Conformity Assessment Report:
Conformity Certificate and Summary

Attachment No. 1 to
TelekomSecurity.031.0315.09.2024

Trust Service Provider:

SIGN8 GmbH

Conformity Certificate

TelekomSecurity.031.0315.09.2024
Attachment No. 1

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

valid from 30.09.2024 up to and including: 29.09.2026

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
„SIGN8 GmbH"

provides the following trust services:

- **issuance qualified certificates for electronic signatures**
- **issuance qualified certificates for electronic seals**
- **management of remote QSCD for qualified el. signatures/seals**
- **creation of qualified electronic timestamps**

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

ed and registered under: **TelekomSecurity.031.0315.U.12.2024**

Bonn, 03.12.2024

_____
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 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

This Attachment No. 1 to Conformity Certificate consists of 18 pages.

1.   Object of the Conformity Assessment

1.1 Name of the Trust Service Provider

SIGN8 GmbH
Fürstenrieder Straße 5
80687 München
Germany

Internet: https://www.SIGN8.eu
Phone: +49 (0)89 / 2153 7472 000
e-mail: info@sign8.eu

1.2 Name(s) of the Qualified Trust Services Provided

- **SIGN8 qualified signatures certificate, SIGN8 qualified electronic signatures certificate**.

The names above represent merely different names of same trusted service for marketing purposes.

- **SIGN8 qualified seal certificate, SIGN8 qualified electronic seal certificate**.

The names above represent merely different names of same trusted service for marketing purposes.

- **SIGN8 qualified remote signing, SIGN8 qualified electronic remote signing**.

The names above represent merely different names of same trusted service for marketing purposes.

- **SIGN8 qualified remote sealing, SIGN8 qualified electronic remote sealing**.

The names above represent merely different names of same trusted service for marketing purposes.

- **SIGN8 qualified timestamping, SIGN8 qualified electronic timestamping**.

The names above represent merely different names of same trusted service for marketing purposes.

1.3 Current Confirmation Status

SIGN8 GmbH (abbreviated as SIGN8) is a 'qualified trust service provider' (qTSP) according to Art. 24 of the eIDAS Regulation[2].

The last full conformity assessment according to Article 20(1) of the eIDAS Regulation was accomplished with issuing the conformity certificate TelekomSecurity.031.0315.09.2024 as of 30.09.2024.

The present conformity re-assessment of the TSP according to Article 20(1) of the eIDAS Regulation as documented here (ID: Attachment #1 to TelekomSecurity.031.0315.09.2024) represents a confined re-assessment serving the attainment 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.

The present re-assessment is based on

– the Service Provision Practice Statement, version 1.5 as of 25.11.2024 (not publicly available), and

– the Certificate Practice Statement, version 1.5 as of 25.11.2024 (publicly available). This document is publicly available under https://www.sign8.eu/trust.

and covers the following modifications of the above stated Practice Statements:

1) Externally visible changes that are (i) visible to TSP subscribers and (ii) transparent for relying parties:

– The identification method "Verimi identity verification service"[3] provided by Verimi GmbH is not used any more in the qualified operation of the qTSP.

– Other service certificates for the qualified electronic timestamping service are in use.

2) Internal changes in the qualified operation that are fully transparent for (i) TSP subscribers and for (ii) for relying parties, as well:

---

[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

[3] The original name in German: „Verimi Identitätsfeststellungsdienst".

– Conformity of the qTSP SIGN8 GmbH and of the qualified trust services provided by the qTSP to a set of ETSI- and DIN-standards is verified and confirmed (additionally to the conformity to eIDAS Regulation), see chapter 2 below for the list of the respective ETSI- and DIN-standards.

2. Reason for the Amendment

SIGN8 GmbH 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),

- creating qualified electronic timestamps (qualified trust service - TSA/QTST).

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

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

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

The remote signing service for TSP's subscribers corresponds with the particular trust service type for remote signing
URI: http://uri.etsi.org/TrstSvc/Svctype/RemoteQSigCDManagement/Q as defined by ETSI TS 119 612 v2.3.1, sec. 5.5.1.1.

The remote sealing service for TSP's subscribers corresponds with the particular trust service type for remote sealing
URI: http://uri.etsi.org/TrstSvc/Svctype/RemoteQSealCDManagement/Q as defined by ETSI TS 119 612 v2.3.1, sec. 5.5.1.1.

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

Besides this, the TSP also issues *portable* qualified secure signature/seal creation devices (qSCD) – so called eToken in USB-stick form factor – to TSP's subscribers.

These devices acting as qSCD for generating qualified electronic signatures locally are "IDPrime 940" and "IDPrime 940C" (contact interface) as well as "IDPrime 3940" and "IDPrime 3940C" (dual interface).

A detailed description of qualified trust services provided by the TSP is given in the reference certificate TelekomSecurity.031.0315.09.2024 as of 30.09.2024 and in all previous Attachments, if any, as listed in sec. 1.3 above and shall be regarded to.

The following changes in the TSP operation have occurred in the meantime and are the reason for this Attachment #1 to the Certificate TelekomSecurity.031.0315.09.2024:

(i)   Conformity of the qTSP SIGN8 GmbH and of the qualified trust services provided by the qTSP to the following ETSI- and DIN-standards is verified and confirmed (additionally to the conformity to eIDAS Regulation as stated in sec. 1.3 above):

1. ETSI EN 319 401 V3.1.0 (2024-03) Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

2. ETSI EN 319 411 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates:

- ETSI EN 319 411-1 V1.4.1 (2023-10) Part 1: General requirements.

- ETSI EN 319 411-2 V2.5.1 (2023-10) Part 2: Requirements for trust service providers issuing EU qualified certificates.

3. ETSI EN 319 412 Electronic Signatures and Infrastructures (ESI); Certificate Profiles:

- ETSI EN 319 412-1 V1.5.1 (2023-09) Part 1: Overview and common data structures.

- ETSI EN 319 412-2 V2.3.1 (2023-09) Part 2: Certificate profile for certificates issued to natural persons.

- ETSI EN 319 412-3 V1.3.1 (2023-09) Part 3: Certificate profile for certificates issued to legal persons.

- ETSI EN 319 412-5 V2.4.1 (2023-09) Part 5: QCStatements.

4. ETSI EN 319 421 V1.2.1 (2023-05) Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Timestamps.

5. ETSI EN 319 422 V1.1.1 (2016-03) Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles.

6. DIN EN 419 241-1:2018-09 Trustworthy Systems Supporting Server Signing – Part 1: General System Security Requirements.

7. TS-119-431-1 V1.2.1 (2021-05) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev.

(ii)   The identification method "Verimi identity verification service"[4] provided by Verimi GmbH is not used any more in the qualified operation of the qTSP.

(iii)   Other service certificates for the qualified electronic timestamping service are in use.

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.

The TSP operates the following PKIs as single branches of the 'SIGN8 PKI':

-   PKI 1st Generation [CA 01 for QC]: The list of the respective service certificate information for all qualified trust services provided by the TSP using the "PKI 1st Generation [CA 01 for QC]" has remained unchanged and is given in the reference certificate TelekomSecurity.031.0315.09.2024 as of 30.09.2024 and in all previous Attachments, if any, as listed in sec. 1.3 above and shall be regarded to.

-   PKI 2nd Generation [CA 03 and CA 04 for QC]: The list of the respective service certificate information for all qualified trust services provided by the TSP using the "PKI 2nd Generation [CA 03 and CA 04 for QC]" has remained unchanged and is given in the reference certificate TelekomSecurity.031.0315.09.2024 as of 30.09.2024 and in all previous Attachments, if any, as listed in sec. 1.3 above and shall be regarded to.

-   PKI 2nd Generation [CA 01 and CA 02 for QTST]: The list of the respective service certificate information for all qualified trust services provided by the TSP using the "PKI 2nd Generation [CA 01 and CA 02 for QTST]" has changed and is given below.

---

[4] The original name in German: „Verimi Identitätsfeststellungsdienst".

PKI 2nd Generation [CA 01 and CA 02 for QTST]:

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:	SIGN8 certification service

Root certificate (root CA)	
/C=DE /O=SIGN8 GmbH/	

certificate name (CN)	Serial number (SN, hex, dec) SHA1 Fingerprint
CN=SIGN8 GmbH ROOT CA 01	HEX: 4a001d778aa039bb1eb44456d0de6b1621d0e315 DEC: 422467883975123211270282792050212362449922876181 SHA1: 2d3fb00cc3f2e9361368938d60cb14a682518cfc

Trust service certificates (SIGN8 TIMESTAMP CA 01)	
/C=DE /O=SIGN8 GmbH/	

certificate name (CN)	Serial number (SN, hex, dec)
CN=SIGN8 TIMESTAMP CA 01 *TSL-registered*	HEX: 629D7A4480DCD113492E32517F46A000F6582630 DEC: 5629929635462779359029130101246676027535204412208

Base64:

-----BEGIN CERTIFICATE-----
MIIGQDCCBCigAwIBAgIUYp16RIDc0RNJLjJRf0agAPZYJjAwDQYJKoZIhvcNAQEN
BQAwgYoxCzAJBgNVBAYTAkRFMRAwDgYDVQQIDAdCYXZhcmlhMRMwEQYDVQQKDApT
SUdOOCBHbWJIMRQwEgYDVQRhDAtERTM0OTk3Nzg4MjEeMBwGA1UECwwVU0lHTtjgg
R21iSCBST09UIENBIDAxMR4wHAYDVQQDDBVTSUdOOCBHbWJIIIFJPT1QgQ0EgMDEw
HhcNMjQxMTE0MTMyNDE5WhcNMzkxMTExMTMyNDE5WjB+MQswCQYDVQQGEwJERTET

```
MBEGA1UECgwKU0lHTjggR21iSDEXMBUGA1UECwwOVHJ1c3QgU2VydmljZXMxITAf
BgNVBGEMGE5UUkRFLURFRDI2MDFWLkhSQjI3MTU3MzEeMBwGA1UEAwwVU0lHTjgg
VElNRVNUQU1QIENBIDAxMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA
wRKin0iqDj/Y6cF8cSTyMF6b0ufKt1K7hCr/p6s9q+2rtWzOTh/mm7g8+K2sLtXp
tVT18L82fJOyjdkZlrW2CNyxmNdhLdNz4IOMbR4yzStOMrx1PC+RZfIjBRZNmanw
GJoHuFr9iau2Yt32RMWO07H+qkhchJ8lvz1ZGGYVLbe39cUafNxL0tw+BK8b+AjH
JZnkrIeiGh6xypuvpKyx/ouBOqJ0oixCGZsr1Hch4S6mw2yoVSebdU5Kmgl9ROh9
EqP9hkuvAoB+krVtZVD1EB9D7eMS3UzPN92nGkzcn3DNpV/WPaId24h1YoTybJ/l
2hdWX1ojAbpsf4WBm9+zm3hGQxNNk7rtwsvch5iuUwBe8N+LfFX+2lcg9fdpaKCS
NIPWwC7jFC3o21SuCElKBDfrv9itK6j2QEjDrOy/YWc7jIwMAG7gRGP9uhPkcUKn
7szIZJFCihiSFpI+KQLPfc+raPbkbmbPGiG4usVp5zxXd2498c1q+NZ4ABpOoD35
DWOYQLbIty+ZUyMxg6slnxd6q7YTyRDAkLJ9WDuRwO2WCJPkjyOKcJVCzUaPzAmk
aD+Tb3fPKrskhrBOZoMr6hV/PfETRhyZ2+TXMclppmZZz80xVrDMtariN0tAwORo
Uuf7ey9hgCbvowjx+jurs93bqWUbX1YqfsDLqo2zAPUCAwEAAaOBqDCBpTAdBgNV
HQ4EFgQUzPAjRLA+4RlzqOSBJmn4VNqISGAwHwYDVR0jBBgwFoAUY/B7DAu3J0Ho
h3FRdu49YuD9nZQwEgYDVR0TAQH/BAgwBgEB/wIBADAOBgNVHQ8BAf8EBAMCAQYw
PwYDVR0gBDgwNjA0BgsrBgEEAYPGVQEKADAlMCMGCCsGAQUFBwIBFhdodHRwczov
L3NpZ244Lm5lL3RydXN0LZANBgkqhkiG9w0BAQ0FAAOCAgEABXnMJroVPd51cJ/V
ckowJk3hD68vqmQaH6i/dzWLM0LiTBrnYTZUY4IlKxvPEoahP08Mz/QylNMeX8aX
byA4NejCjPqyy3Ce/cfZkTxQ9jDwtlyN7gLdw37kcegn+74fnr/rJ4WMD/RU8gTj
IKcDeg+SbtBLy9oZiZqoqFyGu3Rd6YXaO9eWI3VQVBs/nm0ymJpjGPND7ugV/ekh
6Oqfn6JNVurqonSKOmfowv0T0jWJR/ArBxmtv4dgp8dhDZ3DbjDyg2/m9psciLLe
u5NJYhkRAvDxwTSZFfSobbJAzDNHvKoQ9CG4XztxFpT88HP+Ydc5q+N6oW1G1XnC
PSsAAl4iVcJfsWSp6F+uqgOfm3OxSCRRLKUgkt0wF8P9ltjV9UwyE5YoICv+WAh+
LNWIjZ/8mz5NncbmfUnq8WR12vi4W3dUkg3y+7PdviurNyPdVhlQ+cJmAMnHun3x
TNRiRDyFLjUCcr4Ho347q8qBDegGt0Oh5zAxTxNOBEEs85kd6H1KilW/0eZ2vdFo
AOmlZ8IgdtXpDQDAG4hY8/ZuWdoxTFwv/ll8sBNPzDF8xydwRdEKFVAf1fLcMzrj
hxw6DUdzdWFEwi2YUv0l+mZgapi9ZHaXUDTfHPap/mhmPGqH2PH07dZpXIQXKoUY
OVVxXwMhtCDUYIs50spsciKJG3E=
-----END CERTIFICATE-----
```

Table 1: „SIGN8 PKI TIMESTAMP 2nd GEN CA 01": Certificates for the trust service /TSA/QTST

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:	SIGN8 certification service
Root certificate (root CA) /C=DE /O=SIGN8 GmbH/	
certificate name (CN)	**Serial number (SN, hex, dec)**

	SHA1 Fingerprint
CN=SIGN8 GmbH ROOT CA 01	HEX: 4a001d778aa039bb1eb44456d0de6b1621d0e315 DEC: 4224678839751232112702827920502123624499228 76181 SHA1: 2d3fb00cc3f2e9361368938d60cb14a682518cfc

Trust service certificates (SIGN8 TIMESTAMP CA 02)	
/C=DE /O=SIGN8 GmbH/	

certificate name (CN)	Serial number (SN, hex, dec)
CN=SIGN8 TIMESTAMP CA 02 *TSL-registered*	HEX: 629D7A4480DCD113492E32517F46A000F6582631 DEC: 5629929635462779359029130101246676027535 20412209

Base64:

-----BEGIN CERTIFICATE-----
MIIGQDCCBCigAwIBAgIUYp16RIDc0RNJLjJRf0agAPZYJjEwDQYJKoZIhvcNAQEN
BQAwgYoxCzAJBgNVBAYTAkRFMRAwDgYDVQQIDAdCYXZhcmlhMRMwEQYDVQQKDApT
SUdOOCBHbWJIMRQwEgYDVQRhDAtERTM0OTk3Ng4MjEeMBwGA1UECwwVU0lHHTjgg
R21iSCBST09UIENBIDAxMR4wHAYDVQQDDBVTSUdOOCBHbWJIIFJPT1QgQ0EgMDEw
HhcNMjQxMTE0MTMyNzQ1WhcNMzkxMTExMTMyNzQ1WjB+MQswCQYDVQQGEwJERTET
MBEGA1UECgwKU0lHHTjggR21iSDEXMBUGA1UECwwOVHJ1c3QgU2VydmljZXMxITAf
BgNVBGEMGE5UUkRFLURFRDI2MDFWLkhSQjI3MTU3MzEeMBwGA1UEAwwVU0lHHTjgg
VElNRVNUQU1QIENBIDAyMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA
xOO8xqtvfLqruFREb9DvzqGib0BSb7BXREILX0+AVvGy0yiXFLGZkTUNu18bJKer
x3UEjBFx6jhktfSRCVa5x1sCSx4X4voR0OutEcETLa1tLLLt/+T9cSYuYkA5ju74
Cs5uvsbWvoSd5DJblkabmKFmmvcJEObjPRD8mMpaU8zvNllBeUaUl5M2GUCg5BOS
l6dlBn8Wo17kcGfTZZc2xcevzKpubcQxEjeYiQMMqHTu/UanT9kInc9Z46JpZFMp
ZEDjBRFueLXS+LJ5LpQtXgfxikH04nat97Bzi4LX0YO4CJ5dk6HcBeoXm/XcfVQm
jR385QYG58fMheTnCTohpwdYWhwD72eyexvfNogU+m0L0r+AdjDGdQOlEpBvk8jS
INQ3RvFfbVLHlF7iq/19ZJdQdvQuDG07GXOAA7muzlH6F53BZxCbB6wuMBoYk5sF
Tc1yTuRBwwZeHo4v5iAeT2fVoRzJ3G/gY10buyIL5nmSk2lEx/XL6QfOsqSbWTxQ
cNgwR7tv8xohL0JW3OjzfD4xyRwKXYuLFXOmjQfSR4HFVFHixFfakZTiNkdSbo5a
MfQR/r+I0uxV9L++jWxN7K5zlBkmvohn6luDtH9Ea2ERwX+UqRWUXVenU308zyRV
uSalopW3YBGOuyDggXxYZ+PsWCEO+i+lXMHajWyDZ9UCAwEAAaOBqDCBpTAdBgNV

```
HQ4EFgQUgjky7PtBIjju9MOs8jZ8vw/dDs8wHwYDVR0jBBgwFoAUY/B7DAu3J0Ho
h3FRdu49YuD9nZQwEgYDVR0TAQH/BAgwBgEB/wIBADAOBgNVHQ8BAf8EBAMCAQYw
PwYDVR0gBDgwNjA0BgsrBgEEAYPGVQEKADAlMCMGCCsGAQUFBwIBFhodHRwczov
L3NpZ244LmV1L3RydXN0LzANBgkqhkiG9w0BAQ0FAAOCAgEAhnmcXCKopBH2y/a8
KgFp856lgSXrbvKs0bcmqH9wGBYqYwFRUMZGwhyASET3cXj1iR5lyuwB7ymgM8ky
CASQl1/fmMMFno1sAPjdgQdHAf9TCVkEr88ldsbO2wnzbRAi4corf1r2h0H+Pgc3
MndlTW2aapuBqLzuhcsHx2nsFR11h5VCnCgFN7fbJyY/lH5uRvmoqOf3V2Rm/hEh
88KYpd371kifNnOlDfSa4MdoxtS1xiw2W0QWmWjvsH3YPD1cY+GVcs9GenDv0kkk
RFijBgal481kyzQRH09/8vDapB09PkKmsYSGGapFVsuCxQVuoE9CqJIKig1Vj0wv
bRwX7AVQ9yITqye0rp305tKzHpK1SNYGQdjcu8FQDsKlixg6Cl0zTQA93WC5mhqd
fahEH/eYhe/CxFnXADgfd+T6t1R+H7bE+TzUmkjIvqd+3dtgly3fk2pw1yaeRFH+
+4PMtoKjmS07D4UAOEkOd2uWOnTZeA0+1Uaf4WVn1ihGhfCjmy1I01Q/ydrKuCX+
kBI3zNWzFBS/NtQFTIVdqXN1zoK0gBnPZzqJurs9tsKfjiErInapxF+F4/tuHy1F
FayPJr+jjugIIpESf5O6m1zg02mt9G2skVuWtK5qwHN8zzEpuuhSXiZNP0IrDvbN
5n9li3HnlxVSeQX8pbjRHj9bTWI=
-----END CERTIFICATE-----
```

Table 2: „SIGN8 PKI TIMESTAMP 2nd GEN CA 02": Certificates for the trust service /TSA/QTST

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:	SIGN8 certification service
Root certificate (root CA) /C=DE /O=SIGN8 GmbH/	
certificate name (CN)	**Serial number (SN, hex, dec)** **SHA1 Fingerprint (hex)**
CN=SIGN8 GmbH ROOT CA 01	HEX: 4a001d778aa039bb1eb44456d0de6b1621d0e315 DEC: 4224678839751232112702827920502123624499228 76181 SHA1: 2d3fb00cc3f2e9361368938d60cb14a682518cfc
Trust service certificate (SIGN8 TIMESTAMP CA 01)	

/C=DE /O=SIGN8 GmbH/	
certificate name (CN)	**Serial number (SN, hex, dec)**
CN=SIGN8 TIMESTAMP CA 01 *TSL-registered*	HEX: 629D7A4480DCD113492E32517F46A000F6582630 DEC: 56299296354627793590291301012466760275352 0412208
Base64: see Table 1 above.	
Trust service certificate (OSCP-Service-Certificate) /C=DE /O=SIGN8 GmbH/	
certificate name (CN)	**Serial number (SN, hex, dec)**
CN=OCSP SIGN8 TIMESTAMP CA 01	HEX: 5CC000C1BD3B32F7 DEC: 6683342679121277687

Table 3: „SIGN8 PKI TIMESTAMP RSA 2nd GEN CA01": Certificates for the trust service /Certstatus/OCSP/QC

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:	SIGN8 certification service
Root certificate (root CA) /C=DE /O=SIGN8 GmbH/	
certificate name (CN)	**Serial number (SN, hex, dec)** **SHA1 Fingerprint (hex)**
CN=SIGN8 GmbH ROOT CA 01	HEX: 4a001d778aa039bb1eb44456d0de6b1621d0e315 DEC: 42246788397512321127028279205021236244992287 6181

	SHA1: 2d3fb00cc3f2e9361368938d60cb14a682518cfc

Trust service certificate (SIGN8 TIMESTAMP CA 02)	
/C=DE /O=SIGN8 GmbH/	
certificate name (CN)	**Serial number (SN, hex, dec)**
CN=SIGN8 TIMESTAMP CA 02 *TSL-registered*	HEX: 629D7A4480DCD113492E32517F46A000F6582631 DEC: 56299296354627793590291301012466760275352 0412209
Base64: see Table 2 above.	

Trust service certificate (OSCP-Service-Certificate)	
/C=DE /O=SIGN8 GmbH/	
certificate name (CN)	**Serial number (SN, hex, dec)**
CN=OCSP SIGN8 TIMESTAMP CA 02	HEX: 74C03781832EDC6A DEC: 8412785133319281770

Table 4: „SIGN8 PKI TIMESTAMP ECC 2nd GEN CA 02": Certificates for the trust service /Certstatus/OCSP/QC

The TSP does not provide certificate revocation lists (CRLs). Therefore, there are no corresponding trust service certificates for the trust service /Certstatus/CRL/QC.

In implementing the qualified trust services, SIGN8 GmbH 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 and according to the VDG[5], as for its own actions, see §6 VDG:

-   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.

---

[5] Gesetz zur Durchführung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (BGBI. I S. 2745, Stand: 18.07.2017)

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 Programme 031)'.

The Certification Body of Telekom Security is a conformity assessment body as provided by Article 3 paragraph 18 of the 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 the 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 documents of the trust service provider "SIGN8 GmbH" - version 1.5 as of 25.11.2024 of the Service Provision Practice Statement (not publicly available) and version 1.5 as of 25.11.2024 of the Certificate Practice Statement (publicly available) - are suitable for the operations of a qualified trust service provider as defined by eIDAS Regulation.

The current basic documents of the trust service provider "SIGN8 GmbH" are implemented accordingly in practice.

The trust service provider „SIGN8 GmbH" 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/OCSP/QC
creating qualified certificates for electronic seals	URI: http://uri.etsi.org/TrstSvc/Svctype/CA/QC URI:

Description of the trust service	'qualified trust service type' according to ETSI TS 119 612 V2.1.1, sec. 5.5.1
	`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 V2.3.1, sec. 5.5.1 ETSI TS 119 612 V2.3.1 is NOT covered by the IMPLEMENTING DECISION (EU) 2015/1505 (Trusted Lists)
The management of remote qualified electronic signature creation devices as a qualified trust service carried out by a qualified trust service provider	URI: `http://uri.etsi.org/TrstSvc/Svctype/RemoteQSigCDManagement/Q`
The management of remote qualified electronic seal creation devices as a qualified trust service carried out by a qualified trust service provider	URI: `http://uri.etsi.org/TrstSvc/Svctype/RemoteQSealCDManagement/Q`

Table 5: Trust services provided in compliance with eIDAS Regulation

These determinations also apply to the fulfilment of applicable requirements of the VDG and the VDV[6] as well as to the fulfilment of applicable requirements of the ETSI- and DIN-standards listed in chapter 2 above.

---

[6] Vertrauensdiensteverordnung vom 15. Februar 2019 (BGBl. I S. 114; Stand: 15.02.2019)

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 <u>shall</u> use the module for the provision of the qualified trust services listed in chap. 4, Table 5 above. Therefore, the present Conformity Certificate covers the operation of the qualified trust services listed in chap. 4, Table 5 above solely using the respective modules.

In case of the *non-exclusive* service by a module, the TSP <u>may</u> 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	
AusweisIDent Online	identification of *natural* persons *Service name*: "AusweisIDent Online" i) in compliance with eIDAS Art. 24.1a (c) ii) confirmed assurance level: '*substantial*' acc. to Commission Implementing Regulation (EU) 2015/1502: *not applicable*	D-Trust GmbH	Kommandantenstraße 15, 10969 Berlin, Germany	97203.23	26.01.2025	*non-exclusive*
Nect Ident	identification of *natural* persons i) in compliance with eIDAS Art. 24.1a (c) ii) confirmed assurance level: '*substantial*' acc. to Commission Implementing Regulation (EU) 2015/1502: *not applicable* iii) in compliance with VDG § 11 para. 3	Nect GmbH	Großer Burstah 21 20457 Hamburg, Germany	DSC.1269.07.2023	14.07.2025	*non-exclusive*

modul name	modul service	modul provider	address	Conformity Certificate acc. to eIDAS		exclusive or non-exclusive service by the module
				ID	valid until	
cidaas ID validator	identification of *natural* persons i) in compliance with eIDAS Art. 24.1a (c) ii) confirmed assurance level: '*substantial*' acc. to Commission Implementing Regulation (EU) 2015/1502: *not applicable* iii) in compliance with VDG § 11 para. 3	Widas ID GmbH	Maybachstraße 2 71299 Wimsheim, Germany	DSC.1350.10.2023	15.10.2025	*non-exclusive*
Unattended remote identity proofing with automated operation	identification of *natural* persons i) in compliance with eIDAS Art. 24.1a (c) ii) confirmed assurance level: '*substantial*' acc. to Commission Implementing Regulation (EU) 2015/1502: *not applicable* iii) in compliance with ETSI TS 119 461	fidentity AG	Waldeggstrasse 30, CH-3097 Liebefeld, Switzerland	KPMG 215 / 2023	13.04.2025	*non-exclusive*

6. Summary and Notes

1. The current basic documents of the trust service provider "SIGN8 GmbH"

   – version 1.5 as of 25.11.2024 of the Service Provision Practice Statement (<u>not</u> publicly available), and

   – version 1.5 as of 25.11.2024 of the Certificate Practice Statement (publicly available)

   are suitable for the operation of a qualified trust service provider as defined by eIDAS Regulation and are implemented accordingly in practice.
   This determination also applies to the fulfilment of applicable requirements of the VDG and the VDV as well as to the fulfilment of applicable requirements of the ETSI- and DIN-standards listed in chapter 2 above.

2. The trust service provider „SIGN8 GmbH" operates the trust services listed in chap. 4, Table 5 above in compliance with the relevant requirements of the current version of the eIDAS Regulation.
   This determination also applies to the fulfilment of applicable requirements of the VDG and the VDV as well as to the fulfilment of applicable requirements of the ETSI- and DIN-standards listed in chapter 2 above.

3. The present Attachment No. 1 to the Conformity Certificate TelekomSecurity.031.0315.09.2024 amends this Conformity Certificate.

4. All provisions from the Conformity Certificate TelekomSecurity.031.0315.09.2024 as well as from previous Attachments shall continue to apply unless they have been revoked in the meantime by the present Attachment or by previous Attachments, if any.

End of the Attachment No. 1 to Conformity Certificate