Certificate

The certification body of TÜV Informationstechnik GmbH hereby awards this certificate to the company

DATEV eG
Paumgartnerstraße 6 - 14
90329 Nürnberg, Germany

to confirm that its certification services

DATEV STD, INT und BT CAs

fulfil all requirements defined in the technical specification

ETSI TS 102 042 V2.2.1. (2011-12) policy NCP+.

The appendix to the certificate is part of the certificate and consists of 9 pages.

The certificate is valid only in conjunction with the respective evaluation report until 2013-04-30.

ETSI TS 102 042 CA6716.12 TÜViT® 2012 Trusted Site
Voluntary Validation

Certificate-Registration-No.:
TUVIT-CA6716.12

Essen, 2012-03-28

Joachim Faulhaber
Deputy Head of Certification Body

TÜV Informationstechnik GmbH
Member of TÜV NORD Group
Langemarckstr. 20
45141 Essen, Germany
www.certuvit.de

Deutscher Akkreditierungs Rat
DAR
DGA-ZE-014/99

Certification System

The certification body of TÜV Informationstechnik GmbH is accredited by "DAkkS Deutsche Akkreditierungsstelle GmbH" according to DIN EN 45011 for the scope IT security product certification. The certification body performs its certification on the basis of the following accredited product certification system:

- German document: "Zertifizierungsschema für Zertifikate des akkreditierten Bereichs der Zertifizierungsstelle der TÜV Informationstechnik GmbH", version 1.2 as of 2011-01-28, TÜViT GmbH

Evaluation Report

- "Evaluation Report – Surveillance On-Site Inspection – ETSI TS 102 042", Version 2.1 as of 2012-03-26, TÜViT GmbH

Evaluation Requirements

The evaluation requirements are defined in the technical specification ETSI TS 102 042:

- ETSI TS 102 042 V2.2.1 (2011-12): "Electronic Signatures and Infrastructures (ESI); Policy Requirements for certification authorities issuing public key certificates", Version 2.2.1, 2011-12, European Telecommunications Standards Institute

The applicable ETSI Certificate Policy is:

- NCP+: Normalized Certificate Policy requiring a secure user device

Evaluation Target

The target of evaluation is characterized by the certificate information of the inspected CA:

DATEV STD CA:

Root CA (Issuer of the CA certificate): CN = CA DATEV STD 01	
Name of CA (as in certificate)	**serial number of the certificate**
CN = CA DATEV STD 01	6b 1f 36 32 18 9d 2d 6f db ca 19 48 6f d4 14 0b

Root CA (Issuer of the CA certificate): CN = CA DATEV STD 99	
Name of CA (as in certificate)	**serial number of the certificate**
CN = CA DATEV STD 99	51 f4 3e cc ca bf 88 c7 12 c3 28 86 f2 34 1c 82

Root CA (Issuer of the CA certificate): CN = CA DATEV STD 02	
Name of CA (as in certificate)	**serial number of the certificate**
CN = CA DATEV STD 02	54 a2 e4 95 b6 32 91 18 1c db 99 ca ac 7d 9f a5

Root CA (Issuer of the CA certificate): CN = CA DATEV STD 98	
Name of CA (as in certificate)	**serial number of the certificate**
CN = CA DATEV STD 98	6e c7 50 45 3f 16 c1 8c 84 02 ff c6 ad eb 1b b0

DATEV INT CA:

Root CA (Issuer of the CA certificate): CN = CA DATEV INT 01	
Name of CA (as in certificate)	**serial number of the certificate**
CN = CA DATEV INT 01	7f 2a f8 38 ea d3 1b f0 2d e3 20 f6 eb 50 86 06

Root CA (Issuer of the CA certificate): CN = CA DATEV INT 99	
Name of CA (as in certificate)	**serial number of the certificate**
CN = CA DATEV INT 99	53 96 97 38 b7 f0 c3 cf ee e7 ce 9c 08 d3 5d 0c

Root CA (Issuer of the CA certificate): CN = CA DATEV INT 02	
Name of CA (as in certificate)	**serial number of the certificate**
CN = CA DATEV INT 02	6a 46 0a 83 f0 ba ab 9d 5c d9 48 4b b8 3f 33 59

Root CA (Issuer of the CA certificate): CN = CA DATEV INT 98	
Name of CA (as in certificate)	**serial number of the certificate**
CN = CA DATEV INT 98	61 11 9d 21 81 41 9b bd df d3 d5 8d d0 08 5c 52

DATEV BT CA:

Root CA (Issuer of the CA certificate): CN = CA DATEV BT 01	
Name of CA (as in certificate)	**serial number of the certificate**
CN = CA DATEV BT 01	68 c9 f4 d1 f0 6b 09 88 e8 96 9f 4f cf be 5c b3

Root CA (Issuer of the CA certificate): CN = CA DATEV BT 99	
Name of CA (as in certificate)	**serial number of the certificate**
CN = CA DATEV BT 99	40 14 f4 eb d1 4f 19 b4 94 44 eb ec 55 f0 2f fa

Root CA (Issuer of the CA certificate): CN = CA DATEV BT 02	
Name of CA (as in certificate)	**serial number of the certificate**
CN = CA DATEV BT 02	4f 61 6c 00 24 cc e3 1a a3 38 3b 3d c3 94 27 f5

Root CA (Issuer of the CA certificate): CN = CA DATEV BT 98	
Name of CA (as in certificate)	**serial number of the certificate**
CN = CA DATEV BT 98	74 16 2a 6b a5 45 b1 ad 9a 07 c0 d8 aa b4 ce 8d

together with the Certification Practice Statement (CPS) of the operator:

- German document: "Sicherheitsrichtlinien des Zertifizierungsdiensteanbieters DATEV – Certification Practise Statement,

Signatur- und Verschlüsselungszertifikate auf SmartCard / mIDentity", version 2.5 as of 2012-01-31, DATEV eG

Evaluation Result

- The target of evaluation fulfils all applicable evaluation requirements.
- The certification requirements defined in the certification system are fulfilled.

Summary of the Evaluation Requirements

The ETSI specification ETSI TS 102 042 contains the following requirements:

1 Certification Practice Statement (CPS)

The CA shall have a statement of the practices and procedures.

2 Public key infrastructure – Key management life cycle

The CA shall ensure that CA keys are generated in controlled circumstances.

The CA shall ensure that CA private keys remain confidential and maintain their integrity.

The CA shall ensure that the integrity and authenticity of the CA signature verification (public) key and any associated parameters are maintained during its distribution to relying parties.

If the subject's key is to be used for electronic signatures with the meaning of Directive 1999/93/EC, then the CA shall not hold the subject's private signing keys in a way which provides a backup decryption capability (commonly called key escrow).

If a copy of the subject's key is kept by the CA then the CA shall ensure that the private key is kept secret and only made available to appropriately authorized persons.

The CA shall ensure that CA private signing keys are not used inappropriately.

The CA shall ensure that CA private signing keys are not used beyond the end of their life cycle.

In case of NCP, the CA shall ensure the security of cryptographic device throughout its lifecycle.

The CA shall ensure that any subject keys, that it generates, are generated securely and the secrecy of the subject's private key is assured.

In case of NCP+, the CA shall ensure that if it issues to the subject secure user device this is carried out securely.

3 Public key infrastructure – Certificate Management life cycle

The CA shall ensure that evidence of subscriber's and subject's identification and accuracy of their names and associated data are either properly examined as part of the defined service or, where applicable, concluded through examination of attestations from appropriate and authorized sources, and that certificate requests are accurate, authorized and complete according to the collected evidence or attestation.

The CA shall ensure that requests for certificates issued to a subject who has previously been registered with the same CA are complete, accurate and duly authorized. This includes certificate renewals, rekey following revocation or prior to expiration, or update due to change to the subject's attributes.

The CA shall ensure that it issues certificates securely to maintain their authenticity.

The CA shall ensure that the terms and conditions are made available to subscribers and relying parties.

The CA shall ensure that certificates are made available as necessary to subscribers, subjects and relying parties.

The CA shall ensure that certificates are revoked in a timely manner based on authorized and validated certificate revocation requests.

4 CA management and operation

The CA shall ensure that administrative and management procedures are applied which are adequate and correspond to recognized standards.

The CA shall ensure that its assets and information receive an appropriate level of protection.

The CA shall ensure that personnel and hiring practices enhance and support the trustworthiness of the CA's operations.

The CA shall ensure that physical access to critical services is controlled and physical risks to its assets minimized.

The CA shall ensure that the CA systems are secure and correctly operated, with minimal risk of failure.

The CA shall ensure that CA system access is limited to properly authorized individuals.

The CA shall use trustworthy systems and products that are protected against modification.

The CA shall ensure in the event of a disaster, including compromise of the CA's private signing key, operations are restored as soon as possible.

The CA shall ensure that potential disruptions to subscribers and relying parties are minimized as a result of the cessation of the CA's services, and ensure continued maintenance of records required to provide evidence of certification for the purposes of legal proceedings.

The CA shall ensure compliance with legal requirements.

The CA shall ensure that all relevant information concerning a certificate is recorded for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings.

5 Organizational

The CA shall ensure that its organization is reliable.