



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

TelekomSecurity.031.0288.06.2021 (Attachment No. 3)

Trust Service Provider:

**Centrum Certyfikacji Kluczy CenCert, Enigma
Systemy Ochrony Informacji Sp z o.o.**

Conformity Certificate

TelekomSecurity.031.0288.06.2021
Attachment No. 3

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

valid from 18.06.2021 up to and including: 17.06.2023

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
„Centrum Certyfikacji Kluczy CenCert, Enigma Systemy
Ochrony Informacji Sp z o.o.“

provides the following trust services:

- **creating qualified certificates for electronic signatures**
- **creating qualified certificates for electronic seals**
- **creating qualified certificates for website authentication**
- **creating qualified electronic timestamps**

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

This certificate is filed and registered under: **TelekomSecurity.031.0288.U.03.2022**

Bonn, 29.03.2022

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



Deutsche Telekom Security GmbH – Certification Body – is an accredited Conformity Assessment Body (CAB) pursuant to REGULATION (EU) No. 910/2014. DAkkS Registration No. D-ZE-21631-01 (previously Certification Body of T-Systems International GmbH, previous DAkkS 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

Centrum Certyfikacji Kluczy CenCert, Enigma Systemy Ochrony Informacji Sp z o.o.

Biuro Obsługi Klienta [Customer Service Point]

ul. Jagiellonska 78
03 - 301 Warszawa
Poland

with the annotation reading “usługi zaufania” [trust services]

tel. 666 028 044
e-mail: biuro@cencert.pl

1.2 Current confirmation status

Centrum Certyfikacji Kluczy CenCert, Enigma Systemy Ochrony Informacji Sp z o.o. is a qualified trust service provider (qTSP) according to Art. 24 of the eIDAS Regulation².

The last full conformity assessment was accomplished with issuing the conformity certificate TelekomSecurity.031.0288.06.2021 as of 18.06.2021.

The current Attachment No. 1 to conformity certificate TelekomSecurity.031.0288.06.2021 serves 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.

Current assessment is based on the TSP Certification Policy version 1.31 as of 17.09.2021. This document is available from the TSP on request.

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

1.3 Reason for the amendment

The amendment covers newly introduced support for the following user hosted HSM based QSCDs³

- nShield Solo XC Hardware Security Module v12.50.7,
- nShield Solo XC Hardware Security Module v12.60.15,
- Thales Luna K7 Cryptographic Module.

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

Centrum Certyfikacji Kluczy CenCert, Enigma Systemy Ochrony Informacji Sp z o.o. 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 – CA/QC),
- creating qualified certificates for electronic seals (qualified trust service – CA/QC),
- creating qualified certificates for website authentication (qualified trust service – CA/QC)
- creating qualified electronic timestamp (qualified trust service – TSA/QTST).

Centrum Certyfikacji Kluczy CenCert, Enigma Systemy Ochrony Informacji Sp z o.o. operates and provides the following relevant additional services:

- Registration (application submission, subscriber identification, application verification)
- Subscriber's key pair generation (for electronic signatures and seals it takes place on the respective subscriber qSCDs³, for remote signature and seal services it takes place on the HSM qSCD device hosted by TSP).
- Subscriber's public key certification (certificate production) for qualified electronic signatures and seals, website authentication, advanced seals

³ Qualified signature creation device

- Personalization of the respective subscriber's qualified secure signature/seal creation devices (qSCD) (i.e. linking the key pair for electronic signature to subscriber (electronic personalisation))
- Certificate issuance / delivery of qSCD to subscriber
- Certificate suspension and revocation service
- Providing online certificate status information via OCSP operated in compliance with RFC 6960
- Providing certificate status information by certificate revocation lists (CRLs)
- Operation of a server providing two factor secured access (i.e. remote signature and seal on behalf of the authorised user) to signature keys stored in the HSM qSCD device hosted by TSP
- Operation of a web portal providing information about these services (www.cencert.pl/), including the TSP's Certification Policy, online forms for applications, subscriber information, legal basis, service certificates and CRLs and other related information
- Technical support hotline for customers.

The 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 |

| | |
|--|--|
| 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 website authentication | 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:

A) PKI with root /C=PL /O= Minister wlasciwy do spraw gospodarki

| | |
|--|--|
| 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: | CenCert QTSP CA |
| Root certificate (root CA) /C=PL /O=Minister wlasciwy do spraw gospodarki | |
| certificate common name (CN) | Serial number (SN, hex) SHA1 Fingerprint |
| /CN= Narodowe Centrum Certyfikacji (NCCert)/ | 62 a7 0d 04 c3 24 b8 d4 27 56 cc 3f 81 6b f2 eb 32 ef 07 19 a9 51 6f a8 11 53 5e 73 45 88 15 71 06 6c 77 0c f9 7f 66 95 |
| Trust service certificates /SERIALNUMBER = Nr wpisu: 11 /C = PL /O = Enigma SOI sp. z o.o. | |

| certificate common name (CN) | Serial number (SN, hex) |
|---|--|
| /CN = CenCert Centrum Certyfikatów Kwalifikowanych | 0f ee 28 6c ea 99 52 91 2b 66 49 d0 66 dc 2c 05 33 bb de 05 |

Table 1: PKI certificates for the trust service /CA/QC

| 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: | CenCert QTSP CA |
| Root certificate (root CA) /C=PL/O=Minister wlasciwy do spraw gospodarki | |
| certificate common name (CN) | Serial number (SN, hex) SHA1 Fingerprint |
| /CN= Narodowe Centrum Certyfikacji (NCCert) | 62 a7 0d 04 c3 24 b8 d4 27 56 cc 3f 81 6b f2 eb 32 ef 07 19 a9 51 6f a8 11 53 5e 73 45 88 15 71 06 6c 77 0c f9 7f 66 95 |
| Trust service certificates /SERIALNUMBER = Nr wpisu: 11/ C = PL/O = Enigma SOI sp. z o.o. | |
| certificate common name (CN) | Serial number (SN, hex) |
| /CN = CenCert Centrum Certyfikatów Kwalifikowanych | 0f ee 28 6c ea 99 52 91 2b 66 49 d0 66 dc 2c 05 33 bb de 05 |

Table 2: PKI certificates for the trust service /Certstatus/CRL/QC

B) PKI with root /C=PL/O= Narodowy Bank Polski

| | |
|---|--|
| 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: | CenCert QTSP CA |
| Root certificate (root CA) /C=PL/O=Narodowy Bank Polski | |
| certificate common name (CN) | Serial number (SN, hex) SHA1 Fingerprint |
| /CN= Narodowe Centrum Certyfikacji/organizationIdentifier = VATPL-5250008198 | 40 f8 f7 8a b0 e3 64 10 56 91 c8 d9 e0 2c f8 c1 c6 40 0a 46 89 ce c4 84 2f af 40 1b 48 d0 f2 1d 80 43 e9 a6 3e 7c 02 d5 |
| Trust service certificates /C=PL/O=Enigma Systemy Ochrony Informacji Sp. z o.o. | |
| certificate common name (CN) | Serial number (SN, hex) |
| /CN= CenCert QTSP CA/organizationIdentifier = VATPL-5261029614 | 16 7d 4d 14 56 bd e2 72 1e 49 05 99 47 c8 b6 42 59 b7 9f 21 |
| /CN= CenCert QTSP TSA ECC CA/organizationIdentifier = VATPL-5261029614 | 00 a6 52 52 d0 5b 39 4e |
| /CN= CenCert QTSP TSA ECC CA/organizationIdentifier = VATPL-5261029614 | 02 63 3e 0a 58 c0 8f 24 |
| /CN= CenCert QTSP WEB CA CA/organizationIdentifier = VATPL-5261029614 | 00 82 84 6c b7 d5 2f 34 |

Table 3: PKI certificates for the trust service /CA/QC

| | |
|---|--|
| 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: | CenCert QTSP CA |
| Root certificate (root CA) /C=PL/O=Narodowy Bank Polski | |
| certificate common name (CN) | Serial number (SN, hex) SHA1 Fingerprint |
| /CN= Narodowe Centrum Certyfikacji/organizationId entifier = VATPL-5250008198 | 40 f8 f7 8a b0 e3 64 10 56 91 c8 d9 e0 2c f8 c1 c6 40 0a 46 89 ce c4 84 2f af 40 1b 48 d0 f2 1d 80 43 e9 a6 3e 7c 02 d5 |
| Trust service certificates /C=PL/O=Enigma Systemy Ochrony Informacji Sp. z o.o. | |
| certificate common name (CN) | Serial number (SN, hex) |
| /CN= CenCert QTSP CA/organizationIdentifier = VATPL-5261029614 | 16 7d 4d 14 56 bd e2 72 1e 49 05 99 47 c8 b6 42 59 b7 9f 21 |
| /CN= CenCert QTSP WEB CA CA/organizationIdentifier = VATPL-5261029614 | 00 82 84 6c b7 d5 2f 34 |

Table 4: PKI certificates for the trust service /Certstatus/CRL/QC

| | |
|---|--|
| Service type identifier nach ETSI TS 119 612 V2.1.1, Abs. 5.5.1: | URI: http://uri.etsi.org/TrstSvc/Svctype/TSA/Q TST |
| Service name: | CenCert QTSP TSA |
| Root certificate (root CA) /C=PL/O=Narodowy Bank Polski | |
| certificate common name (CN) | Serial number (SN, hex) |

| | SHA1 Fingerprint |
|---|--|
| /CN= Narodowe Centrum Certyfikacji/organizationId entifier = VATPL-5250008198 | 40 f8 f7 8a b0 e3 64 10 56 91 c8 d9 e0 2c f8 c1 c6 40 0a 46 89 ce c4 84 2f af 40 1b 48 d0 f2 1d 80 43 e9 a6 3e 7c 02 d5 |
| Trust service certificates /C=PL/O=Enigma Systemy Ochrony Informacji Sp. z o.o. | |
| certificate common name (CN) | Serial number (SN, hex) |
| /CN= CenCert QTSP TSA/organizationIdentifier = VATPL-5261029614 | 0a 20 8a 59 84 1f 07 c9 2f 47 54 18 c5 63 41 26 d6 f4 15 e3 |
| /CN= CenCert QTSP TSA ECC/organizationIdentifier = VATPL-5261029614 | 4f ca 59 6f ae 9d 10 c4 87 13 a0 1a 9d d8 59 21 bf fc 0c 95 |
| /CN= CenCert QTSP TSA/organizationIdentifier = VATPL-5261029614 | 00 a6 52 52 d0 5b 39 4e |
| /CN= CenCert QTSP TSA ECC/organizationIdentifier = VATPL-5261029614 | 02 63 3e 0a 58 c0 8f 24 |

Table 5: PKI certificates for the trust service TSA/QTST

PKI certificates for the service /Certstatus/OCSP/QC are issued by the TSP using service certificates for the service /CA/QC. These /CA/QC certificates shall be published in the TSL hence the OCSP responses can be verified.

In implementing the following services, Centrum Certyfikacji Kluczy CenCert, Enigma Systemy Ochrony Informacji Sp z o.o. draws on the services of delegated third parties:

- Identification of subscribers and physical delivery of qSCDs to subscribers (by cooperating field registration authorities, face-to-face physical presence identification procedure).

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 Deutsche Telekom Security GmbH (previously of T-Systems International GmbH) 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 (previously D-ZE-12025-01-00).

4. Assessment of the current changes with regard to the TSP's qualified operation

The current Certification Policy (version 1.31 as of 17.09.2021) of the trust service provider "Centrum Certyfikacji Kluczy CenCert, Enigma Systemy Ochrony Informacji Sp z o.o." is suitable for the operations of a qualified trust service provider as defined by the eIDAS Regulation.

This Certification Policy of the trust service provider „Centrum Certyfikacji Kluczy CenCert, Enigma Systemy Ochrony Informacji Sp z o.o.“ is implemented accordingly in practice.

The trust service provider „Centrum Certyfikacji Kluczy CenCert, Enigma Systemy Ochrony Informacji Sp z o.o.“ operates the following trust services in compliance with the relevant requirements of the current version of the 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 | URI: http://uri.etsi.org/TrstSvc/Svctype/CA/QC |

| Description of the trust service | 'qualified trust service type' according to ETSI TS 119 612 V2.1.1, sec. 5.5.1 |
|--|--|
| electronic seals | URI: http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL/QC URI: http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC |
| creating qualified certificates for website authentication | 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 6: Trust services provided in compliance with eIDAS Regulation

5. Integrated Qualified 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 Attachment No. 3 to Conformity Certificate TelekomSecurity.031.0288.06.2021 amends this Certificate.
2. The current Certification Policy (version 1.31 as of 17.09.2021) of the trust service provider "Centrum Certyfikacji Kluczy CenCert, Enigma Systemy Ochrony Informacji Sp z o.o." is suitable for the operations of a qualified trust service provider as defined by the eIDAS Regulation and is implemented accordingly in practice.
3. The trust service provider „Centrum Certyfikacji Kluczy CenCert, Enigma Systemy Ochrony Informacji Sp z o.o.“ operates the trust services listed in chap. 4, Table 6 above in compliance with the relevant requirements of the current version of the eIDAS Regulation.
4. All stipulations stated in Conformity Certificate TelekomSecurity.031.0288.06.2021 as of 18.06.2021 and in all related previous Attachments remain in force, unless they have been meanwhile explicitly repealed by current or previous Attachments.

End of the Attachment #3 to Conformity Certificate

Conformity Certificate:
TelekomSecurity.031.0288.06.2021 (Attachment No. 3)

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