Zertifikat

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH bescheinigt hiermit dem Unternehmen

OPENTRUST
175 rue Jean-Jacques Rousseau
92138 Issy-les-Moulineaux, Frankreich

für den Zertifizierungsdienst

Cloud Signing Personal Signature CA
Protect and Sign Personal Signature
– Face to face Advanced Signature
(OID 1.3.6.1.4.1.22234.2.8.3.7)

die Erfüllung aller Anforderungen der Spezifikation

ETSI TS 101 456 V1.4.3 (2007-05), policy QCP public.

Die Anlage zum Zertifikat ist Bestandteil des Zertifikats und besteht aus 7 Seiten.

Dieses Zertifikat gilt nur in Verbindung mit dem zugehörigen Prüfbericht bis zum 31.10.2016.

ETSI TS 101 456 CA6739.15 TÜVIT® 2015 Trusted Site
Voluntary Validation
© TÜViT - Member of TÜV NORD GROUP

Zertifikat-Registrier-Nr.:
TUVIT-CA6739.15

Essen, 30.10.2015

Dr. Christoph Sutter
Leiter Zertifizierungsstelle

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

DAkkS Deutsche Akkreditierungsstelle D-ZE-12022-01-00

Zertifizierungssystem

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH ist bei der „DAkkS Deutsche Akkreditierungsstelle GmbH“ für die Zertifizierung von Produkten in den Bereichen IT-Sicherheit und Sicherheitstechnik nach DIN EN ISO/IEC 17065 akkreditiert. Die Zertifizierungsstelle führt ihre Zertifizierungen auf Basis des folgenden akkreditierten Produktzertifizierungsprogramms durch:

- „Zertifizierungsprogramm (akkreditierter Bereich) der Zertifizierungsstelle der TÜV Informationstechnik GmbH“, Version 1.6 vom 29.09.2015, TÜV Informationstechnik GmbH

Prüfbericht

- „Evaluation Report – Surveillance On-Site Inspection – ETSI TS 101 456, Cloud Signing Personal Signature CA Protect and Sign Personal Signature – Face to face Advanced Signature (OID 1.3.6.1.4.1.22234.2.8.3.7“, Version 1.0 vom 23.10.2015, TÜV Informationstechnik GmbH

Prüfanforderungen

Die Prüfanforderungen sind in der technischen Spezifikation ETSI TS 101 456 definiert:

- ETSI TS 101 456 V1.4.3 (2007-05): „Electronic Signatures and Infrastructures (ESI); Policy Requirements for certification authorities issuing qualified certificates“, Version 1.4.3, 2007-05, European Telecommunications Standards Institute

Die anwendbare ETSI Zertifizierungspolitik ist:

- QCP public: Zertifizierungspolitik für (öffentlich angebotene) qualifizierte Zertifikate

Prüfgegenstand

Der Prüfgegenstand ist charakterisiert durch die Zertifikatsinformation zum untersuchten Zertifizierungsdienst:

Cloud Signing Personal Signature CA:

Aussteller des CA-Zertifikats (Root CA oder Intermediate CA): CN = KEYNECTIS CDS CA Zertifikatsseriennummer: 3e 1c be 03	
Name der CA (wie im Zertifikat)	**Seriennummer des Zertifikates**
CN = Cloud Signing Personal Signature CA	11 20 86 c8 d4 0a 18 65 c0 38 0e 63 d1 28 d5 33 d5 0c

zusammen mit der Certificate Policy (CP) des Betreibers:

- „Certificate Policy – Cloud Signing Personal Signature CA (ETSI 102 042 and ETSI 101 456)“, Version 1.1 vom 21.10.2014

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

- „Certification Practice Statement – Cloud Signing Personal Signature CA (ETSI 102 042 and ETSI 101 456)“, Version 1.1 vom 22.10.2014

Prüfergebnis

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

Zusammenfassung der Prüfanforderungen

TÜV®

Die ETSI Spezifikation ETSI TS 101 456 enthält folgende Anforderungen:

1 Certification Practice Statement (CPS)

Die CA stellt sicher, dass sie die erforderliche Zuverlässigkeit für die Bereitstellung von Zertifizierungsdiensten darlegt (siehe die Richtlinie 1999/98/EG, Anhang II (a)).

2 Public Key Infrastructure – Schlüsselmanagement-Lebenszyklus

Die CA stellt sicher, dass CA Schlüssel unter kontrollierten Bedingungen erzeugt werden (siehe die Richtlinie 1999/93/EG, Anhang II (g) und Anhang II (f)).

Die CA stellt sicher, dass private CA Schlüssel vertraulich bleiben und ihre Integrität beibehalten (siehe die Richtlinie 1999/93/EG, Anhang II (g) und Anhang II (f)).

Die CA stellt sicher, dass die Integrität und Authentizität der (öffentlichen) CA Signaturprüfschlüssel und aller zugehörigen Parameter während ihrer Übermittlung an vertrauende Parteien (relying party) erhalten bleiben (siehe die Richtlinie 1999/93/EG, Anhang II (g) und Anhang II (f)).

Private Signaturschlüssel von Inhabern (subject) dürfen nicht hinterlegt werden, dass eine (Reserve-)Entschlüsselungsmöglichkeit geboten wird, die es autorisierten Stellen unter bestimmten Bedingungen erlaubt, Daten unter Verwendung von Information, die durch einen oder mehrere Beteiligte bereitgestellt werden, zu entschlüsseln (gemeinhin als Key Escrow bezeichnet) (siehe die Richtlinie 1999/93/EG, Anhang II (j)).

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 hinaus verwendet werden (siehe die Richtlinie 1999/93/EG, Anhang II (g) und Anhang II (f)).

Die CA stellt sicher, dass die Sicherheit der kryptografischen Hardware während ihres gesamten Lebenszyklus gewährleistet ist (siehe die Richtlinie 1999/93/EG, Anhang II (f)).

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 (siehe die Richtlinie 1999/93/EG, Anhang II (f) und Anhang II(j)).

Die CA stellt sicher, dass die Übergabe der sicheren Signaturerstellungseinheit sicher erfolgt, sofern diese Signaturerstellungseinheit der CA bereitgestellt wird (siehe die Richtlinie 1999/93/EG, Anhang III).

3 Public Key Infrastructure – Zertifikatsmanagement Lebenszyklus

Die CA stellt sicher, dass Zertifikatsinhaber (subject) geeignet identifiziert und authentifiziert sind und dass Zertifikatsanträge vollständig, korrekt und ordnungsgemäß autorisiert sind (siehe die Richtlinie 1999/93/EG, Anhang II (d)).

Die CA stellt sicher, dass Zertifikatsanträge von Zertifikatsinhabern (subject), die zuvor bei der gleichen CA registriert wurden, vollständig, korrekt und ordnungsgemäß autorisiert sind. Dies beinhaltet Zertifikatsverlängerungen, erneute Schlüsselgenerierung (rekey) nach Sperrung oder vor Ablauf der Gültigkeit oder Aktualisierung aufgrund Attributsänderungen des Zertifikatsinhabers (subject) (siehe die Richtlinie 1999/93/EG, Anhang II (g)).

Die CA stellt sicher, dass Zertifikate sicher ausgegeben werden, so dass ihre Authentizität erhalten bleibt (siehe die Richtlinie 1999/93/EG, Anhang II (g)).

Die CA stellt sicher, dass die allgemeinen Geschäftsbedingungen den Teilnehmer (subscriber) und vertrauenden Parteien (relying party) zur Verfügung gestellt werden (siehe die Richtlinie 1999/93/EG, Anhang II (k)).

Die CA stellt sicher, dass Zertifikate den Teilnehmern (subscriber), Zertifikatsinhabern (subject) und vertrauenden Parteien (relying party) im erforderlichen Umfang zur Verfügung gestellt werden (siehe die Richtlinie 1999/93/EG, Anhang II (l)).

Die CA stellt sicher, dass Zertifikate kurzfristig anhand von autorisierten und überprüften Sperranfragen gesperrt werden (siehe die Richtlinie 1999/93/EG, Anhang II (b)).

4 CA Management und Betrieb

Die CA stellt sicher, dass Verwaltungs- und Management-Verfahren angewendet werden, die angemessen sind und anerkannten Normen entsprechen (siehe die Richtlinie 1999/93/EG, Anhang II (e), 2. Teil).

Die CA stellt sicher, dass ihre schützenswerte Objekte und Informationen einen angemessenen Schutz erhalten (siehe die Richtlinie 1999/93/EG, Anhang II (e)).

Die CA stellt sicher, dass das Personal und die Einstellungsverfahren die Vertrauenswürdigkeit des CA Betriebs verstärken und unterstützen (siehe die Richtlinie 1999/93/EG, Anhang II (e) 1. Teil).

Die CA stellt sicher, dass der physische Zugriff auf kritische Dienste kontrolliert wird und physische Risiken der schützenswerten Objekte minimiert werden (siehe die Richtlinie 1999/93/EG, Anhang II (f)).

Die CA stellt sicher, dass die CA Systeme sicher sind und ordnungsgemäß betrieben werden mit minimalem Ausfallrisiko (siehe die Richtlinie 1999/93/EG, Anhang II (e)).

Die CA stellt sicher, dass der Zugriff auf die CA Systeme auf geeignet autorisierte Personen beschränkt ist (siehe die Richtlinie 1999/93/EG, Anhang II (f)).

Die CA soll vertrauenswürdige Systeme und Produkte verwenden, die vor Veränderungen geschützt sind (siehe die Richtlinie 1999/93/EG, Anhang II (f)).

Die CA stellt sicher, dass im Falle einer Katastrophe, einschließlich der Kompromittierung des privaten CA Signaturschlüssels, der Betrieb so schnell wie möglich wiederhergestellt wird (siehe die Richtlinie 1999/93/EG, Anhang II (a)).

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, geben ist (siehe die Richtlinie 1999/93/EG, Anhang II (i)).

Die CA stellt sicher, dass die gesetzlichen Anforderungen eingehalten werden (siehe die Richtlinie 1999/93/EG, Artikel 8).

Die CA stellt sicher, dass alle relevanten Informationen über ein qualifiziertes Zertifikat für einen angemessenen Zeitraum aufgezeichnet werden, insbesondere zum Zweck des Nachweises der Zertifizierung in Gerichtsverfahren (siehe die Richtlinie 1999/93/EG, Anhang II (i)).

5 Organisation

Die CA stellt sicher, dass ihre Organisation zuverlässig ist (siehe die Richtlinie 1999/93/EG, Anhang II (a)).

Gegenstand des Nachtrags

Dieser Nachtrag vom 13.04.2016 ergänzt das Zertifikat TUVIT-CA6739.15 vom 30.10.2015 aufgrund des durchgeführten Zusatzaudits. Prüfgegenstand war die Einführung von Registrierungsdiensten für den Zertifizierungsdienst Cloud Signing Personal Signature CA Protect and Sign Personal Signature, die durch die Registrierungsstelle (RA) der IDnow GmbH zur Verfügung gestellt werden.

Zertifizierungssystem

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH ist bei der „DAkkS Deutsche Akkreditierungsstelle GmbH“ für die Zertifizierung von Produkten in den Bereichen IT-Sicherheit und Sicherheitstechnik nach DIN EN ISO/IEC 17065 akkreditiert. Die Zertifizierungsstelle führt ihre Zertifizierungen auf Basis des folgenden akkreditierten Produktzertifizierungsprogramms durch:

- „Zertifizierungsprogramm (akkreditierter Bereich) der Zertifizierungsstelle der TÜV Informationstechnik GmbH”, Version 1.7 vom 18.03.2016, TÜV Informationstechnik GmbH

Prüfbericht

- „Evaluation Report – Supplementary On-Site Inspection – ETSI TS 101 456, Cloud Signing Personal Signature CA Protect and Sign Personal Signature“, Version 1.0 vom 29.03.2016, TÜV Informationstechnik GmbH

Prüfanforderungen

Die Prüfanforderungen sind in der technischen Spezifikation ETSI TS 101 456 definiert:

- ETSI TS 101 456 V1.4.3 (2007-05): „Electronic Signatures and Infrastructures (ESI); Policy Requirements for certification authorities issuing qualified certificates“, Version 1.4.3,

2007-05, European Telecommunications Standards Institute

Die anwendbare ETSI Zertifizierungspolitik ist:

- QCP public: Zertifizierungspolitik für (öffentlich angebotene) qualifizierte Zertifikate

Prüfgegenstand

Der Prüfgegenstand ist charakterisiert durch die Zertifikats-information zum untersuchten Zertifizierungsdienst:

Cloud Signing Personal Signature CA:

Aussteller des CA-Zertifikats (Root CA oder Intermediate CA): CN = KEYNECTIS CDS CA Zertifikatsseriennummer: 3e 1c be 03	
Name der CA (wie im Zertifikat)	**Seriennummer des Zertifikates**
CN = Cloud Signing Personal Signature CA	11 20 86 c8 d4 0a 18 65 c0 38 0e 63 d1 28 d5 33 d5 0c

zusammen mit der Certificate Policy (CP) des Betreibers:

- „Certificate Policy – Cloud Signing Personal Signature CA (ETSI 102 042 and ETSI 101 456)“, Version 1.1 vom 21.10.2014

und dem Certification Practice Statement (CPS) des Betreibers:

- „Certification Practice Statement – Cloud Signing Personal Signature CA (ETSI 102 042 and ETSI 101 456)“, Version 1.1 vom 22.10.2014

Prüfergebnis

- Der Prüfgegenstand erfüllt alle anwendbaren Anforderungen aus den Prüfkriterien mit Relevanz für die Registrierungsdienste.
- Die im Zertifizierungssystem definierten Zertifizierungsvoraussetzungen sind erfüllt.

Zusammenfassung der Prüfanforderungen

Die ETSI Spezifikation ETSI TS 101 456 enthält folgende Anforderungen:

1 Certification Practice Statement (CPS)

Die CA stellt sicher, dass sie die erforderliche Zuverlässigkeit für die Bereitstellung von Zertifizierungsdiensten darlegt (siehe die Richtlinie 1999/98/EG, Anhang II (a)).

2 Public Key Infrastructure – Schlüsselmanagement-Lebenszyklus

Die CA stellt sicher, dass CA Schlüssel unter kontrollierten Bedingungen erzeugt werden (siehe die Richtlinie 1999/93/EG, Anhang II (g) und Anhang II (f)).

Die CA stellt sicher, dass private CA Schlüssel vertraulich bleiben und ihre Integrität beibehalten (siehe die Richtlinie 1999/93/EG, Anhang II (g) und Anhang II (f)).

Die CA stellt sicher, dass die Integrität und Authentizität der (öffentlichen) CA Signaturprüfschlüssel und aller zugehörigen Parameter während ihrer Übermittlung an vertrauende Parteien (relying party) erhalten bleiben (siehe die Richtlinie 1999/93/EG, Anhang II (g) und Anhang II (f)).

Private Signaturschlüssel von Inhabern (subject) dürfen nicht hinterlegt werden, dass eine (Reserve-)Entschlüsselungsmöglichkeit geboten wird, die es autorisierten Stellen unter bestimmten Bedingungen erlaubt, Daten unter Verwendung von Information, die durch einen oder mehrere Beteiligte bereitgestellt werden, zu entschlüsseln (gemeinhin als Key Escrow bezeichnet) (siehe die Richtlinie 1999/93/EG, Anhang II (j)).

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 hinaus verwendet werden (siehe die Richtlinie 1999/93/EG, Anhang II (g) und Anhang II (f)).

Die CA stellt sicher, dass die Sicherheit der kryptografischen Hardware während ihres gesamten Lebenszyklus gewährleistet ist (siehe die Richtlinie 1999/93/EG, Anhang II (f)).

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 (siehe die Richtlinie 1999/93/EG, Anhang II (f) und Anhang II(j)).

Die CA stellt sicher, dass die Übergabe der sicheren Signaturerstellungseinheit sicher erfolgt, sofern diese Signaturerstellungseinheit der CA bereitgestellt wird (siehe die Richtlinie 1999/93/EG, Anhang III).

3 Public Key Infrastructure – Zertifikatsmanagement Lebenszyklus

Die CA stellt sicher, dass Zertifikatsinhaber (subject) geeignet identifiziert und authentifiziert sind und dass Zertifikatsanträge vollständig, korrekt und ordnungsgemäß autorisiert sind (siehe die Richtlinie 1999/93/EG, Anhang II (d)).

Die CA stellt sicher, dass Zertifikatsanträge von Zertifikatsinhabern (subject), die zuvor bei der gleichen CA registriert wurden, vollständig, korrekt und ordnungsgemäß autorisiert sind. Dies beinhaltet Zertifikatsverlängerungen, erneute Schlüsselgenerierung (rekey) nach Sperrung oder vor Ablauf der Gültigkeit oder Aktualisierung aufgrund Attributsänderungen des Zertifikatsinhabers (subject) (siehe die Richtlinie 1999/93/EG, Anhang II (g)).

Die CA stellt sicher, dass Zertifikate sicher ausgegeben werden, so dass ihre Authentizität erhalten bleibt (siehe die Richtlinie 1999/93/EG, Anhang II (g)).

Die CA stellt sicher, dass die allgemeinen Geschäftsbedingungen den Teilnehmer (subscriber) und vertrauenden Parteien (relying party) zur Verfügung gestellt werden (siehe die Richtlinie 1999/93/EG, Anhang II (k)).

Die CA stellt sicher, dass Zertifikate den Teilnehmern (subscriber), Zertifikatsinhabern (subject) und vertrauenden Parteien (relying party) im erforderlichen Umfang zur Verfügung gestellt werden (siehe die Richtlinie 1999/93/EG, Anhang II (l)).

Die CA stellt sicher, dass Zertifikate kurzfristig anhand von autorisierten und überprüften Sperranfragen gesperrt werden (siehe die Richtlinie 1999/93/EG, Anhang II (b)).

4 CA Management und Betrieb

Die CA stellt sicher, dass Verwaltungs- und Management-Verfahren angewendet werden, die angemessen sind und anerkannten Normen entsprechen (siehe die Richtlinie 1999/93/EG, Anhang II (e), 2. Teil).

Die CA stellt sicher, dass ihre schützenswerte Objekte und Informationen einen angemessenen Schutz erhalten (siehe die Richtlinie 1999/93/EG, Anhang II (e)).

Die CA stellt sicher, dass das Personal und die Einstellungsverfahren die Vertrauenswürdigkeit des CA Betriebs verstärken und unterstützen (siehe die Richtlinie 1999/93/EG, Anhang II (e) 1. Teil).

Die CA stellt sicher, dass der physische Zugriff auf kritische Dienste kontrolliert wird und physische Risiken der schützenswerten Objekte minimiert werden (siehe die Richtlinie 1999/93/EG, Anhang II (f)).

Die CA stellt sicher, dass die CA Systeme sicher sind und ordnungsgemäß betrieben werden mit minimalem Ausfallrisiko (siehe die Richtlinie 1999/93/EG, Anhang II (e)).

Die CA stellt sicher, dass der Zugriff auf die CA Systeme auf geeignet autorisierte Personen beschränkt ist (siehe die Richtlinie 1999/93/EG, Anhang II (f)).

Die CA soll vertrauenswürdige Systeme und Produkte verwenden, die vor Veränderungen geschützt sind (siehe die Richtlinie 1999/93/EG, Anhang II (f)).

Die CA stellt sicher, dass im Falle einer Katastrophe, einschließlich der Kompromittierung des privaten CA Signaturschlüssels, der Betrieb so schnell wie möglich wiederhergestellt wird (siehe die Richtlinie 1999/93/EG, Anhang II (a)).

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, geben ist (siehe die Richtlinie 1999/93/EG, Anhang II (i)).

Die CA stellt sicher, dass die gesetzlichen Anforderungen eingehalten werden (siehe die Richtlinie 1999/93/EG, Artikel 8).

Die CA stellt sicher, dass alle relevanten Informationen über ein qualifiziertes Zertifikat für einen angemessenen Zeitraum aufgezeichnet werden, insbesondere zum Zweck des Nachweises der Zertifizierung in Gerichtsverfahren (siehe die Richtlinie 1999/93/EG, Anhang II (i)).

5 Organisation

Die CA stellt sicher, dass ihre Organisation zuverlässig ist (siehe die Richtlinie 1999/93/EG, Anhang II (a)).