CERTIFICATE

This is to certify that

Siemens AG
Siemens Certification Authority

Werner-von-Siemens-Straße 1
80333 München

has implemented the specification listed below for the following certification services.

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 26th – 28th February 2018 covering the audit period 22nd February 2017 to 25th February 2018. 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
ETSI EN 319 411-1

Certificate registration no.	500986 ETSI
Date of certification	1st March 2018
Valid until	28th February 2021

DQS GmbH

Stefan Heinloth

Stefan Heinloth
Managing Director

Annex to Certificate
Registration No. 500986 ETSI

Siemens AG
Siemens Certification Authority

Assessment Requirements

The audit requirements are defined by the following standards:

- For ETSI EN 319 401 “Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers” the latest published version (V2.1.1 | 2016-02) as well as the latest draft version (V2.2.1 | 2018-02) were taken into account.
- For ETSI EN 319 411-1 “Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements” the latest published version (V1.1.1 | 2016-02) as well as the latest draft version (V1.2.1 | 2018-02) were taken into account.
- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates of the CA/Browser Forum in version 1.5.4
- CA / Browser Forum Network and Certificate System Security Requirements in version 1.1

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	4 / 8 / 2022		X			X		
ZZZZZZA3 Siemens Issuing CA EE Enc 2016	4 / 8 / 2022		X			X	X	X
ZZZZZZA4 Siemens Issuing CA Intranet Code Signing 2016	20 / 7 / 2022	X						
ZZZZZZA5 Siemens Issuing CA Multipurpose 2016	4 / 8 / 2022	X						
ZZZZZZA6 Siemens Issuing CA Medium Strength Authentication 2016	4 / 8 / 2022	X						
ZZZZZZA7 Siemens Issuing CA Intranet Server 2016	20 / 7 / 2022	X		X	X			
ZZZZZZB7 Siemens Issuing CA Intranet Server 2017	27 / 6 / 2023	X		X	X			
ZZZZZZA8 Siemens Issuing CA Internet Code Signing 2016	20 / 7 / 2022	X						
ZZZZZZA9 Siemens Issuing CA Class Internet Server 2016 **(revoked)**	5 / 8 / 2022	X		X	X			
ZZZZZZB9 Siemens Issuing CA Class Internet Server 2017	11 / 7 / 2023	X		X	X			
ZZZZZZAD Siemens Issuing CA EE Network Smartcard Auth 2016	4 / 8 / 2022		X					X
ZZZZZZYD Siemens Issuing CA EE Network Smartcard Auth 2015	2 / 12 / 2019		X					X
ZZZZZZAB Siemens Issuing CA MSA Impersonalized Entities 2016	20 / 7 / 2022	X						
ZZZZZZY2 Siemens Issuing CA EE Auth 2013	2 / 12 / 2019		X			X		

Annex to Certificate
Registration No. 500986 ETSI

Siemens AG
Siemens Certification Authority

Issuing CA		Requirements for issued certificates						
		ETSI quality level				Secure device		
	Expiry date	NCP	NCP+	OVCP	DVCP	Smart-Card	Smart-Phone	NwSC
ZZZZZZY3 Siemens Issuing CA EE Enc 2013	2 / 12 / 2019		X			X	X	X
ZZZZZZY4 Siemens Issuing CA Intranet Code Signing 2013	2 / 12 / 2019	X						
ZZZZZZY5 Siemens Issuing CA Multipurpose 2013	2 / 12 / 2019	X						
ZZZZZZY6 Siemens Issuing CA Medium Strength Authentication 2013	2 / 12 / 2019	X						
ZZZZZZY7 Siemens Issuing CA Intranet Server 2013	2 / 12 / 2019	X		X	X			
ZZZZZZY8 Siemens Issuing CA Internet Code Signing 2013	2 / 12 / 2019	X						
ZZZZZZY9 Siemens Issuing CA Class Internet Server 2013 **(indirectly revoked)**	2 / 12 / 2019	X		X	X			
ZZZZZZYB Siemens Issuing CA MSA Impersonalized Entities 2013	2 / 12 / 2019	X						

Audit Objects

The audit object is characterized by the certification information of the reviewed TSP's:

TSP Policy Documents

- Certificate Policy in version 1.7
- Certification Practice Statement Root CA in version 1.5
- Certification Practice Statement Issuing CA in version 1.7

Root-CAs

ZZZZZZA1 Siemens Root CA V3.0 2016

SHA256:
56:DC:CD:96:F3:03:DA:82:6D:89:53:E1:67:A8:90:2E:CB:C0:73:4D:F4:1B:9B:57:B3:F1:20:1C:A6:E4:A1:44

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

SHA1: f9 5b e7 8f e9 4b cf 14 d5 b8 4f 33 7e ec 67 c0 c9 d8 36 5d

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)

Annex to Certificate
Registration No. 500986 ETSI

Siemens AG
Siemens Certification Authority

ZZZZZZV0 Siemens Internet CA V1.0 2011
SHA256:
3E:BF:5F:FE:C5:82:D2:7C:69:3D:1B:C3:01:04:A6:3B:BB:FC:36:52:C7:8A:95:02:7E:91:B7:F8:8D:AC:63:45

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:
94:0D:2F:21:2A:2A:39:CC:84:BD:42:D0:F6:DC:4F:7B:A4:C4:77:E7:A5:A9:92:2C:96:B9:F5:EC:14:E4:A6:C8
CN = Siemens Issuing CA EE Auth 2016
OU = Siemens Trust Center
SERIALNUMBER = ZZZZZZA2
O = Siemens
L = Muenchen
S = Bayern
C = DE

ZZZZZZY2 Siemens Issuing CA EE Auth 2013
SHA1: 0f 22 45 55 cc c7 55 c7 c0 1e 6d 25 02 89 2e ef 19 65 b8 b2
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:
AB:F3:80:3C:D2:93:9E:26:80:3E:52:28:0A:81:F6:7C:46:C3:E0:EE:75:FC:DB:B1:E3:0F:B0:3A:32:1A:CF:AD
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
SHA1: 3c a4 c2 47 74 ae 44 69 6b ad 44 48 61 7a 1b 06 e0 29 e3 91
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:
BD:CF:0D:60:FC:32:96:61:35:97:1F:F8:EA:D9:CB:71:16:40:09:08:B3:38:E6:C5:9B:9A:FD:DA:DF:08:79:92
CN = Siemens Issuing CA Intranet Code Signing 2016
OU = Siemens Trust Center
SERIALNUMBER = ZZZZZZA4
O = Siemens
L = Muenchen
S = Bayern
C = DE

Annex to Certificate
Registration No. 500986 ETSI

Siemens AG
Siemens Certification Authority

ZZZZZZY4 Siemens Issuing CA Intranet Codesigning 2013

SHA256:
4F:59:D9:D8:89:B4:13:7D:15:73:4C:60:53:EB:CE:0D:AB:FE:0B:02:C8:4D:2E:AF:B2:05:C9:BE:71:BB:C3:79
CN = Siemens Issuing CA Intranet Code Signing 2013
OU = Copyright (C) Siemens AG 2013 All Rights Reserved
SERIALNUMBER = ZZZZZZY4
O = Siemens

C = DE

ZZZZZZA5 Siemens Issuing CA Multipurpose 2016

SHA256:
05:BF:B6:60:5D:48:51:6A:57:1B:AF:9A:7F:F7:53:76:13:04:70:DA:5E:E7:FF:68:4C:26:72:EA:A0:C0:C8:AD
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

SHA1: 7b 29 bb cc 25 ab ed ef 2f 17 80 a1 53 88 e9 17 3c 2a 86 25
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:
42:AB:4D:9F:18:09:45:4E:BE:C2:45:D8:DB:06:FF:61:AA:82:89:B0:5A:26:3D:FE:E9:66:2D:AC:91:66:60:43
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

SHA1: c5 34 5c 0d 1d de 11 f2 b0 44 5c 7e 82 c3 f3 76 88 83 ab a0
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:
09:80:FA:A7:AE:6E:FA:16:3B:9D:3B:74:86:61:72:CF:B0:CA:75:BF:65:20:3D:5E:7F:27:4C:87:80:4B:BA:F8
CN = Siemens Issuing CA Intranet Server 2017
OU = Siemens Trust Center
SERIALNUMBER = ZZZZZZB7
O = Siemens
L = Muenchen
S = Bayern
C = DE

ZZZZZZA7 Siemens Issuing CA Intranet Server 2016

SHA256:

BD:CF:0D:60:FC:32:96:61:35:97:1F:F8:EA:D9:CB:71:16:40:09:08:B3:38:E6:C5:9B:9A:FD:DA:DF:08:79:92
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:
E0:0C:86:74:B2:22:53:64:4A:81:AB:7E:CB:6C:95:94:D3:E6:96:B9:F0:4F:8E:23:E9:62:21:7D:15:31:7A:15
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: C4:D7:56:0E:45:A5:C5:5B:32:18:1A:51:42:7A:96:42:19:21:D3:F5:81:49:67:44:A2:52:29:BB:34:8B:35:6A
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
SHA1: 0b 6b b2 27 b4 74 27 43 cf 9c da 06 e8 fe 12 53 52 02 0c 38
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:
1B:04:65:35:37:8E:07:D1:0A:CD:AA:24:EE:FC:E2:04:20:BB:9A:59:61:14:EB:47:5C:A6:96:35:77:53:E9:25
CN = Siemens Issuing CA Internet Code Signing 2016
OU = Siemens Trust Center
SERIALNUMBER = ZZZZZZA8
O = Siemens
L = Muenchen
S = Bayern
C = DE

ZZZZZZY8 Siemens Issuing CA Internet Code-Signing 2013
SHA256:
4F:59:D9:D8:89:B4:13:7D:15:73:4C:60:53:EB:CE:0D:AB:FE:0B:02:C8:4D:2E:AF:B2:05:C9:BE:71:BB:C3:79
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:
7D:33:AE:61:8C:D6:25:53:37:7D:25:3D:2E:BC:A2:85:D8:4E:98:A9:24:D8:9F:98:D4:BE:4F:EE:31:F9:2A:A8
CN = Siemens Issuing CA Internet Server 2017

OU = Siemens Trust Center
SERIALNUMBER = ZZZZZZB9
O = Siemens
L = Muenchen
S = Bayern
C = DE

ZZZZZZA9 Siemens Issuing CA Internet Server 2016 – revoked (15th December 2017)
SHA256:
C9:78:16:36:8C:2B:7A:46:08:B3:34:4D:BE:68:48:D8:BD:12:12:60:C2:F7:9D:AC:8A:C9:0C:AE:17:C8:E5:7C
CN = Siemens Issuing CA Internet Server 2016
OU = Siemens Trust Center
SERIALNUMBER = ZZZZZZA9
O = Siemens
L = Muenchen
S = Bayern
C = DE

ZZZZZZY9 Siemens Issuing CA Internet Server 2013 – revoked (4th October 2017)
SHA256:
E0:0C:86:74:B2:22:53:64:4A:81:AB:7E:CB:6C:95:94:D3:E6:96:B9:F0:4F:8E:23:E9:62:21:7D:15:31:7A:15
CN = Siemens Issuing CA Class Internet Server 2013
OU = Copyright (C) Siemens AG 2013 All Rights Reserved
SERIALNUMBER = ZZZZZZY9
O = Siemens
C = DE

ZZZZZZAD Siemens Issuing CA EE Network Smartcard Auth 2016
SHA256:
37:D2:20:A6:C7:52:27:99:02:11:91:34:9C:18:3F:91:7B:E1:BE:86:26:CF:92:6B:0F:D6:E0:A8:68:1E:E0:31
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
SHA1: 6d 55 48 5a 7e b2 12 71 f5 a9 c3 ea 4b ea e9 ae a5 ef 40 08
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. 500986 ETSI

Siemens AG
Siemens Certification Authority

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.

Accredited body

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

Annex to Certificate
Registration No. 500986 ETSI

Siemens AG
Siemens Certification Authority

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.

6 Certification Body

The Certification Body

DQS GmbH
August-Schanz-Straße 21
60433 Frankfurt am Main
Germany
is accredited by the German accreditation boddy

DAkkS (Deutsche Akkreditierungsstelle GmbH)
Spittelmarkt 10
10117 Berlin
Germany