Zertifikat

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH bescheinigt hiermit dem Unternehmen

Skaitmeninio Sertifikavimo Centras
Jogailos 8 - 16
01116 Vilnius, Litauen

für den Zeitstempeldienst

SSC GDL TSA

die Erfüllung aller Anforderungen der Spezifikation

ETSI TS 102 023 V1.2.2 (2008-10).

Die Anlage zum Zertifikat ist Bestandteil des Zertifikats und besteht aus 5 Seiten.

Dieses Zertifikat gilt nur in Verbindung mit dem zugehörigen Prüfbericht bis zum 30.06.2016.

ETSI TS 102 023 CA6731.13 TÜVIT® 2013 Trusted Site

Voluntary Validation

Zertifikat-Registrier-Nr.:
TUVIT-CA6731.13

Essen, 28.06.2013

Dr. Christoph Sutter
Leiter Zertifizierungsstelle

TÜV Informationstechnik GmbH
Member of TÜV NORD GROUP
Langemarckstraße 20
45141 Essen
www.tuvit.de

Deutscher Akkreditierungs Rat
DAR
DGA-ZE-014/99

Zertifizierungssystem

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, TÜV Informationstechnik GmbH

Prüfbericht

- „Evaluation Report – Initial Certification – ETSI TS 102 023, SSC GDL TSA“, Version 2.2 vom 28.06.2013, TÜV Informationstechnik GmbH

Prüfanforderungen

Die Prüfanforderungen sind in der technischen Spezifikation ETSI TS 102 023 definiert:

- ETSI TS 102 023 V1.2.2 (2008-10): „Electronic Signatures and Infrastructures (ESI); Policy Requirements for time-stamping authorities“, Version 1.2.2, 2008-10, European Telecommunications Standards Institute

Prüfgegenstand

Der Prüfgegenstand ist charakterisiert durch die Zertifikatsinformation zum untersuchten Zeitstempeldienst:

SSC GDL TSA:

Issuing CA (Issuer of TSA certificate): CN = SSC GDL NH CA	
Name of TSA (as in certificate)	**serial number of certificate**
CN = SSC GDL TSA	61 31 cd f0 00 00 00 00 00 08

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

- "Time-Stamp Policy and Practice Statement SSC GDL CA", Version 1.6 vom 27.06.2013, Skaitmeninio Sertifikavimo Centras

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 102 023 enthält folgende Anforderungen:

1 Time-Stamping-Authority (TSA) Practice statement

Die TSA stellt sicher, dass sie die erforderliche Zuverlässigkeit für die Bereitstellung von Zeitstempeldiensten darlegt.

Die TSA legt allen Teilnehmer (subscriber) und potentiellen vertrauenden Parteien (relying parties) die Nutzungsbedingungen hinsichtlich der Verwendung ihrer Zeitstempeldienste offen.

2 Schlüsselmanagement-Lebenszyklus

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

Die TSA stellt sicher, dass private Time-Stamping-Unit (TSU)-Schlüssel vertraulich bleiben und ihre Integrität beibehalten.

Die TSA stellt sicher, dass die Integrität und Authentizität der (öffentlichen) TSU Signaturprüfschlüssel und aller zugehörigen Parameter während ihrer Übermittlung an vertrauende Parteien (relying party) erhalten bleiben.

Die Lebensdauer von TSU Zertifikaten ist nicht länger als der Zeitraum, der für den gewählten Algorithmus und die Schlüssellänge als geeignet für den Zweck anerkannt ist.

Die TSA stellt sicher, dass private TSU Signaturschlüssel nicht über das Ende ihrer Gültigkeit hinaus verwendet werden.

Die TSA stellt sicher, dass die Sicherheit der kryptografischen Hardware während ihres gesamten Lebenszyklus gegeben ist.

3 Zeitstempel

Die TSA stellt sicher, dass Zeitstempel sicher ausgegeben werden und die richtige Zeit enthalten.

Die TSA stellt sicher, dass ihre Uhr mit UTC innerhalb der angegebenen Genauigkeit synchronisiert wird.

4 TSA Management und Betrieb

Die TSA stellt sicher, dass Verwaltungs- und Management-Verfahren angewendet werden, die angemessen sind sowie anerkannten und bewerten Verfahren entsprechen.

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

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

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

Die TSA stellt sicher, dass die TSA Systemkomponenten sicher sind und ordnungsgemäß betrieben werden mit minimalem Ausfallrisiko.

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

Die TSA verwendet vertrauenswürdige Systeme und Produkte verwenden, die vor Veränderungen geschützt sind.

Die TSA stellt sicher, dass bei Ereignissen, die die Sicherheit des TSA-Dienstes betreffen, einschließlich Kompromittierung des privaten TSA Signaturschlüssels oder festgestellten Verlust der Kalibrierung, relevante Information dem Teilnehmer (subscriber) und den vertrauten Parteien (relying parties) bereitgeteilt wird.

Die TSA stellt sicher, dass im Falle der Einstellung des Betriebs der TSA potenzielle Störungen von Teilnehmer (subscriber) und vertrauenden Parteien (relying party) minimiert werden und dass insbesondere der Forterhalt der Informationen, die zur Nachprüfung der Korrektheit des Zeitstempel Tokens notwendig sind, geben ist.

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

Die TSA stellt sicher, dass alle relevanten Informationen über den Betrieb von Zeitstempeldiensten für einen angemessenen Zeitraum aufgezeichnet werden, insbesondere zum Zweck des Nachweises in Gerichtsverfahren.

5 Organisation

Die TSA stellt sicher, dass ihre Organisation zuverlässig ist.

Gegenstand des Nachtrags

Dieser Nachtrag vom 04.07.2014 ergänzt das Zertifikat TUVIT-CA6731.13 vom 28.06.2013 aufgrund des durchgeführten Überwachungsaudits.

Zertifizierungssystem

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 Produktzertifizierungssystems durch:

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

Prüfbericht

- „Evaluation Report - Surveillance On-Site Inspection - ETSI TS 102 023, SSC GDL TSA“, Version 1.0 vom 17.06.2014, TÜV Informationstechnik GmbH

Prüfanforderungen

Die Prüfanforderungen sind in der technischen Spezifikation ETSI TS 102 023 definiert:

- ETSI TS 102 023 V1.2.2 (2008-10): „Electronic Signatures and Infrastructures (ESI); Policy Requirements for time-stamping authorities“, Version 1.2.2, 2008-10, European Telecommunications Standards Institute

Prüfgegenstand

Der Prüfgegenstand ist charakterisiert durch die Zertifikatsinformation zum untersuchten Zeitstempeldienst:

SSC GDL TSA:

Aussteller des CA-Zertifikats (Root CA oder Intermediate CA): CN = SSC GDL NH CA Zertifikatsseriennummer: 61 2b 54 f4 00 00 00 00 00 02	
Name der CA (wie im Zertifikat)	**Seriennummer des Zertifikates**
CN = SSC GDL TSA	61 31 cd f0 00 00 00 00 00 08
CN = SSC GDL QTSA	11 96 94 1b 00 00 00 00 00 12

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

- "Time-Stamp Policy and Practice Statement SSC GDL CA", Version 1.7 vom 17.02.2014, Skaitmeninio Sertifikavimo Centras

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 102 023 enthält folgende Anforderungen:

1 Time-Stamping-Authority (TSA) Practice statement

Die TSA stellt sicher, dass sie die erforderliche Zuverlässigkeit für die Bereitstellung von Zeitstempeldiensten darlegt.

Die TSA legt allen Teilnehmer (subscriber) und potentiellen vertrauenden Parteien (relying parties) die Nutzungsbedingungen hinsichtlich der Verwendung ihrer Zeitstempeldienste offen.

2 Schlüsselmanagement-Lebenszyklus

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

Die TSA stellt sicher, dass private Time-Stamping-Unit (TSU)-Schlüssel vertraulich bleiben und ihre Integrität beibehalten.

Die TSA stellt sicher, dass die Integrität und Authentizität der (öffentlichen) TSU Signaturprüfschlüssel und aller zugehörigen Parameter während ihrer Übermittlung an vertrauende Parteien (relying party) erhalten bleiben.

Die Lebensdauer von TSU Zertifikaten ist nicht länger als der Zeitraum, der für den gewählten Algorithmus und die Schlüssellänge als geeignet für den Zweck anerkannt ist.

Die TSA stellt sicher, dass private TSU Signaturschlüssel nicht über das Ende ihrer Gültigkeit hinaus verwendet werden.

Die TSA stellt sicher, dass die Sicherheit der kryptografischen Hardware während ihres gesamten Lebenszyklus gegeben ist.

3 Zeitstempel

Die TSA stellt sicher, dass Zeitstempel sicher ausgegeben werden und die richtige Zeit enthalten.

Die TSA stellt sicher, dass ihre Uhr mit UTC innerhalb der angegebenen Genauigkeit synchronisiert wird.

4 TSA Management und Betrieb

Die TSA stellt sicher, dass Verwaltungs- und Management-Verfahren angewendet werden, die angemessen sind sowie anerkannten und bewerten Verfahren entsprechen.

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

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

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

Die TSA stellt sicher, dass die TSA Systemkomponenten sicher sind und ordnungsgemäß betrieben werden mit minimalem Ausfallrisiko.

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

Die TSA verwendet vertrauenswürdige Systeme und Produkte verwenden, die vor Veränderungen geschützt sind.

Die TSA stellt sicher, dass bei Ereignissen, die die Sicherheit des TSA-Dienstes betreffen, einschließlich Kompromittierung des privaten TSA Signaturschlüssels oder festgestellten Verlust der Kalibrierung, relevante Information dem Teilnehmer (subscriber) und den vertrauten Parteien (relying parties) bereitgeteilt wird.

Die TSA stellt sicher, dass im Falle der Einstellung des Betriebs der TSA potenzielle Störungen von Teilnehmer (subscriber) und vertrauenden Parteien (relying party) minimiert werden und dass insbesondere der Forterhalt der Informationen, die zur Nachprüfung der Korrektheit des Zeitstempel Tokens notwendig sind, geben ist.

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

Die TSA stellt sicher, dass alle relevanten Informationen über den Betrieb von Zeitstempeldiensten für einen angemessenen Zeitraum aufgezeichnet werden, insbesondere zum Zweck des Nachweises in Gerichtsverfahren.

5 Organisation

Die TSA stellt sicher, dass ihre Organisation zuverlässig ist.

Gegenstand des Nachtrags

Dieser Nachtrag vom 30.06.2015 ergänzt das Zertifikat TUVIT-CA6731.13 vom 28.06.2013 mit dem Nachtrag 1 vom 04.07.2014 aufgrund des durchgeführten Überwachungsaudits.

Zertifizierungssystem

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 Basis des folgenden akkreditierten Produktzertifizierungsprogramms durch:

- „Zertifizierungsprogramm (akkreditierter Bereich) der Zertifizierungsstelle der TÜV Informationstechnik GmbH“, Version 1.4 vom 28.11.2014, TÜV Informationstechnik GmbH

Prüfbericht

- „Evaluation Report - Surveillance On-Site Inspection - ETSI TS 102 023, SSC GDL TSA“, Version 1.1 vom 30.06.2015, TÜV Informationstechnik GmbH

Prüfanforderungen

Die Prüfanforderungen sind in der technischen Spezifikation ETSI TS 102 023 definiert:

- ETSI TS 102 023 V1.2.2 (2008-10): „Electronic Signatures and Infrastructures (ESI); Policy Requirements for time-stamping authorities“, Version 1.2.2, 2008-10, European Telecommunications Standards Institute

Prüfgegenstand

Der Prüfgegenstand ist charakterisiert durch die Zertifikatsinformation zum untersuchten Zeitstempeldienst:

SSC GDL TSA:

Aussteller des CA-Zertifikats (Root CA oder Intermediate CA): CN = SSC GDL NH CA Zertifikatsseriennummer: 61 2b 54 f4 00 00 00 00 00 02	
Name der CA (wie im Zertifikat)	**Seriennummer des Zertifikates**
CN = SSC GDL TSA	11 f5 9d 2d 00 00 00 00 00 4c
CN = SSC GDL QTSA	11 96 94 1b 00 00 00 00 00 12

zusammen mit dem TSA Practice Statement des Betreibers:

- „Time-Stamp Policy and Practice Statement SSC GDL CA“, Version 1.8 vom 22.04.2014, Skaitmeninio Sertifikavimo Centras

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 102 023 enthält folgende Anforderungen:

1 Time-Stamping-Authority (TSA) Practice statement

Die TSA stellt sicher, dass sie die erforderliche Zuverlässigkeit für die Bereitstellung von Zeitstempeldiensten darlegt.

Die TSA legt allen Teilnehmer (subscriber) und potentiellen vertrauenden Parteien (relying parties) die Nutzungsbedingungen hinsichtlich der Verwendung ihrer Zeitstempeldienste offen.

2 Schlüsselmanagement-Lebenszyklus

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

Die TSA stellt sicher, dass private Time-Stamping-Unit (TSU)-Schlüssel vertraulich bleiben und ihre Integrität beibehalten.

Die TSA stellt sicher, dass die Integrität und Authentizität der (öffentlichen) TSU Signaturprüfschlüssel und aller zugehörigen Parameter während ihrer Übermittlung an vertrauende Parteien (relying party) erhalten bleiben.

Die Lebensdauer von TSU Zertifikaten ist nicht länger als der Zeitraum, der für den gewählten Algorithmus und die Schlüssellänge als geeignet für den Zweck anerkannt ist.

Die TSA stellt sicher, dass private TSU Signaturschlüssel nicht über das Ende ihrer Gültigkeit hinaus verwendet werden.

Die TSA stellt sicher, dass die Sicherheit der kryptografischen Hardware während ihres gesamten Lebenszyklus gegeben ist.

3 Zeitstempel

Die TSA stellt sicher, dass Zeitstempel sicher ausgegeben werden und die richtige Zeit enthalten.

Die TSA stellt sicher, dass ihre Uhr mit UTC innerhalb der angegebenen Genauigkeit synchronisiert wird.

4 TSA Management und Betrieb

Die TSA stellt sicher, dass Verwaltungs- und Management-Verfahren angewendet werden, die angemessen sind sowie anerkannten und bewerten Verfahren entsprechen.

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

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

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

Die TSA stellt sicher, dass die TSA Systemkomponenten sicher sind und ordnungsgemäß betrieben werden mit minimalem Ausfallrisiko.

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

Die TSA verwendet vertrauenswürdige Systeme und Produkte verwenden, die vor Veränderungen geschützt sind.

Die TSA stellt sicher, dass bei Ereignissen, die die Sicherheit des TSA-Dienstes betreffen, einschließlich Kompromittierung des privaten TSA Signaturschlüssels oder festgestellten Verlust der Kalibrierung, relevante Information dem Teilnehmer (subscriber) und den vertrauten Parteien (relying parties) bereitgeteilt wird.

Die TSA stellt sicher, dass im Falle der Einstellung des Betriebs der TSA potenzielle Störungen von Teilnehmer (subscriber) und vertrauenden Parteien (relying party) minimiert werden und dass insbesondere der Forterhalt der Informationen, die zur Nachprüfung der Korrektheit des Zeitstempel Tokens notwendig sind, geben ist.

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

Die TSA stellt sicher, dass alle relevanten Informationen über den Betrieb von Zeitstempeldiensten für einen angemessenen Zeitraum aufgezeichnet werden, insbesondere zum Zweck des Nachweises in Gerichtsverfahren.

5 Organisation

Die TSA stellt sicher, dass ihre Organisation zuverlässig ist.