

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH
bescheinigt hiermit dem Unternehmen

DATEV eG
Paumgartnerstraße 6 - 14
90329 Nürnberg

für die Zertifizierungsdienste

DATEV STD, INT und BT CAs

die Erfüllung aller Anforderungen der Spezifikation

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

Die Anlage zum Zertifikat ist Bestandteil des Zertifikats und besteht
aus 9 Seiten.

Dieses Zertifikat gilt nur in Verbindung mit dem zugehörigen
Prüfbericht und ist bis zum 30.04.2013 gültig.



Zertifikat-Registrier-Nr.:
TUVIT-CA6716.12

13

Essen, 28.03.2012

Joachim Faulhaber
stellv. Leiter Zertifizierungsstelle

TÜV Informationstechnik GmbH
Unternehmensgruppe TÜV NORD
Langemarckstraße 20
45141 Essen
www.certuivit.de

The logo for the Deutscher Akkreditierungs Rat (DAR) features the letters 'DAR' in a stylized, bold font. The 'D' is black, the 'A' is yellow, and the 'R' is red. Above the letters, it says 'Deutscher Akkreditierungs Rat'. Below the logo, the text 'DGA-ZE-014/99' is printed.

DGA-ZE-014/99

Zertifikat

Zertifizierungssystem

TÜV[®]

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH ist bei der „DAkkS Deutsche Akkreditierungsstelle GmbH“ für die Zertifizierung von Produkten im Bereich IT-Sicherheit nach DIN EN 45011 akkreditiert. Die Zertifizierungsstelle führt ihre Zertifizierungen auf der Basis des folgenden akkreditierten Produkt-Zertifizierungssystems durch:

- „Zertifizierungsschema für Zertifikate des akkreditierten Bereichs der Zertifizierungsstelle der TÜV Informationstechnik GmbH“, Version 1.2 vom 28.01.2011, TÜVIT GmbH

Prüfbericht

- Englisch Dokument: „Evaluation Report – Surveillance On-Site Inspection – ETSI TS 102 042, Version 2.1 vom 26.03.2012, TÜVIT GmbH

Prüfanforderungen

Die Prüfanforderungen sind in der technischen Spezifikation ETSI TS 102 042 definiert:

- 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

Die anwendbare ETSI Zertifizierungspolitik ist:

- NCP+: Erweiterte standardisierte Zertifizierungspolitik, die eine sichere Nutzereinheit fordert

Prüfgegenstand

Der Prüfgegenstand ist charakterisiert durch die Zertifikatsinformation zur untersuchten 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

zusammen mit dem Certification Practice Statement (CPS) des Betreibers:

- „Sicherheitsrichtlinien des Zertifizierungsdiensteanbieters DATEV – Certification Practise Statement, Signatur- und

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

Prüfergebnis

- Der Prüfgegenstand erfüllt alle anwendbaren Anforderungen aus den Prüfkriterien.
- Die im Zertifizierungssystem definierten Zertifizierungsvoraussetzungen sind erfüllt.

Zusammenfassung der Prüfanforderungen

Die ETSI Spezifikation ETSI TS 102 042 enthält folgende Anforderungen:

1 Certification Practice Statement (CPS)

Die CA hat eine Darstellung der Praktiken und der Verfahren.

2 Public Key Infrastructure - Schlüsselmanagement-Lebenszyklus

Die CA stellt sicher, dass CA Schlüssel unter kontrollierten Bedingungen erzeugt werden.

Die CA stellt sicher, dass private CA Schlüssel vertraulich bleiben und ihre Integrität beibehalten.

Die CA stellt sicher, dass die Integrität und Authentizität der (öffentlichen) CA Signaturprüfchlüssel und aller zugehörigen Parameter während ihrer Verteilung zu vertrauenden Parteien (relying party) beibehalten werden.

Wenn der Schlüssel für elektronische Signaturen in dem Sinne der Richtlinie 1999/93/EG angewandt wird, dann darf die CA private Signaturschlüssel des Zertifikatsinhabers (subject) nicht in einer Weise aufbewahren, die eine (Reserve-)Entschlüsselungsmöglichkeit bietet (gemeinhin als Key Escrow bezeichnet).

Wird eine Kopie des Schlüssels von der CA aufbewahrt, dann sorgt die CA dafür, dass der private Schlüssel geheim gehalten und nur entsprechend befugten Personen zur Verfügung gestellt wird.

Die CA stellt sicher, dass private CA Signaturschlüssel nicht unsachgemäß verwendet werden.

Die CA stellt sicher, dass private CA Signaturschlüssel nicht über das Ende ihres Lebenszyklus verwendet werden.

Im Falle von NCP stellt die CA sicher, dass die Sicherheit von kryptographischen Geräten während ihres gesamten Lebenszyklus gegeben ist.

Die CA stellt sicher, dass jeder Schlüssel, den sie für Zertifikatsinhaber (subject) erzeugt, sicher generiert wird und die Geheimhaltung des privaten Schlüssels des Zertifikatsinhabers sichergestellt ist.

Im Falle von NCP+ stellt die CA sicher, dass die Übergabe, sofern die sichere Nutzereinheit an den Zertifikatsinhaber (subject) übergeben wird, sicher erfolgt.

3 Public Key Infrastructure - Zertifikatsmanagement Lebenszyklus

Die CA stellt sicher, dass Nachweise der Identifizierung eines Teilnehmers (subscriber) und Zertifikatsinhabers (subject) sowie der Korrektheit ihrer Namen und die dazugehörigen Daten entweder richtig als Teil des definierten Service geprüft oder anhand von Bescheinigungen aus geeigneten und zugelassenen Quellen nachgewiesen werden und dass Zertifikatsanträge genau, autorisiert und vollständig gemäß den gesammelten Nachweisen bzw. Bescheinigung erfolgen.

Die CA stellt sicher, dass Zertifikatsanträge von Zertifikatsinhabern (subject), die zuvor bei der gleichen CA registriert wurden, vollständig, korrekt und berechtigt sind. Dies beinhaltet Zertifikatsverlängerungen, erneute Schlüsselgenerierung (rekey) nach Sperrung oder vor Ablauf der Gültigkeit oder Aktualisierung aufgrund Attributsänderungen des Zertifikatsinhabers (subject).

Die CA stellt sicher, dass Zertifikate sicher ausgegeben werden, so dass ihre Authentizität erhalten bleibt.

Die CA stellt sicher, dass die allgemeinen Geschäftsbedingungen den Teilnehmer (subscriber) und vertrauenden Parteien (relying party) zur Verfügung gestellt werden.

Die CA stellt sicher, dass soweit notwendig Zertifikate den Teilnehmern (subscriber), Zertifikatsinhabern (subject) und vertrauenden Parteien (relying party) zur Verfügung gestellt werden.

Die CA stellt sicher, dass Zertifikate kurzfristig anhand von autorisierten und überprüften Sperranfragen gesperrt werden.

4 CA Management und Betrieb

Die CA stellt sicher, dass Verwaltungs- und Management-Verfahren angewendet werden, die angemessen sind und anerkannten Normen entsprechen.

Die CA stellt sicher, dass ihre schützenswerte Objekte und Informationen einen angemessenen Schutz erhalten.

Die CA stellt sicher, dass das Personal und die Einstellungsverfahren die Vertrauenswürdigkeit des CA Betriebs verbessern und unterstützen.

Die CA stellt sicher, dass der physikalische Zugriff auf kritische Dienste kontrolliert wird und physikalische Risiken der schützenswerten Objekte minimiert werden.

Die CA stellt sicher, dass die CA Systeme sicher sind und ordnungsgemäß betrieben werden mit minimalem Ausfallrisiko.

Die CA stellt sicher, dass der Zugriff auf die CA Systeme auf geeignet autorisierte Personen beschränkt ist.

Die CA soll vertrauenswürdige Systeme und Produkte verwenden, die vor Veränderungen geschützt sind.

Die CA stellt sicher, dass im Falle einer Katastrophe, einschließlich der Kompromittierung des privaten CA Signaturschlüssels, der Betrieb so schnell wie möglich wiederhergestellt wird.

Die CA stellt sicher, dass im Falle der Einstellung des Betriebs der CA potenzielle Störungen von Teilnehmer (subscriber) und vertrauenden Parteien (relying party) minimiert werden und dass der Forterhalt der Aufzeichnungen, die zum Nachweis der Zertifizierung in Gerichtsverfahren benötigt werden, gegeben ist.

Die CA stellt sicher, dass die gesetzlichen Anforderungen eingehalten werden.

Die CA stellt sicher, dass alle relevanten Informationen über ein Zertifikat für einen angemessenen Zeitraum aufgezeichnet werden, insbesondere zum Zweck des Nachweises der Zertifizierung in Gerichtsverfahren.

5 Organisation

Die CA stellt sicher, dass ihre Organisation zuverlässig ist.