CERTIFICATE

This is to certify that

Siemens AG
Siemens Certification Authority

Werner-von-Siemens-Straße 1
80333 München
Germany

has implemented the specification listed below for the following certification services.
This certificate is only valid in combination with the respective report.

Scope:
Siemens Certification Authority / Trust Service Provider (TSP)

Consisting of:

Root-CAs
ZZZZZZA1 Siemens Root CA V3.0 2016
ZZZZZZV1 Siemens Root CA V2.0 2013
ZZZZZZV0 Siemens Internet CA V1.0 2011

Issuing-CAs
See the annex of this Certificate.

An audit of the certification service, documented in a report, provided evidence that the requirements of the following specification have been fulfilled. The audit was conducted on 24 February 2020 to 27 February 2020 covering the audit period 28 February 2019 to 27 February 2020. It was a full-surveillance period-of-time audit covering all aspects of the standard performed by the lead auditor Mr. Jens Nicolaysen.

ETSI EN 319 401 V2.2.1
ETSI EN 319 411-1 V1.2.2

Certificate registration no.	500986 ETSI
Date of certification	2020-04-01
Valid until	2021-03-31

DQS GmbH

Markus Bleher
Managing Director

Annex to certificate
Registration No. Fehler! Verweisquelle konnte nicht gefunden werden.

Siemens AG
Siemens Certification Authority

Werner-von-Siemens-Straße 1
80333 München
Germany

Assessment Requirements
The audit requirements are defined by the following standards:

- ETSI EN 319 401 “Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers” version V2.2.1 dated 2018-04
- ETSI EN 319 411-1 “Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements” version V1.2.2 dated 2018-04
- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates of the CA/Browser Forum version 1.6.7 dated 2019-12-19
- CA / Browser Forum Network and Certificate System Security Requirements in version 1.3 dated 2019-09-26

The following table lists the currently operated Issuing CAs as well as the requirements upon their issued certificates according to [ETSI EN TS 319 411-1] including the respective secure devices.

Issuing CA		Requirements for issued certificates						
		ETSI quality level				Secure device		
	Expiry date	NCP	NCP+	OVCP	DVCP	Smart-Card	Smart-Phone	NwSC
ZZZZZZA2 Siemens Issuing CA EE Auth 2016	2022-08-04		X			X		
ZZZZZZA3 Siemens Issuing CA EE Enc 2016	2022-08-04		X			X	X	X
ZZZZZZA4 Siemens Issuing CA Intranet Code Signing 2016	2022-07-22	X						
ZZZZZZA5 Siemens Issuing CA Multipurpose 2016	2022-08-04	X						
ZZZZZZA6 Siemens Issuing CA Medium Strength Authentication 2016	2022-08-04	X						
ZZZZZZA7 Siemens Issuing CA Intranet Server 2016	2022-07-22	X		X	X			
ZZZZZZB7 Siemens Issuing CA Intranet Server 2017	2023-06-27	X		X	X			
ZZZZZZA8 Siemens Issuing CA Internet Code Signing 2016	2022-07-22	X						
ZZZZZZB9 Siemens Issuing CA Class Internet Server 2017	2023-07-11	X		X	X			
ZZZZZZAD Siemens Issuing CA EE Network Smartcard Auth 2016	2022-08-04		X					X
ZZZZZZYD Siemens Issuing CA EE Network Smartcard Auth 2015 **(expired)**	2019-12-02		X					X
ZZZZZZAB Siemens Issuing CA MSA	2022-07-20	X						

Annex to certificate
Registration No. Fehler! Verweisquelle konnte nicht gefunden werden.

Siemens AG
Siemens Certification Authority

Werner-von-Siemens-Straße 1
80333 München
Germany

Issuing CA		Requirements for issued certificates						
		ETSI quality level				Secure device		
	Expiry date	NCP	NCP+	OVCP	DVCP	Smart-Card	Smart-Phone	NwSC
Impersonalized Entities 2016								
ZZZZZZY2 Siemens Issuing CA EE Auth 2013 **(expired)**	2019-12-02		X			X		
ZZZZZZY3 Siemens Issuing CA EE Enc 2013 **(expired)**	2019-12-02		X			X	X	X
ZZZZZZY4 Siemens Issuing CA Intranet Code Signing 2013 **(expired)**	2019-12-02	X						
ZZZZZZY5 Siemens Issuing CA Multipurpose 2013 **(expired)**	2019-12-02	X						
ZZZZZZY6 Siemens Issuing CA Medium Strength Authentication 2013 **(expired)**	2019-12-02	X						
ZZZZZZY7 Siemens Issuing CA Intranet Server 2013 **(expired)**	2019-12-02	X		X	X			
ZZZZZZY8 Siemens Issuing CA Internet Code Signing 2013 **(expired)**	2019-12-02	X						
ZZZZZZYB Siemens Issuing CA MSA Impersonalized Entities 2013 **(expired)**	2019-12-02	X						

Audit Objects
The audit object is characterized by the certification information of the reviewed TSP:

TSP Policy Documents
- Certificate Policy in version 1.11
- Certification Practice Statement Root CA in version 1.8
- Certification Practice Statement Issuing CA in version 1.11

Annex to certificate
Registration No. Fehler! Verweisquelle konnte nicht gefunden werden.

Siemens AG
Siemens Certification Authority

Werner-von-Siemens-Straße 1
80333 München
Germany

Root-CAs

ZZZZZZA1 Siemens Root CA V3.0 2016
SHA256
56DCCD96F303DA826D8953E167A8902ECBC0734DF41B9B57B3F1201CA6E4A144
CN = Siemens Root CA V3.0 2016
OU = Siemens Trust Center
SERIALNUMBER = ZZZZZZA1
O = Siemens
L = Muenchen
S = Bayern
C = DE

ZZZZZZV1 Siemens Root CA V2.0 2013
SHA256
4350F26CB25429A0C7ACAD1128FED16D7D0B70CB24E24779CB86868099C611EA
CN = Siemens Trust Center Root-CA V2.0
OU = Copyright (C) Siemens AG 2011 All Rights Reserved
SERIALNUMBER = ZZZZZZV1
O = Siemens
C = DE

Intermediate-CA (treated as Root CA)

ZZZZZZV0 Siemens Internet CA V1.0 2011
SHA256
24E56F48604446D8A8373B43CA29D1A1C49772E5AABA8BA7C17662BD60DA8DF6
Renewed in 2016 as
67E5B507C861CE7180BC3DB7D37D2F5CAE755831E212E32225F6294694B2EA49
Renewed in 2016 as
3EBF5FFEC582D27C693D1BC30104A63BBBFC3652C78A95027E91B7F88DAC6345
CN = Siemens Internet CA V1.0
OU = Copyright (C) Siemens AG 2011 All Rights Reserved
SERIALNUMBER = ZZZZZZV0
O = Siemens
C = DE

Issuing-CAs

ZZZZZZA2 Siemens Issuing CA EE Auth 2016
SHA256
940D2F212A2A39CC84BD42D0F6DC4F7BA4C477E7A5A9922C96B9F5EC14E4A6C8
Renewed in 2018 as
5972B9BD471017D5F32705BEE915703626575F8B270A39C1C312C7F9246C10D4
CN = Siemens Issuing CA EE Auth 2016
OU = Siemens Trust Center
SERIALNUMBER = ZZZZZZA2
O = Siemens
L = Muenchen
S = Bayern
C = DE

Annex to certificate
Registration No. Fehler! Verweisquelle konnte nicht gefunden werden.

Siemens AG
Siemens Certification Authority

Werner-von-Siemens-Straße 1
80333 München
Germany

ZZZZZZY3 Siemens Issuing CA EE Enc 2013
SHA256
F5629F8E16AA288B21CF253225FAB8A9CE15C468781C1E74284079728EFF2FDA
CN = Siemens Issuing CA EE Auth 2013
OU = Copyright (C) Siemens AG 2013 All Rights Reserved
SERIALNUMBER = ZZZZZZY2
O = Siemens
C = DE

ZZZZZZA3 Siemens Issuing CA EE Enc 2016
SHA256
ABF3803CD2939E26803E52280A81F67C46C3E0EE75FCDBB1E30FB03A321ACFAD
CN = Siemens Issuing CA EE Enc 2016
OU = Siemens Trust Center
SERIALNUMBER = ZZZZZZA3
O = Siemens
L = Muenchen
S = Bayern
C = DE

ZZZZZZY3 Siemens Issuing CA EE Enc 2013
SHA256
F5629F8E16AA288B21CF253225FAB8A9CE15C468781C1E74284079728EFF2FDA
CN = Siemens Issuing CA EE Enc 2013
OU = Copyright (C) Siemens AG 2013 All Rights Reserved
SERIALNUMBER = ZZZZZZY3
O = Siemens
C = DE

ZZZZZZA4 Siemens Issuing CA Intranet Codesigning 2016
SHA256
BDCF0D60FC32966135971FF8EAD9CB7116400908B338E6C59B9AFDDADF087992
CN = Siemens Issuing CA Intranet Code Signing 2016
OU = Siemens Trust Center
SERIALNUMBER = ZZZZZZA4
O = Siemens
L = Muenchen
S = Bayern
C = DE

ZZZZZZY4 Siemens Issuing CA Intranet Codesigning 2013
SHA256
4F59D9D889B4137D15734C6053EBCE0DABFE0B02C84D2EAFB205C9BE71BBC379
CN = Siemens Issuing CA Intranet Code Signing 2013
OU = Copyright (C) Siemens AG 2013 All Rights Reserved
SERIALNUMBER = ZZZZZZY4
O = Siemens
C = DE

Annex to certificate
Registration No. Fehler! Verweisquelle konnte nicht gefunden werden.

Siemens AG
Siemens Certification Authority

Werner-von-Siemens-Straße 1
80333 München
Germany

ZZZZZZA5 Siemens Issuing CA Multipurpose 2016
SHA256
05BFB6605D48516A571BAF9A7FF75376130470DA5EE7FF684C2672EAA0C0C8AD
CN = Siemens Issuing CA Multi Purpose 2016
OU = Siemens Trust Center
SERIALNUMBER = ZZZZZZA5
O = Siemens
L = Muenchen
S = Bayern
C = DE

ZZZZZZY5 Siemens Issuing CA Multipurpose 2013
SHA256
89D2EBFBAFD59C6A1C83EC6C035316145704F895363370D015B8F62595A0497A
CN = Siemens Issuing CA Multipurpose 2013
OU = Copyright (C) Siemens AG 2013 All Rights Reserved
SERIALNUMBER = ZZZZZZY5
O = Siemens
C = DE

ZZZZZZA6 Siemens Issuing CA Medium Strength Authentication 2016
SHA256
42AB4D9F1809454EBEC245D8DB06FF61AA8289B05A263DFEE9662DAC91666043
CN = Siemens Issuing CA Medium Strength Authentication 2016
OU = Siemens Trust Center
SERIALNUMBER = ZZZZZZA6
O = Siemens
L = Muenchen
S = Bayern
C = DE

ZZZZZZY6 Siemens Issuing CA Medium Strength Authentication 2013
SHA256
A66872C6B167A6F1B7F73A22E57BC191AEBFFB1960E68FE8FC36090A29D07226
CN = Siemens Issuing CA Medium Strength Authentication 2013
OU = Copyright (C) Siemens AG 2013 All Rights Reserved
SERIALNUMBER = ZZZZZZY6
O = Siemens
C = DE

ZZZZZZB7 Siemens Issuing CA Intranet Server 2017
SHA256
0980FAA7AE6EFA163B9D3B74866172CFB0CA75BF65203D5E7F274C87804BBAF8
CN = Siemens Issuing CA Intranet Server 2017
OU = Siemens Trust Center
SERIALNUMBER = ZZZZZZB7
O = Siemens
L = Muenchen
S = Bayern
C = DE

Annex to certificate
Registration No. Fehler! Verweisquelle konnte nicht gefunden werden.

Siemens AG
Siemens Certification Authority

Werner-von-Siemens-Straße 1
80333 München
Germany

ZZZZZZA7 Siemens Issuing CA Intranet Server 2016
SHA256
BDCF0D60FC32966135971FF8EAD9CB7116400908B338E6C59B9AFDDADF087992
CN = Siemens Issuing CA Intranet Server 2016
OU = Siemens Trust Center
SERIALNUMBER = ZZZZZZA7
O = Siemens
L = Muenchen
S = Bayern
C = DE

ZZZZZZY7 Siemens Issuing CA Intranet Server 2013
SHA256
E00C8674B22253644A81AB7ECB6C9594D3E696B9F04F8E23E962217D15317A15
CN = Siemens Issuing CA Intranet Server 2013
OU = Issuing CA for Siemens non-personalized SSL/TLS-based End Entities
OU = Copyright (C) Siemens AG 2013 All Rights Reserved
SERIALNUMBER = ZZZZZZY7
O = Siemens
C = DE

ZZZZZZAB Siemens Issuing CA MSA Impersonalized Entities 2016
SHA256
C4D7560E45A5C55B32181A51427A96421921D3F581496744A25229BB348B356A
CN = Siemens Issuing CA MSA Impersonalized Entities 2016
OU = Siemens Trust Center
SERIALNUMBER = ZZZZZZAB
O = Siemens
L = Muenchen
S = Bayern
C = DE

ZZZZZZYB Siemens Issuing CA MSA Impersonalized Entities 2013
SHA256
9B124DAA6A246E9E396602EC0E37DE2D863561D115FC3363B1FC6A13C0D20059
CN = Siemens Issuing CA MSA Impersonalized Entities 2013
OU = Issuing CA for Siemens MSA Impersonalized Entities 2013
OU = Copyright (C) Siemens AG All Rights Reserved
SERIALNUMBER = ZZZZZZYB
O = Siemens
C = DE

ZZZZZZA8 Siemens Issuing CA Internet Code-Signing 2016
SHA256
1B046535378E07D10ACDAA24EEFCE20420BB9A596114EB475CA696357753E925
CN = Siemens Issuing CA Internet Code Signing 2016
OU = Siemens Trust Center
SERIALNUMBER = ZZZZZZA8
O = Siemens
L = Muenchen
S = Bayern
C = DE

Annex to certificate
Registration No. Fehler! Verweisquelle konnte nicht gefunden werden.

Siemens AG
Siemens Certification Authority

Werner-von-Siemens-Straße 1
80333 München
Germany

ZZZZZZY8 Siemens Issuing CA Internet Code-Signing 2013
SHA256
4233DF529F97B932C8D3F3AEF0C6DDAB4902B4287910478EDD3C8820052C1445
Renewed in 2015 as
66A66484E58EC8EF0B25C20F6726856559C666E1E65E0D8D14BB1981A69E6231
CN = Siemens Issuing CA Internet Code Signing 2013
OU = Copyright (C) Siemens AG 2013 All Rights Reserved
SERIALNUMBER = ZZZZZZY8
O = Siemens
C = DE

ZZZZZZB9 Siemens Issuing CA Internet Server 2017
SHA256
7D33AE618CD62553377D253D2EBCA285D84E98A924D89F98D4BE4FEE31F92AA8
CN = Siemens Issuing CA Internet Server 2017
OU = Siemens Trust Center
SERIALNUMBER = ZZZZZZB9
O = Siemens
L = Muenchen
S = Bayern
C = DE

ZZZZZZAD Siemens Issuing CA EE Network Smartcard Auth 2016
SHA256
37D220A6C7522799021191349C183F917BE1BE8626CF926B0FD6E0A8681EE031
CN = Siemens Issuing CA EE Network Smartcard Auth 2016
OU = Siemens Trust Center
SERIALNUMBER = ZZZZZZAD
O = Siemens
L = Muenchen
S = Bayern
C = DE

ZZZZZZYD Siemens Issuing CA EE Network Smartcard Auth 2015
SHA256
9C00120592C15BFDF352869AB007198F3A87874AEF618DA4F2130F187A508B22
CN = Siemens Issuing CA EE Network Smartcard Auth 2015
OU = Copyright (C) Siemens AG 2015 All Rights Reserved
SERIALNUMBER = ZZZZZZYD
O = Siemens
C = DE

Annex to certificate
Registration No. Fehler! Verweisquelle konnte nicht gefunden werden.

Siemens AG
Siemens Certification Authority

Werner-von-Siemens-Straße 1
80333 München
Germany

Audit results

- The audit object fulfills all applicable requirements from the audit criteria.
- The certification requirements as defined in the certification assumptions are fulfilled.
- All requirements for a TSP Practice according to the standards together with the therein demanded measures are implemented in terms of the selected Certificate Policy and Certification Practice Statements.
- The TSP provides the certification services according to the definitions of the Certification Practice Statements.
- The Certificate Policy is part of an effective certificate policy management including regulations concerning responsibilities, communication and PDCA cycle.
- The TSP ensures that certificates are only issued to employees, affiliates and websites of the Siemens cooperation following the requirements of the standards. Due to this fact some requirements of the standards are fulfilled by other parts of the cooperation and not directly by the TSP.
- The TSP stopped issuance of public trusted TLS and CodeSigning certificates on 15 October 2019.
- In the audit all certificates were checked for mis-issuance. No mis-issued certificate was found. Two certificates with with “Warnings” were issued: https://crt.sh/?id=1776913772 & https://crt.sh/?id=1762596107 . The warnings were immediately detected, and the certificates were revoked within 24 hours. A root cause analysis was performed and let to an adaptation of the software.

Accredited body

The audit was performed by DQS GmbH, August-Schanz-Straße 21, 60433 Frankfurt am Main, Germany

Annex to certificate
Registration No. Fehler! Verweisquelle konnte nicht gefunden werden.

Siemens AG
Siemens Certification Authority

Werner-von-Siemens-Straße 1
80333 München
Germany

Summary of audit requirements
The ETSI specifications contain the following requirements:

1 Certification Practice Statement (CPS)
The TSP has a presentation of its practices and policies.

2 Public Key Infrastructure – key management life cycle
The TSP ensures that CA keys are created under controlled conditions.

The TSP ensures that private CA keys are treated confidentially and that their integrity is maintained.

The TSP ensures that the integrity and authenticity of the (published) CA public keys together with all associated parameters are preserved during their transfer to relying parties. If the key for electronic signatures is applied in the terms of guideline 1999/93/EG the TSP is not entitled to store private signature keys of the certification owner (subject) in a way enabling key escrow. If a copy of the key remains at the TSP, the TSP takes care that the private key remains secure and is only made accessible to entitled persons.

The TSP ensures that private CA signature keys are not used improperly. The TSP ensures that private CA signature keys may not be used beyond the end of their lifecycle. In case of NCP+ the TSP ensures that the security of cryptographic devices is warranted during their complete lifecycle.

The TSP ensures that every key created by the TSP for a certificate owner (subject) is safely generated and that the non-disclosure of the certificate owner's private key is guaranteed.

In case of NCP+ the TSP assures that the handover of the secure user unit to the certificate owner (subject) happens in a secure way, in case this user unit is provided by the TSP.

3 Public Key Infrastructure – certificate management lifecycle
The TSP ensures that the identification confirmation of a participant (subscriber) and of a certificate owner (subject) as well as the correctness of their names and their related data are either checked as part of the defined service or proved by attestations from appropriate and licensed sources. It also ensures that applications for a certificate take place in a correct and authorized way, completely according to the collected proofs respectively attestations.

The TSP ensures that the certification applications of certificate owners (subject), who were registered before at the same TSP, are authorized completely, correctly and orderly. This includes new key generations (rekey) after a blocking or before the expiry date, or updates due to attribute changes of the certificate owner (subject).

The TSP ensures that the certificates are handed out in a secure way so that their authenticity is maintained.

The TSP ensures that the legal terms and conditions are made available to the participants (subscriber) and to the relying parties.

The TSP ensures that certificates are made available to the participants (subscriber), certificate owners (subject) and relying parties to the extent necessary.

Siemens AG
Siemens Certification Authority

Werner-von-Siemens-Straße 1
80333 München
Germany

The TSP ensures that certificates are blocked at short notice using authorized and verified blocking queries.

4 TSP Management and Operation
The TSP ensures that the applied administrative and management methods are appropriate and corresponding to acknowledged standards.

The TSP ensures that the objects and information worthy of protection receive an appropriate protection.

The TSP ensures that the employees and the hiring procedures amplify and support the TSP company's trustability.

The TSP ensures that physical access to critical services is controlled and that the physical risks for the objects worthy of protection are minimized.

The TSP ensures that the TSP's systems are operated safely, according to specification and with a minimal default risk.

The TSP ensures that the access to the TSP's systems is restricted to appropriate, authorized persons.

The TSP ensures to use trustworthy systems and products that are protected against modifications.

The TSP ensures that in case of a catastrophe (including a compromise of the private CA signature key) the operation is restored as soon as possible.

The TSP ensures that in case of a cessation of the TSP's operation the potential interference of users (subscriber) and relying parties is minimized and that the continued maintenance of records that are required as proof of certification in legal proceedings is given.

The TSP ensures that statutory requirements are met.

The TSP ensures that all relevant information of a certificate is recorded for a reasonable period of time, especially for the purpose of proof of certification in legal proceedings.

The TSP ensures that the European data privacy regulations are being followed.

5 Organization
The TSP ensures that its organization is reliable.

Annex to certificate
Registration No. Fehler! Verweisquelle konnte nicht gefunden werden.

Siemens AG
Siemens Certification Authority

Werner-von-Siemens-Straße 1
80333 München
Germany

6 Certification Body

The Certification Body

DQS GmbH
August-Schanz-Straße 21
60433 Frankfurt am Main
Germany

is accredited by the German accreditation body

DAkkS (Deutsche Akkreditierungsstelle GmbH)
Spittelmarkt 10
10117 Berlin
Germany