Conformity Assessment Report: Conformity Certificate and Summary

TelekomSecurity.031.0331.02.2026

Trust Service Provider:

Banqup SA

Conformity Certificate

TelekomSecurity.031.0331.02.2026

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

valid from 26.02.2026 up to and including: 25.02.2028

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
„Banqup SA“

provides the following trust services:

- **issuance qualified certificates for electronic signatures**
- **issuance qualified certificates for electronic seals**
- **remote QSCD management for qualified el. signatures**
- **remote QSCD management for qualified el. seals**

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

This certificate is filed and registered under: **TelekomSecurity.031.0331.02.2026**

Bonn, 26.02.2026

Dokument unterschrieben
von: Dr. Furgel, Igor
am: 26.02.2026 16:06
Ort: Bonn

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).

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 amended by the REGULATION (EU) 2024/1183 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework

1. Object of the Conformity Assessment

1.1 Name of the Trust Service Provider

Banqup SA (also abbreviated as **BQCA**)

Company name:	Banqup SA
Enterprise number:	BE0649.860.804
Registered place of business:	Avenue Reine Astrid 92A, 1310 La Hulpe Belgium
Operational office:	Business Park Gate 7, Prins Boudewijnlaan 7, 2550 Kontich, Belgium
e-mail:	qtsp@banqup.com
Tel:	+32 2 634 06 28
URL:	www.banqup.com

1.2 Current Confirmation Status

Banqup SA (abbreviated as BQCA) strives to attain the status 'qualified trust service provider' (qTSP) according to Art. 24 of the eIDAS Regulation[2].

The present conformity assessment of the TSP according to Article 20(1) of the eIDAS Regulation serves the attainment of its status as a 'qualified trust service provider' according to Article 24 of the eIDAS Regulation for all qualified trust services offered by the TSP.

The present assessment is based on

- the Service Provision Practice Statement (SPPS) "CP/CPS Certificate Policy and Certification Practice Statement, v. 1.1.1" as of 05.02.2026 (publicly available). This document is publicly available under https://www.pki.banqup.com/repository/, subsection 'Documents'.

[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 amended by the REGULATION (EU) 2024/1183 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework

2. TSP's Trust Services in Scope of the Conformity Assessment

Banqup SA operates and provides the following trust services in the qualified TSP operation as defined in eIDAS Regulation, Article 3

- issuing qualified certificates for electronic signatures (qualified trust service – CA/QC),
- issuing qualified certificates for electronic seals (qualified trust service - CA/QC),

The TSP also provides qualified remote (server) signing and sealing services for TSP's subscribers for generation qualified electronic signatures and qualified electronic seals, i.e.,

- generating and managing signature and seal creation data on behalf of the subscribes,
- generating qualified electronic signatures based on signature creation data managed by TSP on behalf of subscribers (qualified trust service – RemoteQSigCDManagement/Q),
- generating qualified electronic seals based on seal creation data managed by TSP on behalf of subscribers (qualified trust service – RemoteQSealCDManagement/Q).

The remote signing/sealing service for TSP's subscribers corresponds with the particular trust service types:
URI: http://uri.etsi.org/TrstSvc/Svctype/RemoteQSigCDManagement/Q for remote signing
and URI: http://uri.etsi.org/TrstSvc/Svctype/RemoteQSealCDManagement/Q for remote sealing, see sec. 5.5.1.1 in ETSI TS 119 612 v2.4.1[3].

Signature/seal creation data generated and managed by the TSP on behalf of the subscribes can be used by TSP's subscribers within the remote signing service provided by the TSP to its subscribers.

The certificate policies used for qualified end-user certificates are identified by their CertificatePolicies attributes, which use the following ETSI object identifier values:

- **QCP-n-qscd**: certificate policy for EU qualified certificates issued to natural persons with private key related to the certified public key in a QSCD; itu-

[3] As referred to in COMMISSION IMPLEMENTING DECISION (EU) 2025/2164 of 27 October 2025 amending Implementing Decision (EU) 2015/1505 as regards the version of the standard on which the common template for the trusted lists is based.

t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural-qscd (2)

- **QCP-l-qscd:** certificate policy for EU qualified certificates issued to legal persons with private key related to the certified public key in a QSCD; itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-legal-qscd (3)

The applicable OID 1.3.6.1.5.5.7.1.3 is inserted by reference within each end-user certificate ruled by SPPS.

Banqup SA operates and provides the following relevant additional services:

- Registration (request submission, request verification, subscriber identification),
- Subscriber's key pair generation on behalf of subscriber for qualified electronic signatures and qualified electronic seals,
- Subscriber's public key certification (certificate production) for qualified electronic signatures and qualified electronic seals,

  The certificate extension qcStatement – qcSCD (= 0.4.0.1862.1.4; information about storage of subscriber's keys in the qualified signature/seal creation device), is always placed by the TSP in a qualified certificate,
- Certificate revocation service,
- Providing online certificate status information via OCSP (RFC6960 on the request – response basis),
- Providing certificate status information by certificate revocation lists (CRLs),
- Providing a remote access for subscribers for the execution of transactions (generation of remote signatures and remote seals),
- Operation of a dedicated mobile application Banqup One acting as the front end for subscribers' enrolment and usage of the services. Banqup One also provides online application form and subscriber information about the services.
- Operation of a web portal providing information about these services (https://www.banqup.com/, https://www.pki.banqup.com/repository/), including the TSP's Practice Statement, legal basis (see footer 'Legal' on the website), service certificates (https://www.pki.banqup.com/repository/) and other related information,
- Technical support for customers/subscribers via the functional mailbox qtsp@banqup.com.

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 V2.4.1, 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/OCSP/QC URI: http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL/QC
creating qualified certificates for electronic seals	URI: http://uri.etsi.org/TrstSvc/Svctype/CA/QC URI: http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC URI: http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL/QC

Description of the trust service	‘qualified trust service type’ according to ETSI TS 119 612 V2.4.1, sec. 5.5.1
qualified remote qSCD management The management of remote qualified electronic signature creation devices as a qualified trust service carried out by a qualified trust service provider on behalf and under control of remote signers	URI: http://uri.etsi.org/TrstSvc/Svctype/RemoteQSigCDManagement/Q
qualified remote qSCD management The management of remote qualified electronic seal creation devices as a qualified trust service	URI: http://uri.etsi.org/TrstSvc/Svctype/RemoteQSealCDManagement/Q

Description of the trust service	'qualified trust service type' according to ETSI TS 119 612 V2.4.1, sec. 5.5.1
carried out by a qualified trust service provider on behalf and under control of remote seal creators	

Each qualified trust service covered by the present 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.

The TSP simultaneously operates two separate PKI branches: 'Banqup qualified Issuing CA RSA G1-2025' and 'Banqup qualified Issuing CA ECC G2-2025'.

A) 'Banqup qualified Issuing CA RSA G1-2025'

Service type identifier according to ETSI TS 119 612 V2.4.1, sec. 5.5.1.1:	URI: http://uri.etsi.org/TrstSvc/Svctype/CA/QC
Service name:	A qualified certificate issuing trust service
Root certificate (Banqup Root CA RSA) /C=BE/O=Banqup/organizationIdentifier=NTRBE-0649860804/	
Certificate common name (CN)	**Serial number (SN)** **Fingerprint**
CN=Banqup Root CA RSA G1	HEX: 6FFF84DB2A0FA033C3C1C7074B9680845A15563F DEC: 639396238986561553691652632483863330926965904959 SHA1: FC 13 2E 39 BD 9D 69 BC E1 24 BA 40 40 A4 4E CC D0 C1 22 C5
Trust service certificate (Banqup Intermediate CA)	

/C=BE/O=Banqup/organizationIdentifier=NTRBE-0649860804/	
Certificate common name (CN)	**Serial number (SN)**
CN=Banqup Intermediate CA RSA G1-2025	HEX: 5302ADF2B9C9EB9D321DFCC456A0A0497287C42E DEC: 473905988489530340856775850085629948945850942510
Trust service certificate (Banqup Issuing CA) /C=BE/O=Banqup/organizationIdentifier=NTRBE-0649860804/	
Certificate common name (CN)	**Serial number (SN)**
CN=Banqup Issuing CA RSA G1-2025 TSL-registered	HEX: 36C56C9AE45C507A6B57FF5BE66C107B94BE81C5 DEC: 312688209262506309640404935175315313901858357701

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

Service type identifier according to ETSI TS 119 612 V2.4.1, sec. 5.5.1.1:	URI: http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL/QC
Service name:	A certificate validity status information services (CRL)
Root certificate (Banqup Root CA RSA) /C=BE/O=Banqup/organizationIdentifier=NTRBE-0649860804/	
Certificate common name (CN)	**Serial number (SN)** **Fingerprint**
CN=Banqup Root CA RSA G1	HEX: 6FFF84DB2A0FA033C3C1C7074B9680845A15563F DEC: 639396238986561553691652632483863330926965904959 SHA1: FC 13 2E 39 BD 9D 69 BC E1 24 BA 40 40 A4 4E CC D0 C1 22 C5
Trust service certificate (Banqup Intermediate CA)	

/C=BE/O=Banqup/organizationIdentifier=NTRBE-0649860804/	
Certificate common name (CN)	**Serial number (SN)**
CN=Banqup Intermediate CA RSA G1-2025	HEX: 5302ADF2B9C9EB9D321DFCC456A0A0497287C42E DEC: 473905988489530340856775850085629948945850942510
Trust service certificate (Banqup Issuing CA) /C=BE/O=Banqup/organizationIdentifier=NTRBE-0649860804/	
Certificate common name (CN)	**Serial number (SN)**
CN=Banqup Issuing CA RSA G1-2025 TSL-registered	HEX: 36C56C9AE45C507A6B57FF5BE66C107B94BE81C5 DEC: 31268820926250630964040493517531531390185835770 1

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

Service type identifier according to ETSI TS 119 612 V2.4.1, sec. 5.5.1.1:	URI: http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC
Service name:	A certificate validity status information services (OCSP)
Root certificate (Banqup Root CA RSA) /C=BE/O=Banqup/organizationIdentifier=NTRBE-0649860804/	
Certificate common name (CN)	**Serial number (SN)** **Fingerprint**
CN=Banqup Root CA RSA G1	HEX: 6FFF84DB2A0FA033C3C1C7074B9680845A15563F DEC: 639396238986561553691652632483863330926965904959 SHA1: FC 13 2E 39 BD 9D 69 BC E1 24 BA 40 40 A4 4E CC D0 C1 22 C5
Trust service certificate (Banqup Intermediate CA)	

/C=BE/O=Banqup/organizationIdentifier=NTRBE-0649860804/	
Certificate common name (CN)	**Serial number (SN)**
CN=Banqup Intermediate CA RSA G1-2025	HEX: 5302ADF2B9C9EB9D321DFCC456A0A0497287C42E DEC: 473905988489530340856775850085629948945850942510
Trust service certificate (Banqup Issuing CA) /C=BE/O=Banqup/organizationIdentifier=NTRBE-0649860804/	
Certificate common name (CN)	**Serial number (SN)**
CN=Banqup Issuing CA RSA G1-2025 TSL-registered	HEX: 36C56C9AE45C507A6B57FF5BE66C107B94BE81C5 DEC: 312688209262506309640404935175315313901858357701

Table 3: PKI certificates for the trust service /Certstatus/OCSP/QC – RSA

Service type identifier according to ETSI TS 119 612 V2.4.1, sec. 5.5.1.1:	URI: http://uri.etsi.org/TrstSvc/Svctype/RemoteQSigCDManagement/Q
Service name:	The management of remote qualified electronic signature creation devices
Root certificate (Banqup Root CA RSA) /C=BE/O=Banqup/organizationIdentifier=NTRBE-0649860804/	
Certificate common name (CN)	**Serial number (SN)** **Fingerprint**
CN=Banqup Root CA RSA G1	HEX: 6FFF84DB2A0FA033C3C1C7074B9680845A15563F DEC: 639396238986561553691652632483863330926965904959 SHA1: FC 13 2E 39 BD 9D 69 BC E1 24 BA 40 40 A4 4E CC D0 C1 22 C5
Trust service certificate (Banqup Intermediate CA) /C=BE/O=Banqup/organizationIdentifier=NTRBE-0649860804/	

Certificate common name (CN)	**Serial number (SN)**
CN=Banqup Intermediate CA RSA G1-2025	HEX: 5302ADF2B9C9EB9D321DFCC456A0A0497287C42E DEC: 473905988489530340856775850085629948945850942510
Trust service certificate (Banqup Issuing CA) /C=BE/O=Banqup/organizationIdentifier=NTRBE-0649860804/	
Certificate common name (CN)	**Serial number (SN)**
CN=Banqup Issuing CA RSA G1-2025 TSL-registered	HEX: 36C56C9AE45C507A6B57FF5BE66C107B94BE81C5 DEC: 312688209262506309640404935175315313901858357701

Table 4: PKI certificates for the trust service /RemoteQSigCDManagement/Q – RSA

Service type identifier according to ETSI TS 119 612 V2.4.1, sec. 5.5.1.1:	URI: http://uri.etsi.org/TrstSvc/Svctype/RemoteQSealCDManagement/Q
Service name:	The management of remote qualified electronic seal creation devices
Root certificate (Banqup Root CA RSA) /C=BE/O=Banqup/organizationIdentifier=NTRBE-0649860804/	
Certificate common name (CN)	**Serial number (SN)** **Fingerprint**
CN=Banqup Root CA RSA G1	HEX: 6FFF84DB2A0FA033C3C1C7074B9680845A15563F DEC: 639396238986561553691652632483863330926965904959 SHA1: FC 13 2E 39 BD 9D 69 BC E1 24 BA 40 40 A4 4E CC D0 C1 22 C5
Trust service certificate (Banqup Intermediate CA) /C=BE/O=Banqup/organizationIdentifier=NTRBE-0649860804/	
Certificate common name (CN)	**Serial number (SN)**

CN=Banqup Intermediate CA RSA G1-2025	HEX: 5302ADF2B9C9EB9D321DFCC456A0A0497287C42E DEC: 473905988489530340856775850085629948945850942510
Trust service certificate (Banqup Issuing CA) /C=BE/O=Banqup/organizationIdentifier=NTRBE-0649860804/	
Certificate common name (CN)	**Serial number (SN)**
CN=Banqup Issuing CA RSA G1-2025 TSL-registered	HEX: 36C56C9AE45C507A6B57FF5BE66C107B94BE81C5 DEC: 312688209262506309640404935175315313901858357701

Table 5: PKI certificates for the trust service /RemoteQSealCDManagement/Q - RSA

B) 'Banqup qualified Issuing CA ECC G2-2025'

Service type identifier according to ETSI TS 119 612 V2.4.1, sec. 5.5.1.1:	URI: http://uri.etsi.org/TrstSvc/Svctype/CA/QC
Service name:	A qualified certificate issuing trust service
Root certificate (Banqup Root CA ECC) /C=BE/O=Banqup/organizationIdentifier=NTRBE-0649860804/	
Certificate common name (CN)	**Serial number (SN)** **Fingerprint**
CN=Banqup Root CA ECC G1	HEX: 61E3ACC88D0B618298C550E1476AEBB42F5C29C4 DEC: 558849425487112772665649440253967617186326129092 SHA1: CD 29 5C 19 8E 7E C5 51 73 C3 EC 7E C0 6A 4E 65 B7 C0 1B 48
Trust service certificate (Banqup Intermediate CA) /C=BE/O=Banqup/organizationIdentifier=NTRBE-0649860804/	
Certificate common name (CN)	**Serial number (SN)**
CN=Banqup Intermediate CA ECC	HEX:

G2-2025	4D92CE079FFF9129647B77BE62E6F43416D48D93 DEC: 442866145877973856659567703970767443090281368979
Trust service certificate (Banqup Issuing CA) /C=BE/O=Banqup/organizationIdentifier=NTRBE-0649860804/	
Certificate common name (CN)	**Serial number (SN)**
CN=Banqup Issuing CA ECC G2-2025 TSL-registered	HEX: 305A6D20179BD0DD49EAB933F94D03939AA7DC95 DEC: 276048130226995642772468041126246521425220852885

Table 6: PKI certificates for the trust service /CA/QC - ECC

Service type identifier according to ETSI TS 119 612 V2.4.1, sec. 5.5.1.1:	URI: http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL/QC
Service name:	A qualified certificate issuing trust service
Root certificate (Banqup Root CA ECC) /C=BE/O=Banqup/organizationIdentifier=NTRBE-0649860804/	
Certificate common name (CN)	**Serial number (SN)** **Fingerprint**
CN=Banqup Root CA ECC G1	HEX: 61E3ACC88D0B618298C550E1476AEBB42F5C29C4 DEC: 558849425487112772665649440253967617186326129092 SHA1: CD 29 5C 19 8E 7E C5 51 73 C3 EC 7E C0 6A 4E 65 B7 C0 1B 48
Trust service certificate (Banqup Intermediate CA) /C=BE/O=Banqup/organizationIdentifier=NTRBE-0649860804/	
Certificate common name (CN)	**Serial number (SN)**
CN=Banqup Intermediate CA ECC G2-2025	HEX: 4D92CE079FFF9129647B77BE62E6F43416D48D93 DEC: 44286614587797385665956770397076744309028

	1368979
Trust service certificate (Banqup Issuing CA) /C=BE/O=Banqup/organizationIdentifier=NTRBE-0649860804/	
Certificate common name (CN)	**Serial number (SN)**
CN=Banqup Issuing CA ECC G2-2025 TSL-registered	HEX: 305A6D20179BD0DD49EAB933F94D03939AA7DC95 DEC: 27604813022699564277246804112624652142522085288 5

Table 7: PKI certificates for the trust service /Certstatus/CRL/QC – ECC

Service type identifier according to ETSI TS 119 612 V2.4.1, sec. 5.5.1.1:	URI: http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC
Service name:	A qualified certificate issuing trust service
Root certificate (Banqup Root CA ECC) /C=BE/O=Banqup/organizationIdentifier=NTRBE-0649860804/	
Certificate common name (CN)	**Serial number (SN)** **Fingerprint**
CN=Banqup Root CA ECC G1	HEX: 61E3ACC88D0B618298C550E1476AEBB42F5C29C4 DEC: 55884942548711277266564944025396761718632612 9092 SHA1: CD 29 5C 19 8E 7E C5 51 73 C3 EC 7E C0 6A 4E 65 B7 C0 1B 48
Trust service certificate (Banqup Intermediate CA) /C=BE/O=Banqup/organizationIdentifier=NTRBE-0649860804/	
Certificate common name (CN)	**Serial number (SN)**
CN=Banqup Intermediate CA ECC G2-2025	HEX: 4D92CE079FFF9129647B77BE62E6F43416D48D93 DEC: 44286614587797385665956770397076744309028 1368979
Trust service certificate (Banqup Issuing CA)	

/C=BE/O=Banqup/organizationIdentifier=NTRBE-0649860804/	
Certificate common name (CN)	**Serial number (SN)**
CN=Banqup Issuing CA ECC G2-2025 TSL-registered	HEX: 305A6D20179BD0DD49EAB933F94D03939AA7DC95 DEC: 276048130226995642772468041126246521425220852885

Table 8: PKI certificates for the trust service /Certstatus/OCSP/QC – ECC

Service type identifier according to ETSI TS 119 612 V2.4.1, sec. 5.5.1.1:	URI: http://uri.etsi.org/TrstSvc/Svctype/RemoteQSigCDManagement/Q
Service name:	The management of remote qualified electronic signature creation devices
Root certificate (Banqup Root CA ECC) /C=BE/O=Banqup/organizationIdentifier=NTRBE-0649860804/	
Certificate common name (CN)	**Serial number (SN)** **Fingerprint**
CN=Banqup Root CA ECC G1	HEX: 61E3ACC88D0B618298C550E1476AEBB42F5C29C4 DEC: 558849425487112772665649440253967617186326129092 SHA1: CD 29 5C 19 8E 7E C5 51 73 C3 EC 7E C0 6A 4E 65 B7 C0 1B 48
Trust service certificate (Banqup Intermediate CA) /C=BE/O=Banqup/organizationIdentifier=NTRBE-0649860804/	
Certificate common name (CN)	**Serial number (SN)**
CN=Banqup Intermediate CA ECC G2-2025	HEX: 4D92CE079FFF9129647B77BE62E6F43416D48D93 DEC: 442866145877973856659567703970767443090281368979
Trust service certificate (Banqup Issuing CA) /C=BE/O=Banqup/organizationIdentifier=NTRBE-0649860804/	
Certificate common name (CN)	**Serial number (SN)**
CN=Banqup Issuing CA ECC G2-	HEX:

2025 TSL-registered	305A6D20179BD0DD49EAB933F94D03939AA7DC95 DEC: 27604813022699564277246804112624652142522085288 5

Table 9: PKI certificates for the trust service /RemoteQSigCDManagement/Q – ECC

Service type identifier according to ETSI TS 119 612 V2.4.1, sec. 5.5.1.1:	URI: http://uri.etsi.org/TrstSvc/Svctype/RemoteQSealCDManagement/Q
Service name:	The management of remote qualified electronic seal creation devices
Root certificate (Banqup Root CA ECC) /C=BE/O=Banqup/organizationIdentifier=NTRBE-0649860804/	
Certificate common name (CN)	**Serial number (SN)** **Fingerprint**
CN=Banqup Root CA ECC G1	HEX: 61E3ACC88D0B618298C550E1476AEBB42F5C29C4 DEC: 558849425487112772665649440253967617186326129092 SHA1: CD 29 5C 19 8E 7E C5 51 73 C3 EC 7E C0 6A 4E 65 B7 C0 1B 48
Trust service certificate (Banqup Intermediate CA) /C=BE/O=Banqup/organizationIdentifier=NTRBE-0649860804/	
Certificate common name (CN)	**Serial number (SN)**
CN=Banqup Intermediate CA ECC G2-2025	HEX: 4D92CE079FFF9129647B77BE62E6F43416D48D93 DEC: 44286614587797385665956770397076744309028 1368979
Trust service certificate (Banqup Issuing CA) /C=BE/O=Banqup/organizationIdentifier=NTRBE-0649860804/	
Certificate common name (CN)	**Serial number (SN)**
CN=Banqup Issuing CA ECC G2-2025 TSL-registered	HEX: 305A6D20179BD0DD49EAB933F94D03939AA7DC95 DEC: 27604813022699564277246804112624652142522085288 5

Table 10: PKI certificates for the trust service /RemoteQSealCDManagement/Q - ECC

In implementing the qualified trust services, Banqup SA draws on the services of the following externally visible *delegated third parties*, whereby the TSP is liable for third parties, which it has commissioned with tasks according to Regulation (EU) No. 910/2014 as for its own actions.

- Identification of natural persons, whereby the latter can be either direct TSP's subscribers or the delegates of a legal person subscriber, see chap. 5 for details.

- Service implementing a part of the TSP certification authority: Keyfactor (eIDAS PKI EJBCA) by KEYFACTOR - PrimeKey Solutions AB, Sundbybergsvägen 1, 8th floor, SE-171 73 Solna, Stockholm, Sweden, corp. ID no. 556628-3064.

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

3. Certification Programme/Scheme

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)', see https://www.telekom-zert.com/en/service-area/.

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 current basic document of the trust service provider "Banqup SA" - the Service Provision Practice Statement (publicly available) "CP/CPS Certificate Policy and Certification Practice Statement, v. 1.1.1" as of 05.02.2026 - is suitable for the operations of a qualified trust service provider as defined by eIDAS Regulation.

The current basic document of the trust service provider "Banqup SA" is implemented accordingly in practice.

The trust service provider „Banqup SA" 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 V2.4.1, 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/OCSP/QC URI: http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL/QC
creating qualified certificates for electronic seals	URI: http://uri.etsi.org/TrstSvc/Svctype/CA/QC URI: http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC URI: http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL/QC

Description of the trust service	‘qualified trust service type’ according to ETSI TS 119 612 V2.4.1, sec. 5.5.1
qualified remote qSCD management The management of remote qualified electronic signature creation devices as a qualified trust service carried out by a qualified trust service provider on behalf and under control of remote signers	URI: http://uri.etsi.org/TrstSvc/Svctype/RemoteQSigCDManagement/Q
qualified remote qSCD management The management of remote qualified electronic seal creation devices as a qualified trust service carried out by a qualified trust service provider on behalf and under control of remote seal creators	URI: http://uri.etsi.org/TrstSvc/Svctype/RemoteQSealCDManagement/Q

Table 11: Trust services provided in compliance with eIDAS Regulation

5. Integrated Modules

For implementing the trust services in scope, the TSP uses the following already eIDAS-confirmed qualified services provided by module operators as delegated third parties, whereby single certified and not certified operational options of the modules are exactly stated in each related Conformity Certificates for the modules.

A single module can be used by the TSP as *exclusive* or *non-exclusive* service provided by the respective delegated third party (called 'module provider').

In case of the *exclusive* service by a module, the TSP shall use the module for the provision of the qualified trust services listed in chap. 4, Table 11 above. Therefore, the present Conformity Certificate covers the operation of the qualified trust services listed in chap. 4, Table 11 above solely using the respective modules.

In case of the *non-exclusive* service by a module, the TSP may operatively decide on the usage or non-usage of the module in the qualified TSP operation. Hence, the present Conformity Certificate for the TSP covers the TSP operation with this service as well as without it.

The table below represents a snapshot at the time of issuance of the present Conformity Certificate. Precise information on the modules of the *non-exclusive* services that are integrated by the TSP at a given time can be obtained from the TSP.

modul name	modul service	modul provider	address	Conformity Certificate acc. to eIDAS		exclusive or non-exclusive service by the module
				ID	valid until	
Itsme®	identification service eID means: itsme® mobile App	Belgian Mobile ID NV	Sint Goedelelaan 5, 1000 Brussels; company registration number 0541.659.084	'Belgian eID Scheme FAS / itsme®' is notified acc. to Art. 9 of the eIDAS since 18.12.2019	not limited	non-exclusive
Signicat E - IDENTIFICAZIONE	identification service Trust service components providing identity proofing of trust service subjects. ETSI EN 319 401 V3.1.1 ETSI TS 119 461 V2.1.1	Signicat S.L.U.	Avenida Ciudad de Barcelona, 81, 4ª planta, 28007 Madrid; company registration number B86681533	No. 84181, issued by CSQA	26.07.2026	non-exclusive
Identity Management	identification service	IDnow GmbH	Auenstrasse 100, 80469 Munich; company registration number HRB 283590 at the Amtsgericht München	SRC.00069.TSP.08.2024	26.08.2026	non-exclusive

6. Summary and Notes

1. The current basic document of the trust service provider “Banqup SA”

   - Service Provision Practice Statement (publicly available) “CP/CPS Certificate Policy and Certification Practice Statement, v. 1.1.1” as of 05.02.2026

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

2. The trust service provider „Banqup SA“ operates the trust services listed in chap. 4, Table 11 above in compliance with the relevant requirements of the current version of the eIDAS Regulation.

3. The present Conformity Certificate TelekomSecurity.031.0331.02.2026 covers the use of the integrated modules by the TSP in its qualified operation, only as long as these modules are validly confirmed (listed in full in chap. 5).
   After the expiry of the period of validity of the conformity certificate of each of these modules, the TSP shall either present a new (supplementary) conformity certificate for an eIDAS-compliant operation or discontinue the use of the no longer conformity certified module in the qualified operation.

4. The present Conformity Certificate TelekomSecurity.031.0331.02.2026 is valid for the basic documents listed in para. 1 above up to and including 25.02.2028.
   This validity period (that is, the maximum possible duration of TSP operation in compliance with eIDAS Regulation) results from the specification of the eIDAS Regulation, Article 20 (1).
   The validity of the present 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.031.0331.02.2026

Issuer:	Deutsche Telekom Security GmbH
Head office:	Friedrich-Ebert-Allee 71-77, 53113 Bonn
Address of CB:	Bonner Talweg 100, 53113 Bonn
Phone:	+49-(0)228-181-0
Web:	www.telekom-zert.com