



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

TelekomSecurity.031.0283.09.2022

Trust Service Provider:

SIGN8 GmbH

Conformity Certificate

TelekomSecurity.031.0283.09.2022

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

valid from 30.09.2022 up to and including: 29.09.2024

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:

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

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

This certificate is filed and registered under: **TelekomSecurity.031.0283.09.2022**

Bonn, 30.09.2022

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

SIGN8 GmbH
Fürstenrieder Straße 5
80687 München
Germany

Internet: <https://www.SIGN8.eu>
Phone: +49 (0)89 / 2153 623 20
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.

1.3 Current Confirmation Status

SIGN8 GmbH (abbreviated as SIGN8) strives to attain the status as a 'qualified trust service provider' (qTSP) according to Art. 24 of eIDAS Regulation².

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

The present assessment is based on

- the Service Provision Practice Statement, version 1.0 as of 26.07.2022 (not publicly available), and
- the Certificate Practice Statement, version 1.0 as of 26.07.2022 (publicly available). This document is publicly available under <https://www.sign8.eu/trust>.

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

SIGN8 GmbH operates and provides the following trust services in the qualified TSP operation as defined in 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).

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

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 remote signing service for TSP's subscribers corresponds with the particular trust service type for remote signing

URI: <http://uri.etsi.org/TrstSvc/Svctype/RemoteQSCDManagement/Q> as defined by ETSI TS 119 612 v2.2.1, sec. 5.5.1.1.

Signature/seal creation data generated and managed by the TSP on behalf of subscribers can be used by TSP's subscribers exclusively within the remote signing service provided by the TSP to its subscribers. No *portable* qualified secure signature/seal creation devices (qSCD) are issued to TSP's subscribers.

SIGN8 GmbH operates and provides the following relevant services:

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

The certificate extension qcStatement – qcSCD (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 a remote access for subscribers for the execution of transactions (generation of remote signatures and remote seals),
- Operation of a web portal providing information about these services (<https://www.sign8.eu>, <https://www.sign8.eu/trust>), including the TSP's Practice Statement, online forms for applications (menu entry 'functions'), subscriber information, legal basis (see footer on the website), service certificates and other related information,
- Technical support for customers/subscribers via the functional mailbox info@sign8.eu.

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	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
electronic signatures	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/OCSP/QC

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

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

Service type identifier	URI:
according to ETSI TS 119 612	http://uri.etsi.org/TrstSvc/Svctype/CA/QC

V2.1.1, sec. 5.5.1:	
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: 422467883975123211270282792050212362449922876 181 SHA1: 2d3fb00cc3f2e9361368938d60cb14a682518cfc
Trust service certificates (QES-Seal-CA-01) /C=DE /O=SIGN8 GmbH/	
certificate name (CN)	Serial number (SN, hex, dec)
CN= SIGN8 GmbH QES SEAL CA 01 TSL-registered	HEX: 629D7A4480DCD113492E32517F46A000F658261F DEC: 562992963546277935902913010124667602753520 412191

Table 1: „SIGN8 PKI QSEAL ECC“: 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/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: 42246788397512321127028279205021236244992287 6181 SHA1: 2d3fb00cc3f2e9361368938d60cb14a682518cfc
Trust service certificates (QES-Seal-CA-02) /C=DE /O=SIGN8 GmbH/	
certificate name (CN)	Serial number (SN, hex, dec)
CN=SIGN8 GmbH QES SEAL CA 02 <i>TSL-registered</i>	HEX: 629D7A4480DCD113492E32517F46A000F6582621 DEC: 56299296354627793590291301012466760275352 0412193

Table 2: „SIGN8 PKI QSEAL RSA“: 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/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:

	42246788397512321127028279205021236244992287 6181 SHA1: 2d3fb00cc3f2e9361368938d60cb14a682518cfc
Trust service certificates (QES-Signing-CA-01)	
/C=DE /O=SIGN8 GmbH/	
certificate name (CN)	Serial number (SN, hex, dec)
CN=SIGN8 GmbH QES SIGNATURE CA 01 <i>TSL-registered</i>	HEX: 629d7a4480dcd113492e32517f46a000f658261e DEC: 56299296354627793590291301012466760275352 0412190

Table 3: „SIGN8 PKI QES ECC“: 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/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: 42246788397512321127028279205021236244992287 6181 SHA1: 2d3fb00cc3f2e9361368938d60cb14a682518cfc
Trust service certificates (QES-Signing-CA-02)	

/C=DE /O=SIGN8 GmbH/	
certificate name (CN)	Serial number (SN, hex, dec)
CN=SIGN8 GmbH QES SIGNATURE CA 02 <i>TSL-registered</i>	HEX: 629d7a4480dcd113492e32517f46a000f6582620 DEC: 56299296354627793590291301012466760275352 0412192

Table 4: „SIGN8 PKI QES RSA“: 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/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 (QES-Seal-CA-01)	
/C=DE /O=SIGN8 GmbH/	
certificate name (CN)	Serial number (SN, hex, dec)
CN= SIGN8 GmbH QES SEAL CA 01 <i>TSL-registered</i>	HEX: 629D7A4480DCD113492E32517F46A000F658261F DEC:

	56299296354627793590291301012466760275352 0412191
Trust service certificate (OSCP-Service-Certificate)	
/C=DE /O=SIGN8 GmbH/	
certificate name (CN)	Serial number (SN, hex, dec)
CN=OCSP SEAL-SIGN8-01	HEX: 35CF5B83568751FA DEC: 3877418423839838714

Table 5: „SIGN8 PKI QSEAL ECC“: 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 (QES-Seal-CA-02)	
/C=DE /O=SIGN8 GmbH/	
certificate name (CN)	Serial number (SN, hex, dec)

CN= SIGN8 GmbH QES SEAL CA 02 <i>TSL-registered</i>	HEX: 629D7A4480DCD113492E32517F46A000F6582621 DEC: 56299296354627793590291301012466760275352 0412193
Trust service certificate (OSCP-Service-Certificate)	
/C=DE /O=SIGN8 GmbH/	
certificate name (CN)	Serial number (SN, hex, dec)
CN=OCSP SEAL-SIGN8-02	HEX: 55648cb5e0d8a199 DEC: 6153197703684202905

Table 6: „SIGN8 PKI QSEAL RSA“: 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 (QES-Signing-CA-01)	

/C=DE /O=SIGN8 GmbH/	
certificate name (CN)	Serial number (SN, hex, dec)
CN=SIGN8 GmbH QES SIGNATURE CA 01 <i>TSL-registered</i>	HEX: 629D7A4480DCD113492E32517F46A000F658261E DEC: 56299296354627793590291301012466760275352 0412190
Trust service certificate (OSCP-Service-Certificate)	
/C=DE /O=SIGN8 GmbH/	
certificate name (CN)	Serial number (SN, hex, dec)
CN=OCSP SIGNATURE-SIGN8-01	HEX: 74DAFDB7F36B5AA3 DEC: 8420321419827305123

Table 7: „SIGN8 PKI QES ECC“: 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 (QES-Signing-CA-02)	
/C=DE /O=SIGN8 GmbH/	
certificate name (CN)	Serial number (SN, hex, dec)
CN=SIGN8 GmbH QES SIGNATURE CA 02 <i>TSL-registered</i>	HEX: 629D7A4480DCD113492E32517F46A000F6582620 DEC: 56299296354627793590291301012466760275352 0412192
Trust service certificate (OCSP-Service-Certificate)	
/C=DE /O=SIGN8 GmbH/	
certificate name (CN)	Serial number (SN, hex, dec)
CN=OCSP SIGNATURE-SIGN8-02	HEX: 3890DF25D50A451E DEC: 4076003016351302942

Table 8: „SIGN8 PKI QES RSA“: 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 VDG³, 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.

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

³ 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 (BGBl. I S. 2745, Stand: 18.07.2017)

3. Certification Programme

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

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

4. Assessment of the TSP's Qualified Operation

The current basic documents of the trust service provider "SIGN8 GmbH" - version 1.0 as of 26.07.2022 of the Service Provision Practice Statement (not publicly available) and version 1.0 as of 26.07.2022 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 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: http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC

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

Table 9: Trust services provided in compliance with eIDAS Regulation

These determinations also apply to the fulfilment of applicable requirements of the VDG and the VDV⁴.

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 9 above. Therefore, the present Conformity Certificate covers the operation of the qualified trust services listed in chap. 4, Table 9 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.

⁴ Vertrauensdiensteverordnung vom 15. Februar 2019 (BGBl. I S. 114; Stand: 15.02.2019)

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	
Nect Robo-Ident	<p>identification of <i>natural</i> persons</p> <p>i) in compliance with eIDAS Art. 24.1 (d)</p> <p>ii) confirmed assurance level: '<i>substantial</i>' acc. to Commission Implementing Regulation (EU) 2015/1502: <i>not applicable</i></p> <p>iii) in compliance with VDG § 11 para. 3</p>	Nect GmbH	Großer Burstah 21 20457 Hamburg, Germany	DSC.856.07.2 021	14.07.2023	non-exclusive
Verimi Identitätsfeststellungsdienst	<p>identification of <i>natural</i> persons</p> <p>i) in compliance with eIDAS Art. 24.1 (d)</p> <p>ii) confirmed assurance level: '<i>substantial</i>' acc. to Commission Implementing Regulation (EU) 2015/1502: <i>not applicable</i></p>	Verimi GmbH	Oranienstraße 91, 10969 Berlin, Germany	TÜViT 97188.22	26.06.2024	non-exclusive

6. Summary and Notes

1. The current basic documents of the trust service provider "SIGN8 GmbH"
 - version 1.0 as of 26.07.2022 of the Service Provision Practice Statement (not publicly available), and
 - version 1.0 as of 26.07.2022 of the Certificate Practice Statement (publicly available)

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

This determination also applies to the fulfilment of applicable requirements of the VDG and the VDV.

2. The trust service provider „SIGN8 GmbH“ operates the trust services listed in chap. 4, Table 9 above in compliance with the relevant requirements of the current version of eIDAS Regulation.
This determination also applies to the fulfilment of applicable requirements of the VDG and the VDV.
3. The present Conformity Certificate TelekomSecurity.031.0283.09.2022 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.031.0283.09.2022 is valid for the basic documents listed in para. 1 above up to and including 29.09.2024.
This validity period (that is, the maximum possible duration of TSP operation in compliance with eIDAS Regulation) results from the specification of 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.031.0283.09.2022

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>