Certificate

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

Skaitmeninio Sertifikavimo Centras
Jogailos 8 - 16
01116 Vilnius, Lithuania

to confirm that its time-stamping service

SSC GDL TSA

fulfils all requirements defined in the technical specification

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

The appendix to the certificate is part of the certificate and consists of 5 pages.

The certificate is valid only in conjunction with the respective evaluation report until 2016-06-30.

ETSI TS 102 023 CA6731.13
TÜVIT®
2013 Trusted Site
Voluntary Validation
© TÜViT - Member of TÜV NORD GROUP

Certificate-Registration-No.:
TUVIT-CA6731.13

Essen, 2013-06-28

Dr. Christoph Sutter
Head of Certification Body

TÜV Informationstechnik GmbH
Member of TÜV NORD GROUP
Langemarckstr. 20
45141 Essen, Germany
www.tuvit.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, TÜV Informationstechnik GmbH

Evaluation Report

- "Evaluation Report – Initial Certification – ETSI TS 102 023, SSC GDL TSA", version 2.2 as of 2013-06-28, TÜV Informationstechnik GmbH

Evaluation Requirements

The evaluation requirements are defined in the technical specification ETSI TS 102 023:

- 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

Evaluation Target

The target of evaluation is characterized by the certificate information of the inspected time-stamping service:

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

together with the TSA Practice Statement of the operator:

- "Time-Stamp Policy and Practice Statement SSC GDL CA", version 1.6 as of 2013-06-27, Skaitmeninio Sertifikavimo Centras

Evaluation Result

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

Summary of the Evaluation Requirements

The ETSI specification ETSI TS 102 023 contains the following requirements:

1 Time-Stamping-Authority (TSA) Practice statement

The TSA shall ensure that it demonstrates the reliability necessary for providing time-stamping services.

The TSA shall disclose to all subscribers and potential relying parties the terms and conditions regarding use of its time-stamping services.

2 Key management life cycle

The TSA shall ensure that any cryptographic keys are generated in under controlled circumstances.

The TSA shall ensure that Time-Stamping-Unit (TSU) private keys remain confidential and maintain their integrity.

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

The life-time of TSU's certificate shall be not longer than the period of time that the chosen algorithm and key length is recognized as being fit for purpose.

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

The TSA shall ensure the security of cryptographic hardware throughout its lifecycle.

3 Time-stamping

The TSA shall ensure that time-stamp tokens are issued securely and include the correct time.

The TSA shall ensure that its clock is synchronized with UTC within the declared accuracy.

4 TSA management and operation

The TSA shall ensure that administrative and management procedures are applied which are adequate and correspond to recognized best practice.

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

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

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

The TSA shall ensure that the TSA system components are secure and correctly operated, with minimal risk of failure.

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

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

The TSA shall ensure in the case of events which affect the security of the TSA's services, including compromise of TSU's private signing keys or detected loss of calibration, that relevant information is made available to subscribers and relying parties.

The TSA shall ensure that potential disruptions to subscribers and relying parties are minimized as a result of the cessation of the TSA's time-stamping services, and in particular ensure continued maintenance of information required to verify the correctness of time-stamp tokens.

The TSA shall ensure compliance with legal requirements.

The TSA shall ensure that all relevant information concerning the operation of time-stamping services is recorded for a defined period of time, in particular for the purpose of providing evidence for the purposes of legal proceedings.

5 Organizational

The TSA shall ensure that its organization is reliable.

Scope of the Amendment

This amendment as of 2014-07-04 supplements the certificate TUVIT-CA6731.13 as of 2013-06-28 because of the conducted surveillance audit.

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, TÜV Informationstechnik GmbH

Evaluation Report

- "Evaluation Report - Surveillance On-Site Inspection - ETSI TS 102 023, SSC GDL TSA", Version 1.0 as of 2014-06-17, TÜV Informationstechnik GmbH

Evaluation Requirements

The evaluation requirements are defined in the technical specification ETSI TS 102 023:

- 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

Evaluation Target

The target of evaluation is characterized by the certificate information of the inspected time-stamping service:

SSC GDL TSA:

Issuer of CA certificate (Root CA or intermediate CA): CN = SSC GDL NH CA **Certificate Serial Number: 61 2b 54 f4 00 00 00 00 00 02**	
Name of CA (as in certificate)	**serial number of certificate**
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

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

- "Time-Stamp Policy and Practice Statement SSC GDL CA", version 1.7 as of 2014-02-17, Skaitmeninio Sertifikavimo Centras

Evaluation Result

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

Summary of the Evaluation Requirements

The ETSI specification ETSI TS 102 023 contains the following requirements:

1 Time-Stamping-Authority (TSA) Practice statement

The TSA shall ensure that it demonstrates the reliability necessary for providing time-stamping services.

The TSA shall disclose to all subscribers and potential relying parties the terms and conditions regarding use of its time-stamping services.

2 Key management life cycle

The TSA shall ensure that any cryptographic keys are generated in under controlled circumstances.

The TSA shall ensure that Time-Stamping-Unit (TSU) private keys remain confidential and maintain their integrity.

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

The life-time of TSU's certificate shall be not longer than the period of time that the chosen algorithm and key length is recognized as being fit for purpose.

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

The TSA shall ensure the security of cryptographic hardware throughout its lifecycle.

3 Time-stamping

The TSA shall ensure that time-stamp tokens are issued securely and include the correct time.

The TSA shall ensure that its clock is synchronized with UTC within the declared accuracy.

4 TSA management and operation

The TSA shall ensure that administrative and management procedures are applied which are adequate and correspond to recognized best practice.

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

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

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

The TSA shall ensure that the TSA system components are secure and correctly operated, with minimal risk of failure.

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

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

The TSA shall ensure in the case of events which affect the security of the TSA's services, including compromise of TSU's private signing keys or detected loss of calibration, that relevant information is made available to subscribers and relying parties.

The TSA shall ensure that potential disruptions to subscribers and relying parties are minimized as a result of the cessation of the TSA's time-stamping services, and in particular ensure continued maintenance of information required to verify the correctness of time-stamp tokens.

The TSA shall ensure compliance with legal requirements.

The TSA shall ensure that all relevant information concerning the operation of time-stamping services is recorded for a defined period of time, in particular for the purpose of providing evidence for the purposes of legal proceedings.

5 Organizational

The TSA shall ensure that its organization is reliable.

Scope of the Amendment

This amendment as of 2015-06-30 supplements the certificate TUVIT-CA6731.13 as of 2013-06-28 with the first amendment as of 2014-07-04 because of the conducted surveillance audit.

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 scheme:

- German document: "Zertifizierungsprogramm (akkreditierter Bereich) der Zertifizierungsstelle der TÜV Informationstechnik GmbH", version 1.4 as of 2014-11-28, TÜV Informationstechnik GmbH

Evaluation Report

- "Evaluation Report - Surveillance On-Site Inspection - ETSI TS 102 023, SSC GDL TSA", version 1.1 as of 2015-06-30, TÜV Informationstechnik GmbH

Evaluation Requirements

The evaluation requirements are defined in the technical specification ETSI TS 102 023:

- 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

Evaluation Target

The target of evaluation is characterized by the certificate information of the inspected time-stamping service:

SSC GDL TSA:

Issuer of CA certificate (Root CA or intermediate CA): CN = SSC GDL NH CA **Certificate Serial Number: 61 2b 54 f4 00 00 00 00 00 02**	
Name of CA (as in certificate)	**serial number of certificate**
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

together with the TSA Practice Statement of the operator:

- "Time-Stamp Policy and Practice Statement SSC GDL CA", version 1.8 as of 22.04.2014, Skaitmeninio Sertifikavimo Centras

Evaluation Result

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

Summary of the Evaluation Requirements

The ETSI specification ETSI TS 102 023 contains the following requirements:

1 Time-Stamping-Authority (TSA) Practice statement

The TSA shall ensure that it demonstrates the reliability necessary for providing time-stamping services.

The TSA shall disclose to all subscribers and potential relying parties the terms and conditions regarding use of its time-stamping services.

2 Key management life cycle

The TSA shall ensure that any cryptographic keys are generated in under controlled circumstances.

The TSA shall ensure that Time-Stamping-Unit (TSU) private keys remain confidential and maintain their integrity.

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

The life-time of TSU's certificate shall be not longer than the period of time that the chosen algorithm and key length is recognized as being fit for purpose.

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

The TSA shall ensure the security of cryptographic hardware throughout its lifecycle.

3 Time-stamping

The TSA shall ensure that time-stamp tokens are issued securely and include the correct time.

The TSA shall ensure that its clock is synchronized with UTC within the declared accuracy.

4 TSA management and operation

The TSA shall ensure that administrative and management procedures are applied which are adequate and correspond to recognized best practice.

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

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

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

The TSA shall ensure that the TSA system components are secure and correctly operated, with minimal risk of failure.

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

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

The TSA shall ensure in the case of events which affect the security of the TSA's services, including compromise of TSU's private signing keys or detected loss of calibration, that relevant information is made available to subscribers and relying parties.

The TSA shall ensure that potential disruptions to subscribers and relying parties are minimized as a result of the cessation of the TSA's time-stamping services, and in particular ensure continued maintenance of information required to verify the correctness of time-stamp tokens.

The TSA shall ensure compliance with legal requirements.

The TSA shall ensure that all relevant information concerning the operation of time-stamping services is recorded for a defined period of time, in particular for the purpose of providing evidence for the purposes of legal proceedings.

5 Organizational

TÜV®

The TSA shall ensure that its organization is reliable.