METAI LAIKO SU **SECTIGO CA**: PATIRTIS IR NAUJIENOS

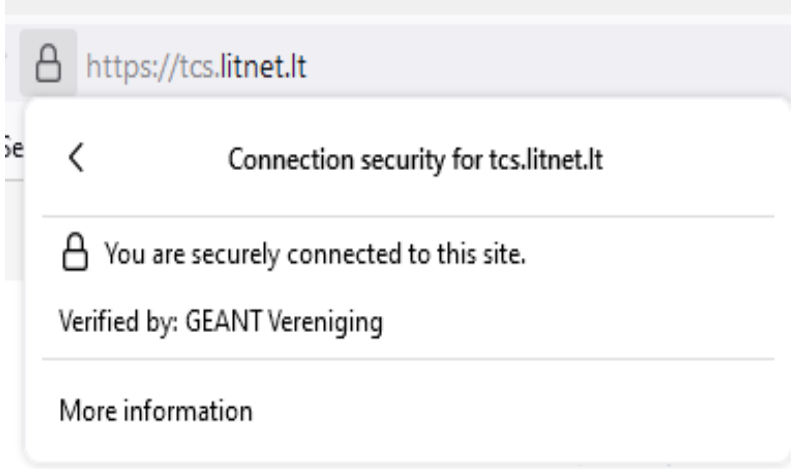
Seminaras "LITNET paslaugų naujienos Mokslo ir studijų institucijom**"**

2021-12-01

Milda Mimienė

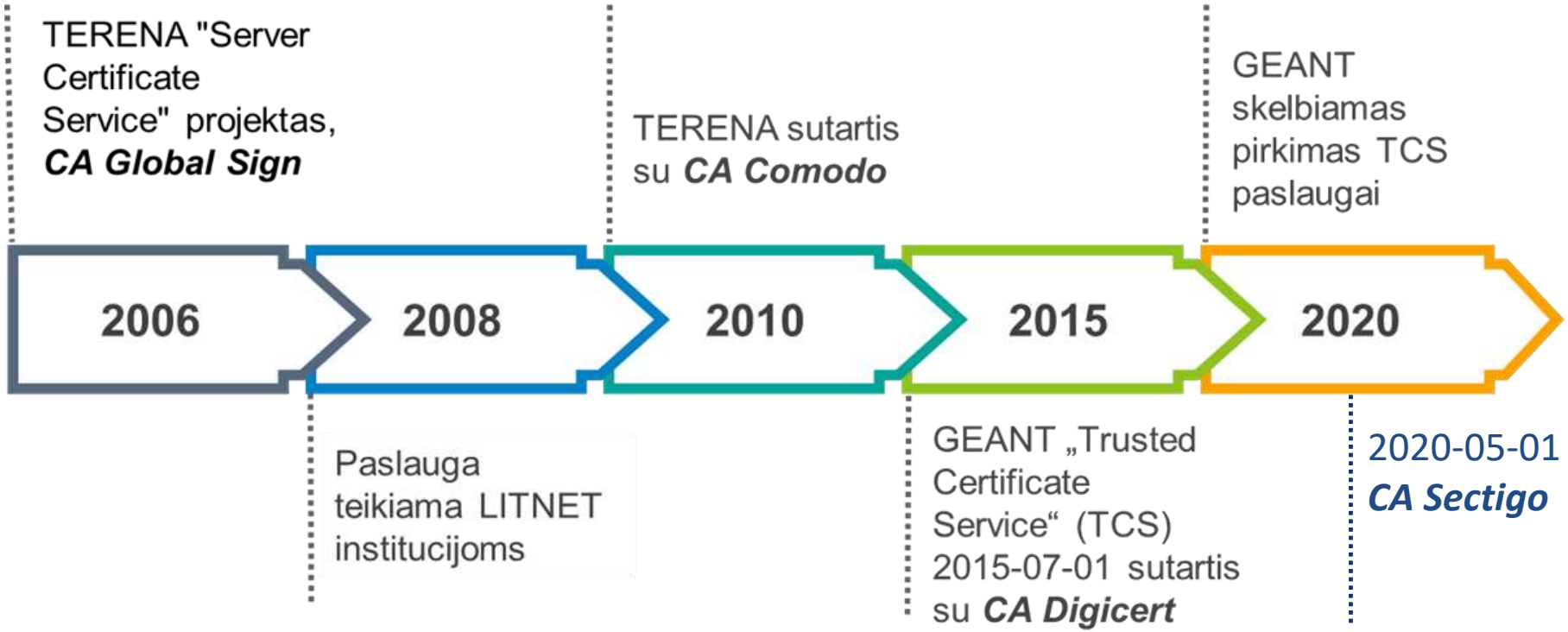
LITNET KTU TC/LITNET CERT

Skaitmeniniai sertifikatai



- ✓Saugus duomenų perdavimo protokolas SSL (*Secure Sockets Layer*)
- ✓SSL sertifikatas – skaitmeninių raktų rinkinys, diegiamas tarnybinėje stotyje
- ✓Skaitmeninis sertifikatas tarp tarnybinės stoties ir naudotojo naršyklės sukuria saugų, šifruojamą duomenų perdavimo kanalą
- ✓SSL sertifikatas patvirtina svetainės tapatybę
- ✓SSL sertifikatus išduoda Sertifikavimo tarnybos
- ✓SSL sertifikatas yra saugios/tvarkingos svetainės įvaizdis

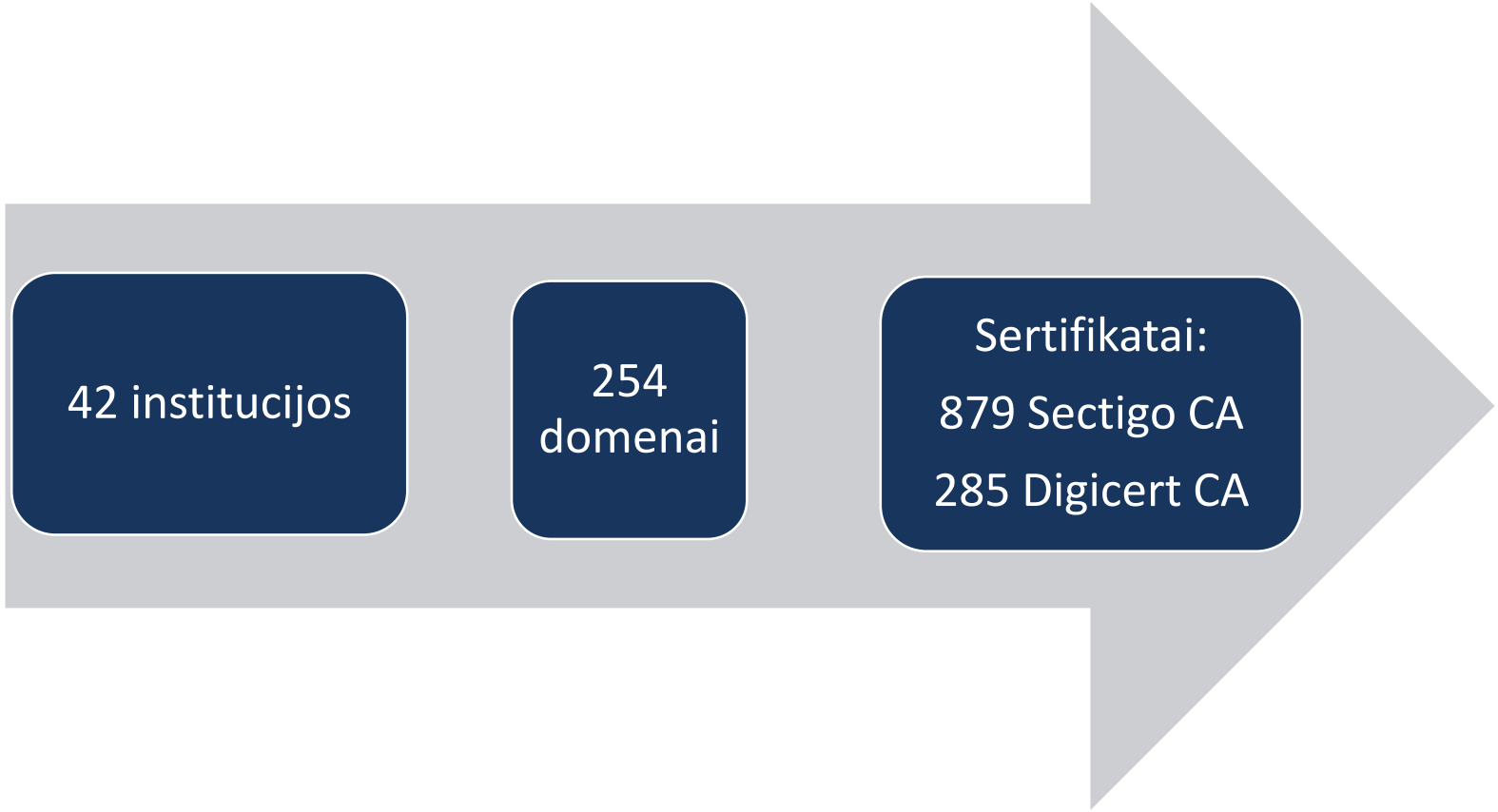
TCS istorija



Išduodami sertifikatai

- SSL sertifikatai (**OV** ir **EV**)
  - ✓SSL (*www.manoinstitucija.lt*)
  - ✓Multi Domain SSL (*www.manoinstitucija.lt, www.mano-institucija.lt, mail.manoinstitucija.lt*)
  - ✓WildCard (**.manoinstitucija.lt*)
- Programinio kodo sertifikatai
- Vardiniai sertifikatai (reikalinga SSO ir „Face to Face“ patikros procesas)

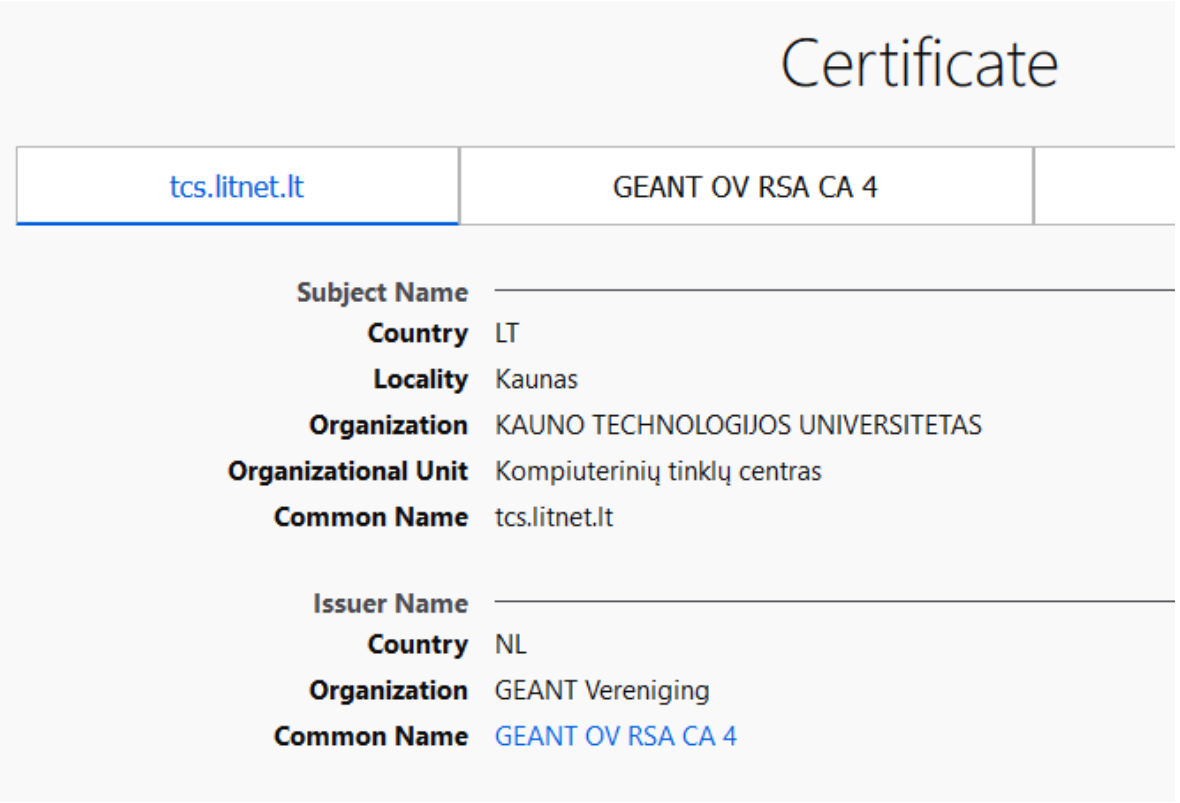
GEANT TCS paslauga



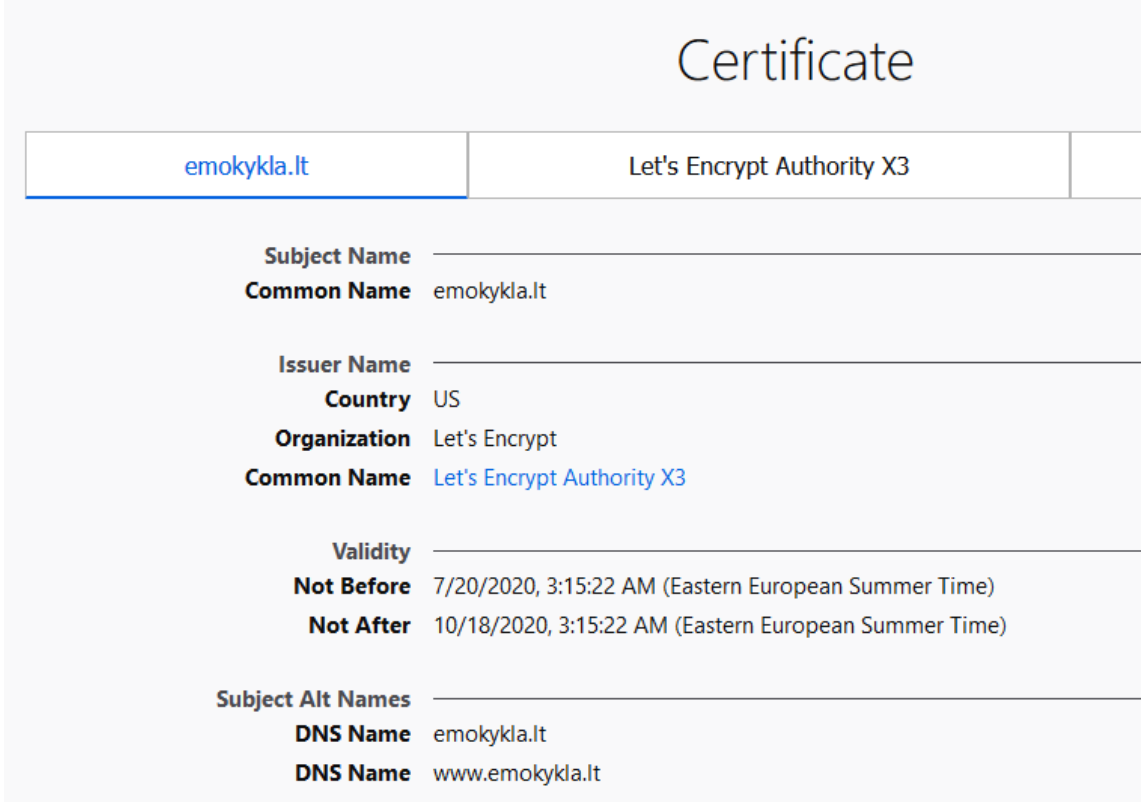
Kodėl GEANT TCS?

- ✓Pasaulinis sertifikatų pripažinimas;
- ✓Už paslaugą mokama iš LITNET lėšų;
- ✓Institucijoms nereikia atskirai rūpintis sertifikatų paslaugos pirkimu;
- ✓Institucijos gali užsisakyti sertifikatus pagal poreikį (tiek kiek reikia).

GEANT TCS vs Let‘s Encrypt

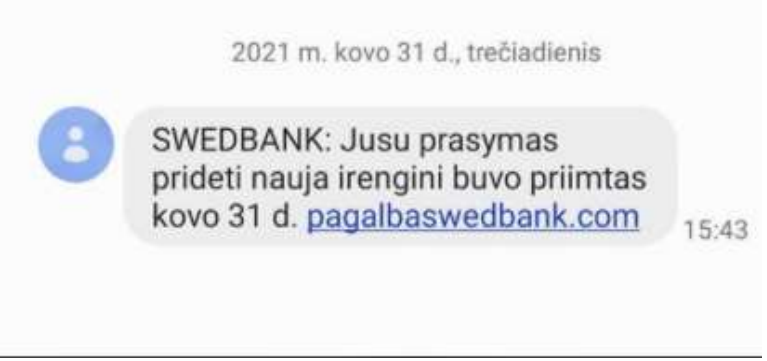


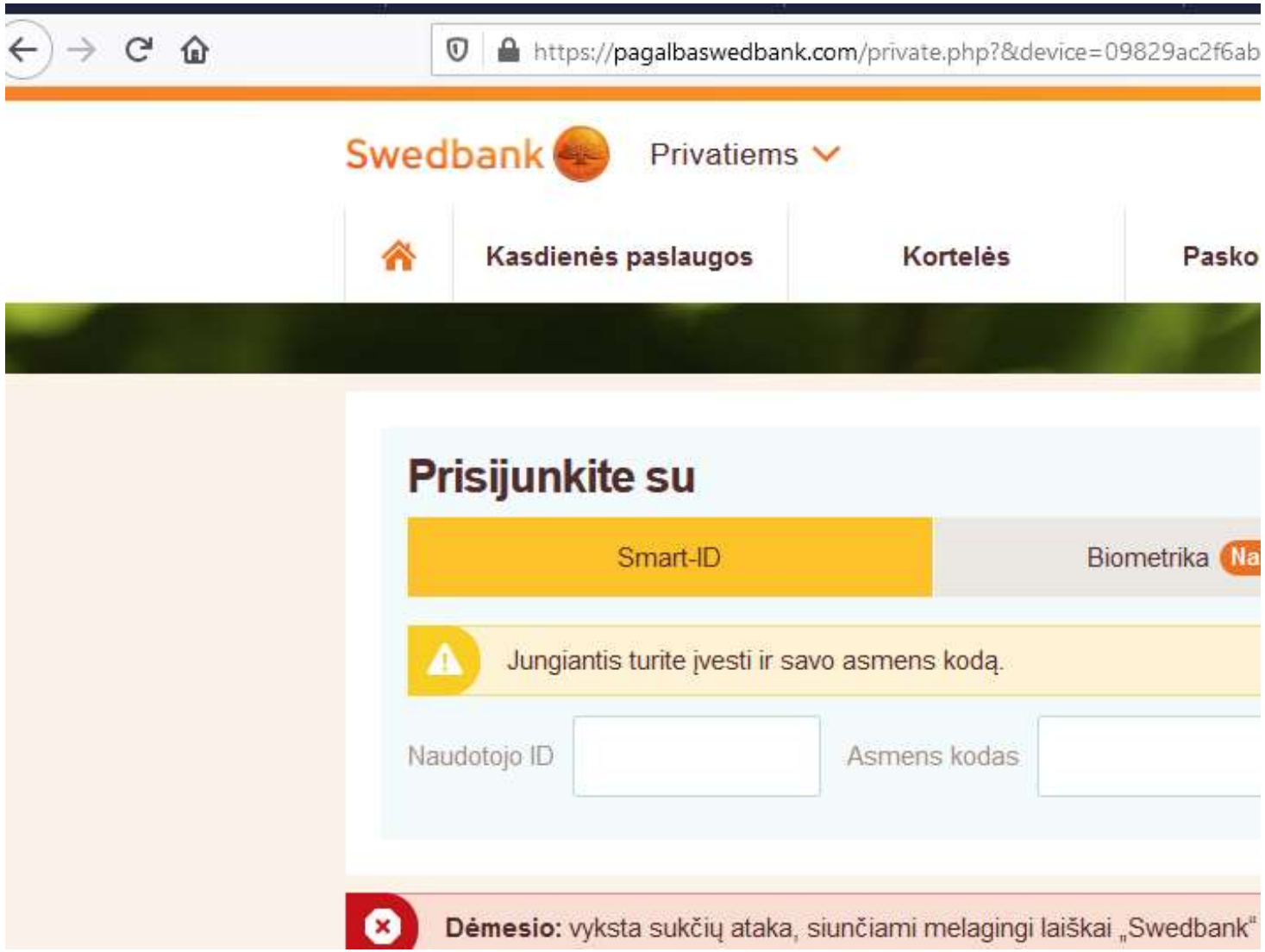
OV SSL sertifikatas



DV SSL sertifikatas

Kodėl OV SSL sertifikatas?





OV ar DV sertifikatas?

www.swedbank.lt | DigiCert SHA2 Extended Validation Server CA

Subject Name

Business Category	Private Organization
Inc. Country	LT
Serial Number	112029651
Country	LT
Locality	Vilnius
Organization	Swedbank AB
Common Name	www.swedbank.lt

pagalbaswedbank.com | Sectigo RSA Domain Validation Secure Server CA | USERTr

Subject Name

Common Name	pagalbaswedbank.com

Issuer Name

Country	GB
State/Province	Greater Manchester
Locality	Salford
Organization	Sectigo Limited
Common Name	Sectigo RSA Domain Validation Secure Server CA

Validity

Not Before	Wed, 31 Mar 2021 00:00:00 GMT
Not After	Thu, 31 Mar 2022 23:59:59 GMT

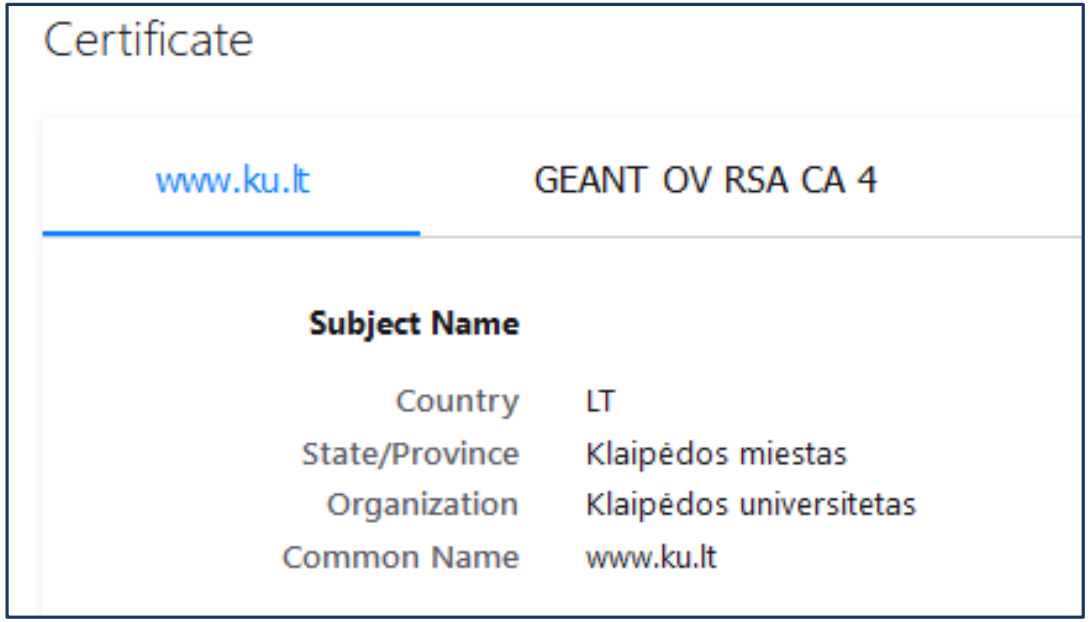
Subject Alt Names

DNS Name	pagalbaswedbank.com

Pasikeitimai nuo 2020-05-01

- ✓ sertifikatų galiojimo terminas 1 metai (2020-08-18);
- ✓ į sertifikatą yra įtraukiama tik ***State/Province*** reikšmė, aprašoma pagal ISO (2021-09-01) : https://www.iso.org/obp/ui/#iso:code:3166:LT

CA/BROWSER FORUM



Sectigo pasikeitimai ir patirtis

- ✓ Nauja Sectigo Certificate Manager (SCM) versija SCM 21.11;
- ✓ HTTP/HTTPS validavimo metodas – tik vienam domenui (2021-11-22):
  - Domenų validacija gali būti atšaukta, jei domenas validuotas HTTP/HTTPS metodu ir naudojamas Wildcard sertifikate;
  - Išduoti sertifikatai galios iki dienos nurodytos sertifikate (t.y nebus atšaukiami)

https://sectigo.com/knowledge-base/detail/Domain-Control-Validation-DCV-using-file-based-validation-policy-change/kA03l000000Xsf9

Patarimas – naudokite E-MAIL ir CNAME validavimo metodus

Paslaugos užsakymas

https://tcs.litnet.lt

- ✓Prijungtos prie LITNET kompiuterių tinklo
- ✓Mokslo ir studijų institucijos, ir/arba nepelno siekiančios
- ✓Oficialiai registruotos Lietuvos Respublikoje

1. Paslaugos užsakymo formos užpildymas (*tcs.litnet.lt*);
2. Institucijos registracija **Sectigo CA SCM** portale;
3. Sukuriamos paskyros institucijos administratoriams;
4. Administratoriai jungiasi prie sukurtos paskyros **SCM** portale ir naudojasi paslauga:
   - prideda institucijos valdomus domenus ir užsako jų patikrą (angl. Validation);
   - pateikia sertifikatų prašymus ir gauna sertifikatus;
   - rengia ataskaitas;
   - Reikia reikia kreipiasi pagalbos tiek į Sectigo support komandą, tiek į GEANT TCS paslaugos administratorių LITNET‘o tinkle.

Ačiū už dėmesį

Milda Mimienė

El. paštas tcs@litnet.lt

https://tcs.litnet.lt

Tel. +370 37 300645