Conformity Assessment Report: Conformity Certificate and Summary

TelekomSecurity.031.0301.06.2023

Trust Service Provider:

State Enterprise Centre of Registers

Conformity Certificate

TelekomSecurity.031.0301.06.2023

pursuant to Article 20 par. 1 of REGULATION (EU) No. 910/2014[1]

valid from 22.06.2023 and up to and including: 21.06.2025

Certification Body of Deutsche Telekom Security GmbH

Bonner Talweg 100, 53113 Bonn

This is to certify
– pursuant to Article 20 par. 1 of REGULATION (EU) No. 910/2014 –
that the

Trust Service Provider „State Enterprise Centre of Registers under the Ministry of the Economy and Innovation of the Republic of Lithuania“

provides the following trust services:

- **creating qualified certificates for electronic signatures**
- **creating qualified certificates for electronic seals**
- **creating qualified electronic timestamps**
- **remote QSCD management for qualified el. signatures/seals**

in accordance with the requirements of REGULATION (EU) No. 910/2014.

This certificate is filed and registered under **TelekomSecurity.031.0301.06.2023**

Dokument unterschrieben
von: Dr. Furgel, Igor
am: 02.06.2023 11:36
Ort: Bonn

Bonn, 02.06.2023

i.V. Dr. Igor Furgel
Head of Certification Body

T · · CERTIFICATION BODY

Deutsche Telekom Security GmbH – Certification Body – is an accredited Conformity Assessment Body (CAB).
DAkkS Registration No.: D-ZE-21631-01 (former Certification Body of T-Systems International GmbH, former registration no.: D-ZE-12025-01).

DAkkS Deutsche Akkreditierungsstelle D-ZE-21631-01-00

[1] REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

This Conformity Certificate consists of 15 pages.

1. Object of the conformity assessment

1.1 Name of the trust service provider

State Enterprise Centre of Registers
under the Ministry of the Economy and Innovation of the Republic of Lithuania
Original name: Valstybės įmonė Registrų Centras

Lvivo str. 25-101
09320 Vilnius

Lithuania

Tel.: +370 5 268 8262,
e-mail: info@registrucentras.lt
web: https://www.elektroninis.lt/, https://www.registrucentras.lt/.

1.2 Current confirmation status

State Enterprise Centre of Registers is a qualified trust service provider (qTSP) according to Art. 24 of eIDAS Regulation[2].

The last full conformity assessment according to Article 20(1) of eIDAS Regulation was accomplished with issuing the conformity certificate TelekomSecurity.031.0286.06.2021 as of 08.06.2021.

The current – 24 months periodic – conformity assessment of the TSP according to §20(1) eIDAS Regulation serves the continuation of its status as a ‘qualified trust service provider’ according to Article 24 eIDAS Regulation for all qualified trust services offered by the TSP.

The present assessment is based on (publicly available on https://www.elektroninis.lt/lt/n/teisininformacija-504)

[2] REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

- Rules For The Certification Practice Of The State Enterprise Centre Of Registers CP OF THE STATE ENTERPRISE CENTRE OF REGISTERS (OID: 1.3.6.1.4.1.30903.1.5.1), v. 1.1 as of 31.03.2023 (publicly available),

- the Certification Practice Statement for REMOTE ELECTRONIC SIGNATURE AND ELECTRONIC SEAL CPS_RS (remote signing/sealing; OID: 1.3.6.1.4.1.30903.1.6.1), v. 1.1 as of 31.03.2023 (publicly available),

- the Certification Practice Statement CPS_QC (non-remote services; OID: 1.3.6.1.4.1.30903.1.2.6), v. 6.8 as of 08.05.2022 (publicly available), and

- the Time-Stamping Practice Statement TSPS (time stamping service; OID: 1.3.6.1.4.1.30903.1.4.2), v. 2.11 as of 08.05.2022 (publicly available).

2. TSP’s trust services in scope of the conformity assessment

State Enterprise Centre of Registers operates and provides the following trust services in the qualified TSP operation as defined in the eIDAS Regulation, Article 3

- creating qualified certificates for electronic signatures (qualified trust service - QC),

- creating qualified certificates for electronic seals (qualified trust service - QC),

- creating qualified electronic time stamps (qualified trust service - QTST),

- generating and managing signature/seal creation data on behalf of subscribes (qualified trust service – RemoteQSCDManagement/Q), and

- generating qualified electronic signatures/seals based on signature/seal creation data managed by TSP on behalf of subscribers (qualified trust service – RemoteQSCDManagement/Q).

  The remote signing/sealing service for TSP’s subscribers corresponds with the particular trust service type for remote signing/sealing:
  “A qualified service for remote QSCD (qualified electronic signature/seal creation device) management which supports generation and management of signature creation data within QSCD(s) on behalf and under control of remote signers or seal creators”,
  URI: http://uri.etsi.org/TrstSvc/Svctype/RemoteQSCDManagement/Q as defined by ETSI TS 119 612 v2.2.1, sec. 5.5.1.1.

State Enterprise Centre of Registers operates and provides the following relevant additional services:

- Registration (application submission, application verification, subscriber identification).
- Subscriber's key pair generation (for electronic signatures and seals it takes place on the respective local subscriber qSCDs[3] and/or on the qSCD for remote signing/sealing operated by qTSP on behalf of subscribers).
- Subscriber's public key certification (certificate production) for qualified electronic signatures and qualified electronic seals.
- Personalisation of the respective subscriber's qualified secure signature creation devices (qSCD), i.e., linking the key pair for electronic signature/seal to the subscriber. It includes writing key pair and certificate into qSCD (electronic personalisation).
  Please note that the TSP issues the locally used qSCD of the following types:
  a) qSCD (flash memory, smart card or other) used when connected to the computer workplace;
  b) SIM qSCD used along with the mobile phone.
  The TSP can also issue qualified certificates for qSCDs operated by subscriber in subscriber's operational environment under subscriber's responsibility (i.e. for qSCDs not issued by TSP itself). In this case, TSP verifies and ascertains the qSCD-property of the subscriber's device, before placing the qcSSCD statement in the relevant certificate extension.
- Certificate issuance.
- Delivery of the locally used qSCD to subscriber.
- Certificate suspension and revocation service.
- Providing online certificate status information via OCSP (RFC 2560 on the request – response basis).
- Providing certificate status information by certificate revocation lists (CRLs).
- Operation of a web portal providing information about these services (www.elektroninis.lt), including the TSP's policies, subscriber information, the legal basis, service certificates and CRLs and other related information.
- Technical support hotline for customers/subscribers.

[3] Qualified signature creation devices

Following qualified trust services are covered by the current conformity assessment:

Description of the trust service	'qualified trust service type' according to ETSI TS 119 612 V2.1.1, sec. 5.5.1
creating qualified certificates for electronic signatures	URI: http://uri.etsi.org/TrstSvc/Svctype/CA/QC URI: http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL/QC URI: http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC
creating qualified certificates for electronic seals	URI: http://uri.etsi.org/TrstSvc/Svctype/CA/QC URI: http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL/QC URI: http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC
creating qualified electronic timestamp	URI: http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

Description of the trust service	'qualified trust service type' according to ETSI TS 119 612 V2.2.1, sec. 5.5.1 ETSI TS 119 612 V2.2.1 is NOT covered by the IMPLEMENTING DECISION (EU) 2015/1505 (Trusted Lists)
qualified remote qSCD management supports generation and management of signature creation data within qSCD(s) on behalf and under control of remote signers	URI: http://uri.etsi.org/TrstSvc/Svctype/RemoteQSCDManagement/Q

Description of the trust service	‘qualified trust service type’ according to ETSI TS 119 612 V2.2.1, sec. 5.5.1 ETSI TS 119 612 V2.2.1 is NOT covered by the IMPLEMENTING DECISION (EU) 2015/1505 (Trusted Lists)
or seal creators	

Each qualified trust service covered by the current conformity assessment is identified by the service certificate information, which is unambiguously assignable to each single trust service.

This service certificate information is summarised below, whereby certificates tagged as ‘*for verification only*’ or ‘*expired*’, if any, shall be kept on trusted lists for enabling a long period verification[4].

qTSP simultaneously operates two separate PKI branches: ‘RCSC IssuingCA’ (RCSC ICA) and ‘RCSC IssuingCA-2’ (RCSC ICA-2).

Service type identifier according to ETSI TS 119 612 V2.1.1, sec. 5.5.1:	URI: http://uri.etsi.org/TrstSvc/Svctype/CA/QC
Service name:	RCSC qualified signatures and seals certificate issuing authority
Root certificate (root CA) /C=LT/O=VI Registru centras- i.k. 124110246/	
certificate common name (CN)	**Serial number (SN)** **Fingerprint**
CN=RCSC RootCA	HEX: 4F001BA124BDCB8848BEBD3F2B62C7C5 DEC: 105009572059172725838931195944411252677 SHA1: FDE7C6FDB32BB8E63939840D6AE052C3D8B73B87
Trust service certificates (RCSC Issuing CA / RCSC Issuing CA-2) /C=LT/O=VI Registru centras- i.k. 124110246/	

[4] It shall be noted that all service certificates for the 'qualified trust service type' http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST according to ETSI TS 119 612 V2.1.1 (sec. 5.5.1), which are marked as '*expired*', are no longer service indicating.

certificate common name (CN)	**Serial number (SN)**
CN=RCSC IssuingCA TSL-registered	HEX: 5773F88261267CEB000000000002 DEC: 1773757784108407495586941652434946
CN=RCSC IssuingCA-2 TSL-registered	HEX: 2554746F8A1D3379000000000006 DEC: 757140356090440502505633189199878

Table 1: PKI certificates for the trust service /CA/QC – ICA and ICA-2

Service type identifier according to ETSI TS 119 612 V2.1.1, sec. 5.5.1:	URI: http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL/QC
Service name:	RCSC certificate validity status information services (CRL)
Root certificate (root CA) /C=LT/O=VI Registru centras- i.k. 124110246/	
certificate common name (CN)	**Serial number (SN)** **Fingerprint**
CN=RCSC RootCA,	HEX: 4F001BA124BDCB8848BEBD3F2B62C7C5 DEC: 105009572059172725838931195944411252677 SHA1: FDE7C6FDB32BB8E63939840D6AE052C3D8B73B87
Trust service certificates (RCSC Issuing CA / RCSC Issuing CA-2) /C=LT/O=VI Registru centras- i.k. 124110246/	
certificate common name (CN)	**Serial number (SN)**
CN=RCSC IssuingCA TSL-registered	HEX: 5773F88261267CEB000000000002 DEC: 1773757784108407495586941652434946
CN=RCSC IssuingCA-2 TSL-registered	HEX: 2554746F8A1D3379000000000006 DEC: 757140356090440502505633189199878

Table 2: PKI certificates for the trust service /Certstatus/CRL/QC – ICA and ICA-2

Service type identifier according to ETSI TS 119 612 V2.1.1, sec. 5.5.1:	URI: http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC
Service name:	RCSC certificate validity status information services (OCSP)
Root certificate (RCSC RootCA) /C=LT/O=VI Registru centras- i.k. 124110246/	
certificate common name (CN)	**Serial number (SN)** **Fingerprint**
CN=RCSC RootCA	HEX: 4F001BA124BDCB8848BEBD3F2B62C7C5 DEC: 105009572059172725838931195944411252677 SHA1: FDE7C6FDB32BB8E63939840D6AE052C3D8B73B87
Trust service certificates (RCSC RootCA OCSP) /C=LT/O=VI Registru centras- i.k. 124110246/	
certificate common name (CN)	**Serial number (SN)**
CN=RCSC RootCA OCSP	HEX: 2554746f8a1d337900000000000007 DEC: 757140356090440502505633189199879

Table 3: PKI certificates for the trust service /Certstatus/OCSP/QC - RootCA OCSP

Root certificate (RCSC RootCA) /C=LT/O=VI Registru centras- i.k. 124110246/	
certificate common name (CN)	**Serial number (SN)** **Fingerprint**
CN=RCSC RootCA	HEX: 4F001BA124BDCB8848BEBD3F2B62C7C5 DEC: 105009572059172725838931195944411252677 SHA1: FDE7C6FDB32BB8E63939840D6AE052C3D8B73B87
Trust service certificates (RCSC Issuing CA) /C=LT/O=VI Registru centras- i.k. 124110246/	

certificate common name (CN)	**Serial number (SN)**
CN = RCSC IssuingCA TSL-registered	HEX: 5773F88261267CEB000000000002 DEC: 1773757784108407495586941652434946
Trust service certificates (RCSC IssuingCA OCSP) /C=LT/O=VI Registru centras- i.k. 124110246/	
certificate common name (CN)	**Serial number (SN)**
CN = RCSC IssuingCA OCSP TSL-registered	HEX: 70944e6fb3a36b2e0000000505c6 DEC: 2283379918530948394413227711464902

Table 4: PKI certificates for the trust service /Certstatus/OCSP/QC – ICA OCSP

Root certificate (RCSC RootCA) /C=LT/O=VI Registru centras- i.k. 124110246/	
certificate common name (CN)	**Serial number (SN)** **Fingerprint**
CN=RCSC RootCA	HEX: 4F001BA124BDCB8848BEBD3F2B62C7C5 DEC: 105009572059172725838931195944411252677 SHA1: FDE7C6FDB32BB8E63939840D6AE052C3D8B73B87
Trust service certificates (RCSC Issuing CA-2) /C=LT/O=VI Registru centras- i.k. 124110246/	
certificate common name (CN)	**Serial number (SN)**
CN = RCSC IssuingCA-2 TSL-registered	HEX: 2554746F8A1D3379000000000006 DEC: 7571403560904405025056331891998781
Trust service certificates (RCSC IssuingCA-2 OCSP) /C=LT/O=VI Registru centras- i.k. 124110246/	
certificate common name (CN)	**Serial number (SN)**

CN = RCSC IssuingCA-2 OCSP	HEX: 267FB3B30F9538B2000000000004 DEC: 780849155866142926208139018633220

Table 5: PKI certificates for the trust service /Certstatus/OCSP/QC – ICA-2 OCSP

Service type identifier nach ETSI TS 119 612 V2.1.1, Abs.5.5.1:	URI: http://uri.etsi.org/TrstSvc/Svctype/CA/QTST
Service name:	RCSC Time stamping authority
Root certificate (root CA) /C=LT/O=VI Registru centras- i.k. 124110246/	
certificate name (CN)	**Serial number (SN)** **Fingerprint**
CN=RCSC RootCA	HEX: 4F001BA124BDCB8848BEBD3F2B62C7C5 DEC: 105009572059172725838931195944411252677 SHA1: FDE7C6FDB32BB8E63939840D6AE052C3D8B73B87
Trust service certificates (RCSC Issuing CA) /C=LT/O=VI Registru centras- i.k. 124110246/	
certificate common name (CN)	**Serial number (SN)**
CN = RCSC IssuingCA TSL-registered	HEX: 5773F88261267CEB000000000002 DEC: 1773757784108407495586941652434946
Trust service certificate(s) (RCSC TSA) /C=LT/O=VI Registru centras- i.k. 124110246/	
certificate name (CN)	**Serial number (SN)**
CN=RCSC TSA TSL-registered	**FOR VERIFICATION ONLY** HEX: 70944E6FB3A36B2E000000000019
CN=RCSC TSA2 TSL-registered	HEX: 70944e6fb3a36b2e00000002e96c DEC: 2283379918530948394413227711326572

Table 6: PKI certificates for the trust service /TSA/QTST – TSA and TSA2

Service type identifier nach ETSI TS 119 612 V2.1.1, Abs.5.5.1:	URI: http://uri.etsi.org/TrstSvc/Svctype/CA/QTST
Service name:	RCSC Time stamping authority
Root certificate (root CA) /C=LT/O=VI Registru centras- i.k. 124110246/	
certificate name (CN)	**Serial number (SN)** **Fingerprint**
CN=RCSC RootCA	HEX: 4F001BA124BDCB8848BEBD3F2B62C7C5 DEC: 105009572059172725838931195944411252677 SHA1: FDE7C6FDB32BB8E63939840D6AE052C3D8B73B87
Trust service certificates (RCSC Issuing CA-2) /C=LT/O=VI Registru centras- i.k. 124110246/	
certificate common name (CN)	**Serial number (SN)**
CN = RCSC IssuingCA-2 TSL-registered	HEX: 2554746F8A1D3379000000000000006 DEC: 75714035609044050250563318919987 8
Trust service certificate(s) (RCSC TSA) /C=LT/O=VI Registru centras- i.k. 124110246/	
certificate name (CN)	**Serial number (SN)**
CN=RCSC TSA3 TSL-registered	HEX: 267FB3B30F9538B2000000000000008 DEC: 78084915586614292620813901863322 4

Table 7: PKI certificates for the trust service /TSA/QTST – TSA3

For the remote signing service, no particular, dedicated trust service certificate was generated by the TSP. The remote signing service can currently be used for the generation of qualified electronic signatures and seals. For issuing the related qualified subscribers' certificates, only the ICA (i.e. not the ICA-2) is used. Thus, the trust service certificate as stated in Table 1: PKI certificates for the trust service

/CA/QC – ICA and ICA-2 (only ICA certificates) above is also used for the provision of the remote signing service.

Please note that the IMPLEMENTING DECISION (EU) 2015/1505, Chapter II refers to ETSI TS 119 612 v2.1.1 (Trusted Lists). This version v2.1.1 lists in sec. 5.5.1.1 “Regulation (EU) No 910/2014 qualified trust service types” all the qualified trust service types admissible for including in the national trusted lists acc. to Art. 22 of eIDAS.
The admissible qualified trust service types listed in sec. 5.5.1.1 of ETSI TS 119 612 v2.1.1 do NOT comprise any qualified service for remote signing.
Hence, the responsible Supervisory Body might be currently not able to include particular trust service certificates dedicated to the remote signing service.
Please also note that the newer version of this technical standard ETSI TS 119 612 v2.2.1
http://uri.etsi.org/TrstSvc/Svctype/RemoteQSCDManagement/Q
does include a particular trust service type for remote signing, namely
URI:, see sec. 5.5.1.1 there.

In implementing the following services, State Enterprise Centre of Registers draws on the services of delegated third parties:

- Identification of subscribers and physical delivery of locally used qSCDs to subscribers (by contracted registration authorities; only face-to-face physical presence identification procedure).

A detailed information about the identification procedures and other customer related questions can be directly requested from the TSP.

3. Certification Programme

The current conformity assessment procedure has been performed in accordance with the Certification Program 031 ‘eIDAS TSP’ (accredited area) of the Certification Body of Deutsche Telekom Security GmbH (certification program 031)’.

The Certification Body of Telekom Security is a conformity assessment body as provided by Article 3 paragraph 18 of eIDAS. The Certification Body of T-Systems is accredited by the German Accreditation Authority (DAkkS; http://www.dakks.de/en, member of EA) for performing conformity assessment (audit) according to eIDAS requirements and according to ETSI EN 319 4xx / 5xx; accreditation ID: D-ZE-21631-01-00 (former D-ZE-12025-01-00).

4. Assessment of the TSP’s qualified operation

- The Certification Practice Statement for REMOTE ELECTRONIC SIGNATURE AND ELECTRONIC SEAL CPS_RS (remote signing/sealing; OID: 1.3.6.1.4.1.30903.1.6.1), v. 1.1 as of 31.03.2023,
- the Certification Practice Statement CPS_QC (non-remote services; OID: 1.3.6.1.4.1.30903.1.2.6), v. 6.8 as of 08.05.2022, and
- the Time-Stamping Practice Statement TSPS (time stamping service; OID: 1.3.6.1.4.1.30903.1.4.2), v. 2.11 as of 08.05.2022

of the trust service provider “State Enterprise Centre of Registers” are suitable for the operations of a qualified trust service provider as defined by eIDAS Regulation.

These Certification Practice Statements and the Time-Stamping Practice Statement of the trust service provider „State Enterprise Centre of Registers“ are implemented accordingly in practice.

The trust service provider „State Enterprise Centre of Registers“ operates the following trust services in compliance with the relevant requirements of the current version of eIDAS Regulation:

Description of the trust service	‘qualified trust service type’ according to ETSI TS 119 612 V2.1.1, sec. 5.5.1

creating qualified certificates for electronic signatures	`URI: http://uri.etsi.org/TrstSvc/Svctype/CA/QC`
	`URI: http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL/QC`
	`URI: http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC`

creating qualified certificates for electronic seals	`URI: http://uri.etsi.org/TrstSvc/Svctype/CA/QC`
	`URI: http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL/QC`
	`URI: http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC`

creating qualified electronic	`URI: http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST`

Description of the trust service	‘qualified trust service type’ according to ETSI TS 119 612 V2.1.1, sec. 5.5.1
timestamp	

Description of the trust service	‘qualified trust service type’ according to ETSI TS 119 612 V2.2.1, sec. 5.5.1 ETSI TS 119 612 V2.2.1 is NOT covered by the IMPLEMENTING DECISION (EU) 2015/1505 (Trusted Lists)

qualified remote qSCD management
supports generation and management of signature creation data within qSCD(s) on behalf and under control of remote signers or seal creators
	`URI:`
	`http://uri.etsi.org/TrstSvc/Svctype/RemoteQSCDManagement/Q`

Table 8: Trust services provided in compliance with eIDAS Regulation

5. Integrated Modules

For providing the trust services in scope, the TSP does not use any already eIDAS-confirmed services provided by a module operator as delegated third party.

6. Summary and Notes

1. The Certification Practice Statement for REMOTE ELECTRONIC SIGNATURE AND ELECTRONIC SEAL CPS_RS (remote signing/sealing; OID: 1.3.6.1.4.1.30903.1.6.1), v. 1.1 as of 31.03.2023,
   - the Certification Practice Statement CPS_QC (non-remote services; OID: 1.3.6.1.4.1.30903.1.2.6), v. 6.8 as of 08.05.2022, and
   - the Time-Stamping Practice Statement TSPS (time stamping service; OID: 1.3.6.1.4.1.30903.1.4.2), v. 2.11 as of 08.05.2022

   are suitable for the operations of a qualified trust service provider as defined by the eIDAS Regulation and are implemented accordingly in practice.

2. The trust service provider „State Enterprise Centre of Registers“ operates the trust services listed in chap. 4, Table 8 above in compliance with the relevant requirements of the current version of the eIDAS Regulation.

3. Only subscriber agreements for electronic signature and electronic seal also signed off by „State Enterprise Centre of Registers“ in the role of trust service provider are covered by the current Conformity Certificate.

4. The current conformity certificate TelekomSecurity.031.0301.06.2023 is valid for the current Certification Practice Statement up to and including 21.06.2025. This validity period (that is, the maximum possible duration of TSP operation in compliance with the eIDAS Regulation) results from the specification of the eIDAS Regulation, Article 20 (1).
   The validity of the current conformity certificate can be extended or reduced if the basics upon which it was issued allow an extension or make a reduction necessary.

End of the Conformity Certificate

Conformity Certificate:
TelekomSecurity.031.0301.06.2023

Issuer:	Deutsche Telekom Security GmbH
Address:	Bonner Talweg 100, 53113 Bonn
Phone:	+49-(0)228-181-0
Fax:	+49-(0)228-181-49990
Web:	www.telekom-zert.com https://www.telekom.de/security