

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 certification service

**SSC GDL Class 2-4 QCA and**  
**SSC GDL VS Class 2-4 QCA**

fulfils all requirements defined in the technical specification

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

The appendix to the certificate is part of the certificate and  
consists of 6 pages.

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



16  
Certificate-Registration-No.:  
TUVIT-CA6730.13

**Voluntary Validation**  
© TÜViT - Member of TÜV NORD GROUP

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

The logo for the Deutscher Akkreditierungs Rat (DAR) features the letters 'DAR' in a bold, black, sans-serif font. To the left of the letters is a vertical bar with red, yellow, and black segments. To the right, the text 'Deutscher Akkreditierungs Rat' is written in a smaller font.

DGA-ZE-014/99

**Certificate**

## Certification System

TÜV®

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 101 456, SSC GDL Class 2-4 QCA and SSC GDL VS Class 2-4 QCA”, version 2.1 as of 2013-06-26, TÜV Informationstechnik GmbH

## Evaluation Requirements

The evaluation requirements are defined in the technical specification ETSI TS 101 456:

- 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

The applicable ETSI Certificate Policy is:

- QCP public + SSCD: Qualified Certificate Policy for qualified certificates issued to the public, requiring use of secure signature-creation devices

### Evaluation Target

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

#### SSC GDL Class 2-4 QCA:

Root CA (Issuer of CA certificate): CN = SSC GDL CA Root A	
Name of CA (as in certificate)	serial number of certificate
CN = SSC GDL Class 2-4 QCA	61 39 bb 2c 00 00 00 00 00 02

#### SSC GDL VS Class 2-4 QCA

Root CA (Issuer of CA certificate): CN = SSC GDL CA VS Root	
Name of CA (as in certificate)	serial number of certificate
CN = SSC GDL VS Class 2-4 QCA	61 26 aa dd 00 00 00 00 00 02

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

- “Certification Practice Statement SSC GDL CA”, version 4.6 as of 2013-06-21

### 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

TÜV<sup>®</sup>

The ETSI specification ETSI TS 101 456 contains the following requirements:

### 1 Certification Practice Statement (CPS)

The CA shall ensure that it demonstrates the reliability necessary for providing certification services (see the Directive 1999/98/EC, annex II (a)).

### 2 Public key infrastructure - Key management life cycle

The CA shall ensure that CA keys are generated in controlled circumstances (see the Directive 1999/93/EC, annex II (g) and annex II (f)).

The CA shall ensure that CA private keys remain confidential and maintain their integrity (see the Directive 1999/93/EC, annex II (g) and annex II (f)).

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 (see the Directive 1999/93/EC, annex II (g) and annex II (f)).

Subject private signing keys shall not be held in a way which provides a backup decryption capability, allowing authorized entities under certain conditions to decrypt data using information supplied by one or more parties (commonly called key escrow) (see the Directive 1999/93/EC, annex II (j)).

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 (see the Directive 1999/93/EC, annex II (g) and annex II (f)).

The CA shall ensure the security of cryptographic hardware throughout its lifecycle (see the Directive 1999/93/EC, annex II (f)).

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 (see the Directive 1999/93/EC, annex II (f) and annex II (j)).

The CA shall ensure that if it issues SSCD this is carried out securely (see the Directive 1999/93/EC, annex III).

### **3 Public key infrastructure - Certificate Management life cycle**

The CA shall ensure that subjects are properly identified and authenticated; and that subject certificate requests are complete, accurate and duly authorized (see the Directive 1999/93/EC, annex II (d)).

The CA shall ensure that requests for certificates issued to a subject who has already previously been registered 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 (see the Directive 1999/93/EC, annex II (g)).

The CA shall ensure that it issues certificates securely to maintain their authenticity (see the Directive 1999/93/EC, annex II (g)).

The CA shall ensure that the terms and conditions are made available to subscribers and relying parties (see the Directive 1999/93/EC, annex II (k)).

The CA shall ensure that certificates are made available as necessary to subscribers, subjects and relying parties (see the Directive 1999/93/EC, annex II (l)).

The CA shall ensure that certificates are revoked in a timely manner based on authorized and validated certificate revocation requests (see the Directive 1999/93/EC, annex II (b)).

#### **4 CA management and operation**

The CA shall ensure that administrative and management procedures are applied which are adequate and correspond to recognized standards (see the Directive 1999/93/EC, annex II (e), 2<sup>nd</sup> part).

The CA shall ensure that its assets and information receive an appropriate level of protection (see the Directive 1999/93/EC, annex II (e)).

The CA shall ensure that personnel and hiring practices enhance and support the trustworthiness of the CA's operations (see Directive 1999/93/EC, annex II (e) 1<sup>st</sup> part).

The CA shall ensure that physical access to critical services is controlled and physical risks to its assets minimized (see Directive 1999/93/EC, annex II (f)).

The CA shall ensure that the CA systems are secure and correctly operated, with minimal risk of failure (see the Directive 1999/93/EC, annex II (e)).

The CA shall ensure that CA system access is limited to properly authorized individuals (see the Directive 1999/93/EC, annex II (f)).

The CA shall use trustworthy systems and products that are protected against modification (see the Directive 1999/93/EC, annex II (f)).

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 (see the Directive 1999/93/EC, annex II (a)).

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 as covered by the certificate policy, and ensure continued maintenance of records required to provide evidence of certification for the purposes of legal proceedings (see the Directive 1999/93/EC, annex II (i)).

The CA shall ensure compliance with legal requirements (see the Directive 1999/93/EC, article 8).

The CA shall ensure that all relevant information concerning a qualified 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 (see the Directive 1999/93/EC, annex II (i)).

## **5 Organizational**

The CA shall ensure that its organization is reliable (see Directive 1999/93/EC, annex II (a)).

## Scope of the Amendment

This amendment as of 2014-07-04 supplements the certificate TUVIT-CA6730.13 as of 2013-06-28 because of the conducted surveillance audit

TÜV®

## 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 101 456, SSC GDL Class 2-4 QCA and SSC GDL VS Class 2-4 QCA”, Version 1.0 as of 2014-06-17, TÜV Informationstechnik GmbH

## Evaluation Requirements

The evaluation requirements are defined in the technical specification ETSI TS 101 456:

- 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

The applicable ETSI Certificate Policy is:

- QCP public + SSCD: Qualified Certificate Policy for qualified



certificates issued to the public, requiring use of secure signature-creation devices

### Evaluation Target

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

#### SSC GDL Class 2-4 QCA:

<b>Issuer of CA certificate (Root CA or intermediate CA):</b> <b>CN = SSC GDL CA Root A</b> <b>Certificate Serial Number: 50 96 6e 72 bd 10 d6 8c 4f 6b c7 62 3f 9c 70 38</b>	
<b>Name of CA (as in certificate)</b>	<b>serial number of certificate</b>
CN = SSC GDL Class 2-4 QCA	61 39 bb 2c 00 00 00 00 00 02

#### SSC GDL VS Class 2-4 QCA:

<b>Issuer of CA certificate (Root CA or intermediate CA):</b> <b>CN = SSC GDL CA VS Root</b> <b>Certificate Serial Number: 33 bd 22 7b 2b bc 70 84 4c 20 5f 57 3f 94 55 f5</b>	
<b>Name of CA (as in certificate)</b>	<b>serial number of certificate</b>
CN = SSC GDL VS Class 2-4 QCA	61 26 aa dd 00 00 00 00 00 02

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

- “Certification Practice Statement SSC GDL CA”, version 4.6 as of 2013-06-21, 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 101 456 contains the following requirements:

### **1 Certification Practice Statement (CPS)**

The CA shall ensure that it demonstrates the reliability necessary for providing certification services (see the Directive 1999/98/EC, annex II (a)).

### **2 Public key infrastructure - Key management life cycle**

The CA shall ensure that CA keys are generated in controlled circumstances (see the Directive 1999/93/EC, annex II (g) and annex II (f)).

The CA shall ensure that CA private keys remain confidential and maintain their integrity (see the Directive 1999/93/EC, annex II (g) and annex II (f)).

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 (see the Directive 1999/93/EC, annex II (g) and annex II (f)).

Subject private signing keys shall not be held in a way which provides a backup decryption capability, allowing authorized entities under certain conditions to decrypt data using information supplied by one or more parties (commonly called key escrow) (see the Directive 1999/93/EC, annex II (j)).

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 (see the Directive 1999/93/EC, annex II (g) and annex II (f)).

The CA shall ensure the security of cryptographic hardware throughout its lifecycle (see the Directive 1999/93/EC, annex II (f)).

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 (see the Directive 1999/93/EC, annex II (f) and annex II (j)).

The CA shall ensure that if it issues SSCD this is carried out securely (see the Directive 1999/93/EC, annex III).

### **3 Public key infrastructure - Certificate Management life cycle**

The CA shall ensure that subjects are properly identified and authenticated; and that subject certificate requests are complete, accurate and duly authorized (see the Directive 1999/93/EC, annex II (d)).

The CA shall ensure that requests for certificates issued to a subject who has already previously been registered 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 (see the Directive 1999/93/EC, annex II (g)).

The CA shall ensure that it issues certificates securely to maintain their authenticity (see the Directive 1999/93/EC, annex II (g)).

The CA shall ensure that the terms and conditions are made available to subscribers and relying parties (see the Directive 1999/93/EC, annex II (k)).

The CA shall ensure that certificates are made available as necessary to subscribers, subjects and relying parties (see the Directive 1999/93/EC, annex II (l)).

The CA shall ensure that certificates are revoked in a timely manner based on authorized and validated certificate revocation requests (see the Directive 1999/93/EC, annex II (b)).

#### **4 CA management and operation**

The CA shall ensure that administrative and management procedures are applied which are adequate and correspond to recognized standards (see the Directive 1999/93/EC, annex II (e), 2nd part).

The CA shall ensure that its assets and information receive an appropriate level of protection (see the Directive 1999/93/EC, annex II (e)).

The CA shall ensure that personnel and hiring practices enhance and support the trustworthiness of the CA's operations (see Directive 1999/93/EC, annex II (e) 1st part).

The CA shall ensure that physical access to critical services is controlled and physical risks to its assets minimized (see Directive 1999/93/EC, annex II (f)).

The CA shall ensure that the CA systems are secure and correctly operated, with minimal risk of failure (see the Directive 1999/93/EC, annex II (e)).

The CA shall ensure that CA system access is limited to properly authorized individuals (see the Directive 1999/93/EC, annex II (f)).

The CA shall use trustworthy systems and products that are protected against modification (see the Directive 1999/93/EC, annex II (f)).

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 (see the Directive 1999/93/EC, annex II (a)).

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 as covered by the certificate policy, and ensure continued maintenance of records required to provide evidence of certification for the purposes of legal proceedings (see the Directive 1999/93/EC, annex II (i)).

The CA shall ensure compliance with legal requirements (see the Directive 1999/93/EC, article 8).

The CA shall ensure that all relevant information concerning a qualified 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 (see the Directive 1999/93/EC, annex II (i)).

## **5 Organizational**

The CA shall ensure that its organization is reliable (see Directive 1999/93/EC, annex II (a)).

## Scope of the Amendment

This amendment as of 2015-06-30 supplements the certificate TUVIT-CA6730.13 as of 2013-06-28 with the first amendment as of 2014-07-04 because of the conducted surveillance audit.

**TÜV**<sup>®</sup>

## 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 101 456, SSC GDL Class 2-4 QCA and SSC GDL VS Class 2-4 QCA”, version 1.0 as of 2015-06-30 TÜV Informationstechnik GmbH

## Evaluation Requirements

The evaluation requirements are defined in the technical specification ETSI TS 101 456:

- 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

The applicable ETSI Certificate Policy is:



- QCP public + SSCD: Qualified Certificate Policy for qualified certificates issued to the public, requiring use of secure signature-creation devices

### Evaluation Target

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

#### SSC GDL Class 2-4 QCA:

<b>Issuer of CA certificate (Root CA or intermediate CA): CN = SSC GDL CA Root A Certificate Serial Number: 50 96 6e 72 bd 10 d6 8c 4f 6b c7 62 3f 9c 70 38</b>	
<b>Name of CA (as in certificate)</b>	<b>serial number of certificate</b>
CN = SSC GDL Class 2-4 QCA	61 39 bb 2c 00 00 00 00 00 02

#### SSC GDL Class VS 2-4 QCA:

<b>Issuer of CA certificate (Root CA or intermediate CA): CN = SSC GDL CA VS Root Certificate Serial Number: 33 bd 22 7b 2b bc 70 84 4c 20 5f 57 3f 94 55 f5</b>	
<b>Name of CA (as in certificate)</b>	<b>serial number of certificate</b>
CN = C GDL VS Class 2-4 QCA	61 26 aa dd 00 00 00 00 00 02

together with the Certificate Policy (CP) of the operator:

- “Certificate Policy SSC GDL CA”, version 4.4 as of 2013-07-12, Skaitmeninio Sertifikavimo Centras

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

- “Certification Practice Statement SSC GDL CA”, version 4.7 as of 2014-04-22, 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 101 456 contains the following requirements:

### **1 Certification Practice Statement (CPS)**

The CA shall ensure that it demonstrates the reliability necessary for providing certification services (see the Directive 1999/98/EC, annex II (a)).

### **2 Public key infrastructure - Key management life cycle**

The CA shall ensure that CA keys are generated in controlled circumstances (see the Directive 1999/93/EC, annex II (g) and annex II (f)).

The CA shall ensure that CA private keys remain confidential and maintain their integrity (see the Directive 1999/93/EC, annex II (g) and annex II (f)).

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 (see the Directive 1999/93/EC, annex II (g) and annex II (f)).



Subject private signing keys shall not be held in a way which provides a backup decryption capability, allowing authorized entities under certain conditions to decrypt data using information supplied by one or more parties (commonly called key escrow) (see the Directive 1999/93/EC, annex II (j)).

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 (see the Directive 1999/93/EC, annex II (g) and annex II (f)).

The CA shall ensure the security of cryptographic hardware throughout its lifecycle (see the Directive 1999/93/EC, annex II (f)).

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 (see the Directive 1999/93/EC, annex II (f) and annex II (j)).

The CA shall ensure that if it issues SSCD this is carried out securely (see the Directive 1999/93/EC, annex III).

### **3 Public key infrastructure - Certificate Management life cycle**

The CA shall ensure that subjects are properly identified and authenticated; and that subject certificate requests are complete, accurate and duly authorized (see the Directive 1999/93/EC, annex II (d)).

The CA shall ensure that requests for certificates issued to a subject who has already previously been registered 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 (see the Directive 1999/93/EC, annex II (g)).

The CA shall ensure that it issues certificates securely to maintain their authenticity (see the Directive 1999/93/EC, annex II (g)).

The CA shall ensure that the terms and conditions are made available to subscribers and relying parties (see the Directive 1999/93/EC, annex II (k)).

The CA shall ensure that certificates are made available as necessary to subscribers, subjects and relying parties (see the Directive 1999/93/EC, annex II (l)).

The CA shall ensure that certificates are revoked in a timely manner based on authorized and validated certificate revocation requests (see the Directive 1999/93/EC, annex II (b)).

#### **4 CA management and operation**

The CA shall ensure that administrative and management procedures are applied which are adequate and correspond to recognized standards (see the Directive 1999/93/EC, annex II (e), 2nd part).

The CA shall ensure that its assets and information receive an appropriate level of protection (see the Directive 1999/93/EC, annex II (e)).

The CA shall ensure that personnel and hiring practices enhance and support the trustworthiness of the CA's operations (see Directive 1999/93/EC, annex II (e) 1st part).

The CA shall ensure that physical access to critical services is controlled and physical risks to its assets minimized (see Directive 1999/93/EC, annex II (f)).

The CA shall ensure that the CA systems are secure and correctly operated, with minimal risk of failure (see the Directive 1999/93/EC, annex II (e)).

The CA shall ensure that CA system access is limited to properly authorized individuals (see the Directive 1999/93/EC, annex II (f)).

The CA shall use trustworthy systems and products that are protected against modification (see the Directive 1999/93/EC, annex II (f)).

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 (see the Directive 1999/93/EC, annex II (a)).

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 as covered by the certificate policy, and ensure continued maintenance of records required to provide evidence of certification for the purposes of legal proceedings (see the Directive 1999/93/EC, annex II (i)).

The CA shall ensure compliance with legal requirements (see the Directive 1999/93/EC, article 8).

The CA shall ensure that all relevant information concerning a qualified 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 (see the Directive 1999/93/EC, annex II (i)).

**TÜV**<sup>®</sup>

## **5 Organizational**

The CA shall ensure that its organization is reliable (see Directive 1999/93/EC, annex II (a)).