„GetCertificatesLTID“ metodas skirtas grąžinti galutinio naudotojo turimus aktyvius sertifikatus.

„GetCertificatesLTID“ metodo užklauso parametrai:

Pavadinimas	Tipas	Aprašymas
SP	<a href="#">SPIInfo</a>	Perduodamas licencijos numeris, kuris buvo gautas iš Patikimo Paslaugų Tiekėjo, ir MAC suformuotas iš licencijos numerio ir kitų parametru pasirašytos eilutės.
Person	<a href="#">PersonInfoLTID</a>	Fizinio asmens atveju paduodamas fizinio asmens kodas. Įmonės atveju paduodamas įmonės kodas ir fizinio asmens kodas.

Visi parametrai privalomi.

„CertificatesLTID“ grąžinamas rezultatas:

Pavadinimas	Tipas	Aprašymas
Error	<a href="#">ErrorResult</a>	Klaida vykdant metodą (jei Error.ErrorNumber = 0, metodas įvykdytas be klaidų).
Certificate	string	Sertifikatas base-64 formatu.

„GetCertificatesLTID“ metodo užklauso – atsakymo pavyzdys:

POST: <https://api.ltid.lt/api/certificatesltid>



LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

```

AQkBFgZzQHmubHQxCzAJBgNVBAYTAkxUMRswGQYDVQQDExJOT1REBUkFTIE5PVEFS
SUFOQVMxEzARBgNVBAQTCk5PVEFSSUFOQVMxEDAOBgNVBCoTB05PVEFSQVMxFDAS
BgNVBAUTCzEwMDAwMDAwMDAxMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKc
AQEA3CIrBjXNpIP6ML38Mh+3nItqsXaVXvYuEmIE+QUkSlaNb+hMTUWHo2nCVboS
5FsX+CtLzmOaR26aAKVYbStyt+xMhlpO3ZjTxBnXYR7L2/ZsPqceCH75vtl8hAK5
iygSFeJP8JjdyYt7H39XGbdUhoLdcW707DpU6Z9mnPgTdiurKhBLZeVzud3pVjP
/GA2OX5RwCgCho+Fxm08bEX4kCMQRWyJgRh+wNKMntj3SYAFdZHwWsruiKpMx1S9
bMKl0s9e1W0ZcSnLiKHY9fOpv7U9FFCWgLbnwCiXUJZ8A/A3IbR95L1dSH5B/RTZ
9KmtF/Sc94S2dpf2R7uvwFM1twIDAQABo4IBxzCCAcMwDgYDVR0PAQH/BAQDAgeA
MB0GA1UdDgQWBRT+o3pNDg/ZqQhozLY6eT/AERTQTafBgNVHSMEGDAWgBSsAx3w
Bh61eAECLDkdYj2ut1rcijA7BgNVHR8ENDAyMDCgLqAshipodHRwOi8vY3NmMi5y
Y3NjLmx0L2NkcC9SQ1NDX01zc3VpbmdDQS5jcmwwewYIKwYBBQUHAQEebZbtMDMG
CCsGAQUFBzABhidodHRwOi8vb2NzcDIucmNzYy5sdC9vY3NwcmVzcG9uZGVyLnJj
c2MwNgYIKwYBBQUHMAKGKmh0dHA6Ly9jc3AyLnJjc2MubHQvYW1hL1JDU0NfSXNz
dWluZ0NBmNydDA9BgkrBgEEAYI3FQcEMDAuBiYrBgEEAYI3FQiCnOx7hKbACoTl
kQ6Gk5hj4LRXoFhj/MIg4bTLgIBZAIbcZATBgNVHSUEDDAKBggrBgEFBQcDAjBG
BgNVHSAEPzA9MDsGCysGAQQBgfe3AQIGMCwwKgYIKwYBBQUHAQEWHmh0dHA6Ly93
d3cucmNzYy5sdC9yZXBvc2l0b3J5LzAbBgkrBgEEAYI3FQoEDjAMMAoGCCsGAQUF
BwMCMA0GCSqGSIb3DQEBCwUAA4IBAQBEG55X/dh1ZqTZ4POpznfHmwW0S6CUhMLEF
EhkGF68F1AyzRe+bsZLDjOuvIPRIIEqox5h9iPUmnLK1icsdcmv+YCoB79H9cpUp
CvblA0zRrPuxYbX3CqVob7ai2G7a6dAK1HPJAp+nhKI5Eq4W0taGNmwbGY0BFX6D
0ZWxOJY/1ICg7PaiEg1JV4GyIlkY+6A2bHqngkSgxGvKkgdHMKeG7jEutmhiDpGs
idZXAzm0+OLrKRWDOn+ZbDM71c937K7aahukxca/pr2X0WEZY2EvpwSukgsbHVPF
oD2s+Ct+sX2yiTCHRHwrRj0d8QXJRIVMjZipewyHqMOVKymRfBAN"
}

```

Error.MAC yra skaičiuojamas MAC iš gražintų laukų pasirašant tokeną serverio privačiu raktu.

Klientas **privalo** patikrinti ar gautas MAC'as ir gražintos reikšmės sutampa.

Token'as kuri šiuo atveju reikia tikrint serverio viešuoju raktu: 0Certificate

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

## Priedas A. Viešųjų raktų formatai

wPKITSP servisas gali priimti kelis viešojo rakto formatus: PKCS#1 arba X.509 SubjectPublicKeyInfo. Be to, nepriklausomai nuo formato, raktas gali būti užkoduotas PEM arba DER koduotėmis. Naudojantis wPKITSP servisu rekomenduotina naudoti X.509 SubjectPublicKeyInfo formatą PEM koduotėje.

- **PKCS#1** viešojo rakto formatas. Jis naudojamas viešajam raktui saugoti sertifikate, o X.509 SubjectPublicKeyInfo apgaubia šį formatą.

- Asn1 **PEM** koduotėje:

-----BEGIN RSA PUBLIC KEY-----

```
MIIBCgKCAQEAwphU9VBbjJqDE828gckVxUZd32NoXJMDF/tGUmSYZtPg2tc33X2OpCCcggibJRai
gASX2ySsmogio+k+wwJW9K+CulgebkU6bEdIAEDFAzuaSsr1cnc2LaIAoKh13GAW2NMQeqLitfx
MMdT4ditQwVUjPwmNnb08NIokZnYIwbhAF87PgSz6zqbj/VAvpRBZrST8u8NvHOTImPP2OnrFOI
iImkrauOaRcmboSgTbdDHVAsDbrPH6P6dbE6MgQtInZsZqfBqqzviJiOb1tdsI3pW68yPdB+4wCi
3qrr+2bnnJhgZnPYE2W+7GeW9IUUevs2F6c+3wQm6YOZayg0swIDAQAB
```

-----END RSA PUBLIC KEY-----

- Asn1 **DER** koduotėje:

```
3082010A0282010100D4DE0B07CBC328682134E8BD0EA7D3252766FD94AF082E9E43538D50F183
05013B1F8BDB6E072E6BEDA5F0D5BBBBC46DA5F72EC51715917B53B3E74334096682595439541
C6270C65055BD7819FBBE090DC92EDA5E26459DC194E6F8FBEEBAB06906446C215FAB32554883
C19A76B67C99013BA32393484BA5F9AF1B57247F4FC40F2542BB536F9C41A3827512C9CF6460C9
9B450E1FED62A4E4C4619B5376D6F69BB802904337A45D5435C09ACEE4E384C36415D6B7012674
946E8E931B17F109835CFE161AD2774D5710E704DEFD98CF8E790417B112814785DFC7C9267BF2
7A075390A6EF78FE61BCBDDFC533642F55D48F398EB4070639D913BA479F29090203010001
```

- **X.509 SubjectPublicKeyInfo** viešojo rakto formatas. Jis naudojamas **OpenSsl** bibliotekoje. Taip pat šis formatas asn1 PEM koduotėje gražinamas Paslaugų Tiekėjui iš Patikimo Paslaugų Tiekėjo.

- Asn1 **PEM** koduotėje:

-----BEGIN PUBLIC KEY-----

```
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0ANZ6DAwL54g4dlcWscnBfkjH8BrQf3Q
```

LT ID identifikavimo ir pasirašymo paslauga. Serviso vadovas	Versija: 1.4
Programinės įrangos dokumentas	Data: 2024-03-25

Ogv/DEurlszsWiGfvYWsdGIgVFscaax7YDb9mijdQji9jsRIcjkh/+U7rXNr9wRPryhEqIq/b8r6  
tIPCdA+VF12glDYZ6U6yDn5hnpPX6Ua5uV4L4dMAicDIx7e5VrsHtEzUJLT61nRQhHond0rGNYSZ  
hkh5TvRI1uR+m6+q6HBdqXxXPkfyHH9ZpyF2kttBNOPS3z/UMmWSJY/T6tzm3eTR/t9RXmw4Bqn5  
3IbLFtATWWzz8jOQYMixaOx2nVSnAcgc4zsgWwP6eOEyI7JzCTyQEGaUYPJSpTlqhbbU48Po5Yz6  
Ok7kzwIDAQAB  
-----END PUBLIC KEY-----

- Asn1 **DER** koduotėje:

30820122300D06092A864886F70D01010105000382010F003082010A0282010100D00359E830302  
F9E20E1D95C5AC72705F9231FC06B41FDD03A0BFF0C4BAB96CCEC5A219FBD85AC746220545B1C  
69AC7B6036FD9A28DD4238BD8EC448723921FFE53BAD736BF7044FAF2844A88ABF6FCAFAB483C  
2740F95175DA0943619E94EB20E7E619E93D7E946B9B95E0BE1D30089C0C8C7B7B956BB07B44C  
D424B4FAD67450847A27774AC6358B198648794EF448D6E47E9BAFAAE8705DA97C573E47F21C7F  
59A7217692DB4134E3D2DF3FD4326592258FD3EADCE6DDE4D1FEDF515E6C3806A9F9DC86CB16  
D013596CF3F2339060C8B168EC769D54A701C81CE33B205B03FA78E13223B273093C9010669460  
F252A5396A8616D4E3C3E8E58CFA3A4EE4CF0203010001