



**Conformity Assessment Report:
Conformity Certificate and Summary**

**Attachment No. 1 to
TelekomSecurity.031.0286.06.2021**

**Trust Service Provider:
State Enterprise Centre of Registers**

Conformity Certificate

TelekomSecurity.031.0286.06.2021
Attachment No. 1

pursuant to Article 20 par. 1 of REGULATION (EU) No. 910/2014¹

valid from 22.06.2021 and up to and including: 21.06.2023

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**

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

This certificate is filed and registered under **TelekomSecurity.031.0286.U.11.2021**

Bonn, 23.11.2021

i.V. Dr. Igor Furgel
Head of 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).



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

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

Lvovo str. 25-101
09320 Vilnius

and

Vinco Kudirkos st. 18-3
03105 Vilnius
Lithuania

Tel.: +370 5 268 8202, Fax: +370 5 268 8311,
e-mail: info@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 Regulation².

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 conformity re-assessment activities as documented here (ID Attachment #1 to TelekomSecurity.031.0286.06.2021) represent a confined re-assessment serving the continuation of the status as a 'qualified trust service provider' according to Art. 24 of the eIDAS Regulation for all qualified trust services offered by the qTSP in the eIDAS context.

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

The present assessment is based on

- the Certification Practice Statement CPS (OID: 1.3.6.1.4.1.30903.1.2.6), v. 6.6 as of 08.11.2021 (publicly available) and
- Time-Stamping Practice Statement TSPS (OID: 1.3.6.1.4.1.30903.1.4.2), v. 2.10 as of 08.11.2021 (publicly available).

and covers the following externally visible modifications of the Service Provision Practice Statement:

- 1) An additional PKI branch RCSC ICA-2 was established and commissioned.

2. Reason for the Amendment

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).

A description of qualified trust services provided by the qTSP is given in the reference certificate TelekomSecurity.031.0286.06.2021 as of 08.06.2021 and in all previous Attachments, if any, as listed in sec. 1.2 above and shall be regarded to.

The following changes in the TSP operation have occurred in the meantime and are the reason for this 1nd attachment to the certificate TelekomSecurity.031.0286.06.2021:

- establishing and commissioning an additional PKI branch RCSC ICA-2 was, see the listing below for the PKI branch RCSC ICA-2;
- changes in internal qTSP infrastructure, which are fully transparent for qTSP subscribers and relying parties.

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 |

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 verification³.

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

³ 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.

| | |
|---|---|
| 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, hex/dec) SHA1 Fingerprint |
| CN=RCSC RootCA | 4F001BA124BDCB8848BEBD3F2B62C7C5 (hex) 105009572059172725838931195944411252677 (dec) 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, hex/dec) |
| CN=RCSC IssuingCA | 5773F88261267CEB000000000002 (hex) 1773757784108407495586941652434946 (dec) |
| CN=RCSC IssuingCA-2 | 2554746F8A1D3379000000000006 (hex) 757140356090440502505633189199878 (dec) |

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/Certs/tatus/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, hex/dec) |

| | SHA1 Fingerprint |
|---|---|
| CN=RCSC RootCA | 4F001BA124BDCB8848BEBD3F2B62C7C5 (hex) 105009572059172725838931195944411252677 (dec) 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, hex/dec) |
| CN=RCSC IssuingCA | 5773F88261267CEB000000000002 (hex) 1773757784108407495586941652434946 (dec) |
| CN=RCSC IssuingCA-2 | 2554746F8A1D3379000000000006 (hex) 757140356090440502505633189199878 (dec) |

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, hex/dec) SHA1 Fingerprint |
| CN=RCSC RootCA | 4F001BA124BDCB8848BEBD3F2B62C7C5 (hex) 105009572059172725838931195944411252677 (dec) FDE7C6FDB32BB8E63939840D6AE052C3D8B73B87 |
| Trust service certificates (RCSC RootCA OCSP) /C=LT/O=VI Registru centras- i.k. 124110246/ | |
| certificate common name (CN) | Serial number (SN, hex/dec) |
| CN=RCSC RootCA OCSP | 2554746F8A1D3379000000000003 (HEX) |

| | |
|--|---|
| | 757140356090440502505633189199875 (DEC) |
|--|---|

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, hex/dec) SHA1 Fingerprint |
| CN=RCSC RootCA | 4F001BA124BDCB8848BEBD3F2B62C7C5 (hex) 105009572059172725838931195944411252677 (dec) FDE7C6FDB32BB8E63939840D6AE052C3D8B73B87 |
| Trust service certificates (RCSC Issuing CA) /C=LT/O=VI Registru centras- i.k. 124110246/ | |
| certificate common name (CN) | Serial number (SN, hex/dec) |
| CN = RCSC IssuingCA | 5773F88261267CEB000000000002 (hex) 1773757784108407495586941652434946 (dec) |
| Trust service certificates (RCSC IssuingCA OCSP) /C=LT/O=VI Registru centras- i.k. 124110246/ | |
| certificate common name (CN) | Serial number (SN, hex/dec) |
| CN = RCSC IssuingCA OCSP | EXPIRED 70944E6FB3A36B2E000000000008 (HEX) |
| CN = RCSC IssuingCA OCSP | 70944E6FB3A36B2E000000002C351 (HEX) 2283379918530948394413227711316817 (DEC) |

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, hex/dec) |
| | |

| SHA1 Fingerprint | |
|---|---|
| CN=RCSC RootCA | 4F001BA124BDCB8848BEBD3F2B62C7C5 (hex) 105009572059172725838931195944411252677 (dec) FDE7C6FDB32BB8E63939840D6AE052C3D8B73B87 |
| Trust service certificates (RCSC Issuing CA-2) /C=LT/O=VI Registru centras- i.k. 124110246/ | |
| certificate common name (CN) | Serial number (SN, hex/dec) |
| CN = RCSC IssuingCA-2 | 2554746F8A1D3379000000000006 (hex) 757140356090440502505633189199878 (dec) |
| Trust service certificates (RCSC IssuingCA-2 OCSP) /C=LT/O=VI Registru centras- i.k. 124110246/ | |
| certificate common name (CN) | Serial number (SN, hex/dec) |
| CN = RCSC IssuingCA-2 OCSP | 267FB3B30F9538B2000000000004 (HEX) 780849155866142926208139018633220 (DEC) |

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, hex/dec) SHA1 Fingerprint |
| CN=RCSC RootCA | 4F001BA124BDCB8848BEBD3F2B62C7C5 (hex) 105009572059172725838931195944411252677 (dec) FDE7C6FDB32BB8E63939840D6AE052C3D8B73B87 |
| Trust service certificates (RCSC Issuing CA) /C=LT/O=VI Registru centras- i.k. 124110246/ | |

| certificate common name (CN) | Serial number (SN, hex/dec) |
|--|---|
| CN = RCSC IssuingCA | 5773F88261267CEB0000000000002 (hex) 1773757784108407495586941652434946 (dec) |
| Trust service certificate(s) (RCSC TSA) /C=LT/O=VI Registru centras- i.k. 124110246/ | |
| certificate name (CN) | Serial number (SN, hex/dec) |
| CN=RCSC TSA | FOR VERIFICATION ONLY 70944E6FB3A36B2E0000000000019 (hex) |
| CN=RCSC TSA2 | 70944e6fb3a36b2e00000002e96c (hex) 2283379918530948394413227711326572 (dec) |

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, hex/dec) SHA1 Fingerprint |
| CN=RCSC RootCA | 4F001BA124BDCB8848BEBD3F2B62C7C5 (hex) 105009572059172725838931195944411252677 (dec) FDE7C6FDB32BB8E63939840D6AE052C3D8B73B87 |
| Trust service certificates (RCSC Issuing CA-2) /C=LT/O=VI Registru centras- i.k. 124110246/ | |
| certificate common name (CN) | Serial number (SN, hex/dec) |
| CN = RCSC IssuingCA-2 | 2554746F8A1D337900000000000006 (hex) 757140356090440502505633189199878 (dec) |

| Trust service certificate(s) (RCSC TSA) | |
|--|--|
| /C=LT/O=VI Registru centras- i.k. 124110246/ | |
| certificate name (CN) | Serial number (SN, hex/dec) |
| CN=RCSC TSA3 | 267FB3B30F9538B20000000000008 (hex) 780849155866142926208139018633224 (dec) |

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

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 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 Telekom Security 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 current changes with regard to the TSP's qualified operation

The current Certification Practice Statement (version CPS (OID: 1.3.6.1.4.1.30903.1.2.6), v. 6.6 as of 08.11.2021) and Time-Stamping Practice Statement TSPS (OID: 1.3.6.1.4.1.30903.1.4.2), v. 2.10 as of 08.11.2021 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.

The Certification Practice Statement and 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 timestamp | URI: http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST |

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 current Certification Practice Statement of the trust service provider “State Enterprise Centre of Registers” (version CPS (OID: 1.3.6.1.4.1.30903.1.2.6), v. 6.6 as of 08.11.2021) and Time-Stamping Practice Statement TSPS (OID: 1.3.6.1.4.1.30903.1.4.2), v. 2.10 as of 08.11.2021 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.031.0286.11.2021 is valid for the current Certification Practice Statement up to and including 21.06.2023. 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 Attachment No. 1 to Conformity Certificate

Conformity Certificate:
TelekomSecurity.031.0286.U.11.2021

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>