

# Mozilla - CA Program

Case Information			
<b>Case Number</b>	00000039	<b>Case Record Type</b>	CA Owner/Root Inclusion Request
<b>CA Owner/Certificate Name</b>	SSC, Skaitmeninio Sertifikavimo Centras	<b>Request Status</b>	Ready for Public Discussion

Additional Case Information			
<b>Subject</b>	SSC Root inclusion requested	<b>Case Reason</b>	New Owner/Root inclusion requested

Bugzilla Information	
<b>Link to Bugzilla Bug</b>	<a href="http://bugzilla.mozilla.org/show_bug.cgi?id=379152">http://bugzilla.mozilla.org/show_bug.cgi?id=379152</a>

General information about CA's associated organization			
<b>CA Email Alias 1</b>	itpro@ssc.lt		
<b>CA Email Alias 2</b>			
<b>Company Website</b>	<a href="http://www.ssc.lt/">http://www.ssc.lt/</a>	<b>Verified?</b>	Verified
<b>Organizational Type</b>	Private Corporation	<b>Verified?</b>	Verified
<b>Organizational Type (Others)</b>		<b>Verified?</b>	Not Applicable
<b>Geographic Focus</b>	Lithuania and the EU market	<b>Verified?</b>	Verified
<b>Primary Market / Customer Base</b>	SSC is a Qualified CA (QCA) and a Trusted Service Provider (TSP) that issues certificates to public institutions, private organizations and natural persons.	<b>Verified?</b>	Verified
<b>Impact to Mozilla Users</b>	Since 2005 SSC CA operates the first QCA in Lithuania and serves all major public sector institutions, International and local businesses, citizens. Mozilla users: TLS based mail server/client authentication, email signing and encryption; Public sector websites (client and server) and e-services; FireFox based business applications; FireFox based e-service consumers, citizens.	<b>Verified?</b>	Verified

Response to Mozilla's list of Recommended Practices			
<b>Recommended Practices</b>	<a href="https://wiki.mozilla.org/CA:Recommended_Practices#CA_Recommended_Practices">https://wiki.mozilla.org/CA:Recommended_Practices#CA_Recommended_Practices</a>	<b>Recommended Practices Statement</b>	I have reviewed Mozilla's list of Recommended Practices, and confirm that we follow those practices, with exceptions and clarifications noted in the text box below.

<b>CA's Response to Recommended Practices</b>	<ul style="list-style-type: none"> <li>* Revocation of Compromised Certificates -- CPS section 4.9.1</li> <li>* Domain Owned by Natural Person -- according to ETSI QC profile</li> <li>* OCSP -- All issued EE certs provide OCSP access info.</li> </ul>	<b>Verified?</b>	Verified
---	--	------------------	----------

## Response to Mozilla's list of Potentially Problematic Practices

<b>Potentially Problematic Practices</b>	<a href="https://wiki.mozilla.org/CA:Problematic_Practices#Potentially_problematic_CA_practices">https://wiki.mozilla.org/CA:Problematic_Practices#Potentially_problematic_CA_practices</a>	<b>Problematic Practices Statement</b>	I have reviewed Mozilla's list of Potentially Problematic Practices, and confirm that we do not do those practices, with exceptions and clarifications noted in the text box below.
--	---	--	---

<b>CA's Response to Problematic Practices</b>	<ul style="list-style-type: none"> <li>* Email Address Prefixes for DV Certs -- admin@, administrator@, webmaster@, hostmaster@, postmaster@</li> <li>* Distributing generated private keys in PKCS#12 files -- Where applicable, private keys are generated by the CA only on SSCD.</li> <li>* SSC operates its services with exclusively owned/managed resources only.</li> </ul>	<b>Verified?</b>	Verified
---	---	------------------	----------

## Root Case Record # 1

### Root Case Information

<b>Root Certificate Name</b>	SSC GDL CA Root A	<b>Root Case No</b>	R00000048
<b>Request Status</b>	Ready for Public Discussion	<b>Case Number</b>	00000039

### Additional Root Case Information

<b>Subject</b>	Include SSC GDL CA Root A root
----------------	--------------------------------

### Technical Information about Root Certificate

<b>O From Issuer Field</b>	Skaitmeninio sertifikavimo centras	<b>Verified?</b>	Verified
<b>OU From Issuer Field</b>	CA ROOT Services	<b>Verified?</b>	Verified
<b>Certificate Summary</b>	This root has two internally-operated subordinate CAs that issue client (authentication, signing, and encryption) certificates.	<b>Verified?</b>	Verified
<b>Root Certificate Download URL</b>	<a href="https://gdl.repository.ssc.lt/certs/roota.crt">https://gdl.repository.ssc.lt/certs/roota.crt</a>	<b>Verified?</b>	Verified
<b>Valid From</b>	2013 Jun 04	<b>Verified?</b>	Verified
<b>Valid To</b>	2033 Jun 04	<b>Verified?</b>	Verified
<b>Certificate Version</b>	3	<b>Verified?</b>	Verified
<b>Certificate Signature Algorithm</b>	SHA-256	<b>Verified?</b>	Verified
<b>Signing Key Parameters</b>	4096	<b>Verified?</b>	Verified
<b>Test Website URL (SSL) or Example Cert</b>	Example Cert: <a href="https://gdl.repository.ssc.lt/certs/test-v-class2-4qca.cer">https://gdl.repository.ssc.lt/certs/test-v-class2-4qca.cer</a>	<b>Verified?</b>	Verified

<b>CRL URL(s)</b>	<a href="https://gdl.repository.ssc.lt/crls/class2-4qca.crl">https://gdl.repository.ssc.lt/crls/class2-4qca.crl</a> NextUpdate for CRLs of end-entity certs: 7 days CRL updates: please see section 4.9.7 of CPS	<b>Verified?</b>	Verified
<b>OCSP URL(s)</b>	<a href="http://class2-4qca.ocsp.gdl.ssc.lt/">http://class2-4qca.ocsp.gdl.ssc.lt/</a> Maximum expiration time of OCSP responses: 5 min.	<b>Verified?</b>	Verified
<b>Revocation Tested</b>	Not requesting Websites trust bit for this root.	<b>Verified?</b>	Not Applicable
<b>Trust Bits</b>	Code; Email	<b>Verified?</b>	Verified
<b>SSL Validation Type</b>		<b>Verified?</b>	Not Applicable
<b>EV Policy OID(s)</b>	Not EV	<b>Verified?</b>	Not Applicable
<b>EV Tested</b>	Not applicable.	<b>Verified?</b>	Not Applicable
<b>Root Stores Included In</b>	Microsoft	<b>Verified?</b>	Verified
<b>Mozilla Applied Constraints</b>	None	<b>Verified?</b>	Verified

### Digital Fingerprint Information

<b>SHA-1 Fingerprint</b>	0C:20:09:A4:A8:8D:8B:42:02:18:52:50:54:0C:C4:2B:DF:B5:B0:89	<b>Verified?</b>	Verified
<b>SHA-256 Fingerprint</b>	B0:42:8B:08:C2:28:C4:3F:6F:9A:A0:FC:29:E9:D6:02:ED:10:98:FF:6F:15:3C:67:33:38:3F:EA:17:21:65:28	<b>Verified?</b>	Verified

### CA Hierarchy Information

<b>CA Hierarchy</b>	This root has two internally-operated Intermediate/Issuing CAs: 1. SSC GDL Class 1 CA -- Issues technically functional certificates with no identity assurances. 2. SSC GDL Class 2-4 QCA -- Issues QCs, SSL/TLS client (authentication/signing/encryption) and CS certificates only to Public.	<b>Verified?</b>	Verified
<b>Externally Operated SubCAs</b>	None, and none planned. The CPS does appear to allow for externally-operated subCAs in the future. CPS section 1.3.1: In the event when any of the CAs listed above in the table become a Subject of a third party issued certificate, the CA shall disclose all cross signing certificates.	<b>Verified?</b>	Verified
<b>Cross Signing</b>	None, and none planned.	<b>Verified?</b>	Verified
<b>Technical Constraint on 3rd party Issuer</b>	CPS section 1.3.2: SSC PKI currently operates a RA which is a wholly owned division of SSC. Besides establishing enrollment procedures, identity verification, identification and authentication of applicants the RA also conveys the Root and CA public key certificates and performs other functions detailed in this CPS. * Currently SSC doesn't have third-party RAs, however may have registration	<b>Verified?</b>	Verified

## Verification Policies and Practices

<b>Policy Documentation</b>	<p>Documents are provided in Lithuanian and English. Lithuanian: CP: <a href="https://gdl.repository.ssc.lt/lt/talpykla/dokumentai/sertifikato-taisykles-ssc-gdl-ca-v4.4.pdf">https://gdl.repository.ssc.lt/lt/talpykla/dokumentai/sertifikato-taisykles-ssc-gdl-ca-v4.4.pdf</a> CPS: <a href="https://gdl.repository.ssc.lt/lt/talpykla/dokumentai/sertifikavimo-veiklos-nuostatai-ssc-gdl-ca-v4.7.pdf">https://gdl.repository.ssc.lt/lt/talpykla/dokumentai/sertifikavimo-veiklos-nuostatai-ssc-gdl-ca-v4.7.pdf</a></p> <p>Documents SSC intends to change in the near future. <a href="https://gdl.repository.ssc.lt/en/repository/working-documents/">https://gdl.repository.ssc.lt/en/repository/working-documents/</a></p> <p>Draft CPS v4.10: <a href="https://gdl.repository.ssc.lt/en/repository/working-documents/certificate-practice-statement-v4.10.pdf">https://gdl.repository.ssc.lt/en/repository/working-documents/certificate-practice-statement-v4.10.pdf</a></p>	<b>Verified?</b>	Verified
<b>CA Document Repository</b>	<a href="https://gdl.repository.ssc.lt/en/repository/documents/">https://gdl.repository.ssc.lt/en/repository/documents/</a>	<b>Verified?</b>	Verified
<b>CP Doc Language</b>	English		
<b>CP</b>	<a href="https://gdl.repository.ssc.lt/en/repository/documents/certificate-policy-ssc-gdl-ca-v4.4.pdf">https://gdl.repository.ssc.lt/en/repository/documents/certificate-policy-ssc-gdl-ca-v4.4.pdf</a>	<b>Verified?</b>	Verified
<b>CP Doc Language</b>	English		
<b>CPS</b>	<a href="https://gdl.repository.ssc.lt/en/repository/documents/certificate-practice-statement-ssc-gdl-ca-v4.7.pdf">https://gdl.repository.ssc.lt/en/repository/documents/certificate-practice-statement-ssc-gdl-ca-v4.7.pdf</a>	<b>Verified?</b>	Verified
<b>Other Relevant Documents</b>	RPA: <a href="https://gdl.repository.ssc.lt/en/repository/documents/ssc-gdl-ca-rpa-v2.pdf">https://gdl.repository.ssc.lt/en/repository/documents/ssc-gdl-ca-rpa-v2.pdf</a>	<b>Verified?</b>	Verified
<b>Auditor Name</b>	TÜV Informationstechnik GmbH	<b>Verified?</b>	Verified
<b>Auditor Website</b>	<a href="https://www.tuvit.de">https://www.tuvit.de</a>	<b>Verified?</b>	Verified
<b>Auditor Qualifications</b>	<a href="http://www.dakks.de/en/content/accredited-bodies-dakks">http://www.dakks.de/en/content/accredited-bodies-dakks</a>	<b>Verified?</b>	Verified
<b>Standard Audit</b>	<a href="https://www.tuvit.de/data/content_data/tuevit_en/6730UE_s.pdf">https://www.tuvit.de/data/content_data/tuevit_en/6730UE_s.pdf</a>	<b>Verified?</b>	Verified
<b>Standard Audit Type</b>	ETSI TS 101 456	<b>Verified?</b>	Verified
<b>Standard Audit Statement Date</b>	7/4/2014	<b>Verified?</b>	Verified
<b>BR Audit</b>		<b>Verified?</b>	Not Applicable
<b>BR Audit Type</b>		<b>Verified?</b>	Not Applicable
<b>BR Audit Statement Date</b>		<b>Verified?</b>	Not Applicable
<b>EV Audit</b>		<b>Verified?</b>	Not Applicable
<b>EV Audit Type</b>		<b>Verified?</b>	Not Applicable
<b>EV Audit Statement Date</b>		<b>Verified?</b>	Not Applicable
<b>BR Commitment to Comply</b>		<b>Verified?</b>	Not Applicable

<b>SSL Verification Procedures</b>	Not requesting Websites trust bit for this root.	<b>Verified?</b>	Not Applicable
<b>EV SSL Verification Procedures</b>		<b>Verified?</b>	Not Applicable
<b>Organization Verification Procedures</b>	CPS sections 3.2.2 through 3.2.5. CPS section 4.1  For each type of entities we verify physical, legal, operational existence and for legal entities we also verify the relationship (representation/authorization) between a physical entity and associated legal entity.  The verification procedures above are applicable to all types of certificates issued by the CA (to the level of assurance required by appropriate certificate policy).	<b>Verified?</b>	Verified
<b>Email Address Verification Procedures</b>	CPS section 3.2.6: Information about the Subject, including email address, is included in certificates only after it is reliably verified.  DRAFT CPS v4.10 section 4: For digital assets whose identifiers are maintained by third parties (e.g. email addresses, domain names etc.) the RA verifies operational existence by directly accessing/using the resource (e.g. a server) or communicating through the resource (e.g. email address) and legal existence - by obtaining independent ownership conformation from the associated registrar.	<b>Verified?</b>	Verified
<b>Code Signing Subscriber Verification Pro</b>	CPS sections 3.2.2 through 3.2.5, and 3.2.7	<b>Verified?</b>	Verified
<b>Multi-Factor Authentication</b>	CPS section 5.	<b>Verified?</b>	Verified
<b>Network Security</b>	The CA's Security management documentation incorporates provisions of CA/B Forum "Network and Certificate System Security Requirements". An automatic procedure is run regularly to detect any "suspicious mis-issued" certificates including for high-profile domains. The certificate issuance system, that is not accessible from the public Internet, can be quickly shut down in case of any emergency alert. CPS section 6.7	<b>Verified?</b>	Verified

<b>Link to Publicly Disclosed and Audited subordinate CA Certificates</b>			
<b>Publicly Disclosed &amp; Audited subCAs</b>	<a href="https://gdl.repository.ssc.lt/en/repository/authority-certificates-and-crls/">https://gdl.repository.ssc.lt/en/repository/authority-certificates-and-crls/</a>	<b>Verified?</b>	Verified

## Root Case Record # 2

<b>Root Case Information</b>
------------------------------

<b>Root Certificate Name</b>	SSC GDL CA Root B	<b>Root Case No</b>	R00000049
<b>Request Status</b>	Ready for Public Discussion	<b>Case Number</b>	00000039

### Additional Root Case Information

**Subject** Include SSC GDL CA Root B root

### Technical Information about Root Certificate

<b>O From Issuer Field</b>	Skaitmeninio sertifikavimo centras	<b>Verified?</b>	Verified
<b>OU From Issuer Field</b>	CA ROOT Services	<b>Verified?</b>	Verified
<b>Certificate Summary</b>	This root has two internally-operated intermediate/issuing CAs, which sign SSL/TLS and CS certificates.	<b>Verified?</b>	Verified
<b>Root Certificate Download URL</b>	<a href="https://gdl.repository.ssc.lt/certs/rootb.crt">https://gdl.repository.ssc.lt/certs/rootb.crt</a>	<b>Verified?</b>	Verified
<b>Valid From</b>	2013 Jun 04	<b>Verified?</b>	Verified
<b>Valid To</b>	2033 Jun 04	<b>Verified?</b>	Verified
<b>Certificate Version</b>	3	<b>Verified?</b>	Verified
<b>Certificate Signature Algorithm</b>	SHA-256	<b>Verified?</b>	Verified
<b>Signing Key Parameters</b>	4096	<b>Verified?</b>	Verified
<b>Test Website URL (SSL) or Example Cert</b>	<a href="https://evssl.gdl.ssc.lt/">https://evssl.gdl.ssc.lt/</a>	<b>Verified?</b>	Verified
<b>CRL URL(s)</b>	<a href="https://gdl.repository.ssc.lt/crls/nhca.crl">https://gdl.repository.ssc.lt/crls/nhca.crl</a> <a href="https://gdl.repository.ssc.lt/crls/evca.crl">https://gdl.repository.ssc.lt/crls/evca.crl</a> <a href="http://gdl.repository.ssc.lt/crls/rootb.crl">http://gdl.repository.ssc.lt/crls/rootb.crl</a> NextUpdate for CRLs of end-entity certs: 7 days CRL updates: please see section 4.9.7 of CPS	<b>Verified?</b>	Verified
<b>OCSP URL(s)</b>	<a href="http://nhca.ocsp.gdl.ssc.lt/">http://nhca.ocsp.gdl.ssc.lt/</a> <a href="http://evca.ocsp.gdl.ssc.lt/">http://evca.ocsp.gdl.ssc.lt/</a> <a href="http://rootb.ocsp.gdl.ssc.lt/">http://rootb.ocsp.gdl.ssc.lt/</a> Maximum expiration time of OCSP responses: 5 min.	<b>Verified?</b>	Verified
<b>Revocation Tested</b>	<a href="http://certificate.revocationcheck.com/evssl.gdl.ssc.lt">http://certificate.revocationcheck.com/evssl.gdl.ssc.lt</a>	<b>Verified?</b>	Verified
<b>Trust Bits</b>	Code; Email; Websites	<b>Verified?</b>	Verified
<b>SSL Validation Type</b>	OV; EV	<b>Verified?</b>	Verified
<b>EV Policy OID(s)</b>	2.23.140.1.1	<b>Verified?</b>	Verified
<b>EV Tested</b>	// CN=SSC GDL CA Root B,OU=CA ROOT Services,O=Skaitmeninio sertifikavimo centras,C=LT "2.23.140.1.1", "SSC EV OID", SEC_OID_UNKNOWN, { 0xC3, 0x1E, 0xEF, 0x56, 0x82, 0xAB, 0xB5, 0x51, 0xEB, 0xC8, 0x28, 0xDE, 0xD8, 0x40, 0x98, 0x51, 0x8A, 0x67, 0x68, 0x52, 0x6D, 0x15, 0x2E, 0xE1, 0x64, 0xCF, 0xB9, 0x72, 0xA1, 0x42, 0x5D, 0x53 },	<b>Verified?</b>	Verified

```
"MHExCzAJBgNVBAYTAkxUMSswKQYDVQQKEyJTa2FpdG1lbmluaW8gc2VydGhmaWth"
"dmltbyBjZW50cmFzMRkwFwYDVQQLExBDQSBST09UIFNlcnZpY2VzMR0wGAYDVQQD"
"ExFTU0MgR0RMIENBIFJvb3QgQg==",
"PoxPvOQpg4JNhFWO1TWAzw==",
Success!
```

<b>Root Stores Included In</b>	Microsoft	<b>Verified?</b>	Verified
<b>Mozilla Applied Constraints</b>	None	<b>Verified?</b>	Verified

### Digital Fingerprint Information

<b>SHA-1 Fingerprint</b>	C8:60:A3:18:FC:F5:B7:13:0B:10:07:AD:7F:61:4A:40:FF:FF:18:5F	<b>Verified?</b>	Verified
<b>SHA-256 Fingerprint</b>	C3:1E:EF:56:82:AB:B5:51:EB:C8:28:DE:D8:40:98:51:8A:67:68:52:6D:15:2E:E1:64:CF:B9:72:A1:42:5D:53	<b>Verified?</b>	Verified

### CA Hierarchy Information

<b>CA Hierarchy</b>	This CA has two internally-operated Intermediate/Issuing CAs: 1. SSC GDL NH CA -- Issues device/e-service certificates including SSL/TLS and CS certificates. 2. SSC GDL EV CA -- Issues exclusively EV SSL and Qualified web site certificates (see section 8 of REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014).	<b>Verified?</b>	Verified
<b>Externally Operated SubCAs</b>	None, and none planned.	<b>Verified?</b>	Verified
<b>Cross Signing</b>	None, and none planned.	<b>Verified?</b>	Verified
<b>Technical Constraint on 3rd party Issuer</b>	CPS section 1.3.2: SSC PKI currently operates a RA which is a wholly owned division of SSC. Besides establishing enrollment procedures, identity verification, identification and authentication of applicants the RA also conveys the Root and CA public key certificates and performs other functions detailed in this CPS.  * Currently SSC doesn't have third-party RAs, however may have registration partners in the future. * According to ETSI TS 102 042 Registration service only verifies identity and, if applicable, any specific attributes of a subject. The results of this service are passed to the certificate generation service. So, based on this ETSI definition, RAs are not allowed to issue certificates. Activities of registration service personnel, including those employed by SSC, are constrained/controlled by SSC's RA management software which has no certificate generation/issuing capabilities.	<b>Verified?</b>	Verified

### Verification Policies and Practices

<b>Policy Documentation</b>	Documents are provided in Lithuanian and English. Lithuanian: CP: <a href="https://gdl.repository.ssc.lt/lt/talpykla/dokumentai/sertifikato-taisykles-ssc-gdl-ca-v4.4.pdf">https://gdl.repository.ssc.lt/lt/talpykla/dokumentai/sertifikato-taisykles-ssc-gdl-ca-v4.4.pdf</a> CPS: <a href="https://gdl.repository.ssc.lt/lt/talpykla/dokumentai/sertifikavimo-veiklos-nuostatai-ssc-gdl-ca-v4.7.pdf">https://gdl.repository.ssc.lt/lt/talpykla/dokumentai/sertifikavimo-veiklos-nuostatai-ssc-gdl-ca-v4.7.pdf</a>  Documents SSC intends to change in the near future. <a href="https://gdl.repository.ssc.lt/en/repository/working-documents/">https://gdl.repository.ssc.lt/en/repository/working-documents/</a>  Draft CPS v4.10: <a href="https://gdl.repository.ssc.lt/en/repository/working-documents/certificate-practice-statement-v4.10.pdf">https://gdl.repository.ssc.lt/en/repository/working-documents/certificate-practice-statement-v4.10.pdf</a>	<b>Verified?</b>	Verified
<b>CA Document Repository</b>	<a href="https://gdl.repository.ssc.lt/en/repository/documents/">https://gdl.repository.ssc.lt/en/repository/documents/</a>	<b>Verified?</b>	Verified
<b>CP Doc Language</b>	English		
<b>CP</b>	<a href="https://gdl.repository.ssc.lt/en/repository/documents/certificate-policy-ssc-gdl-ca-v4.4.pdf">https://gdl.repository.ssc.lt/en/repository/documents/certificate-policy-ssc-gdl-ca-v4.4.pdf</a>	<b>Verified?</b>	Verified
<b>CP Doc Language</b>	English		
<b>CPS</b>	<a href="https://gdl.repository.ssc.lt/en/repository/documents/certificate-practice-statement-ssc-gdl-ca-v4.7.pdf">https://gdl.repository.ssc.lt/en/repository/documents/certificate-practice-statement-ssc-gdl-ca-v4.7.pdf</a>	<b>Verified?</b>	Verified
<b>Other Relevant Documents</b>	RPA: <a href="https://gdl.repository.ssc.lt/en/repository/documents/ssc-gdl-ca-rpa-v2.pdf">https://gdl.repository.ssc.lt/en/repository/documents/ssc-gdl-ca-rpa-v2.pdf</a>	<b>Verified?</b>	Verified
<b>Auditor Name</b>	TÜV Informationstechnik GmbH	<b>Verified?</b>	Verified
<b>Auditor Website</b>	<a href="https://www.tuvit.de/">https://www.tuvit.de/</a>	<b>Verified?</b>	Verified
<b>Auditor Qualifications</b>	<a href="http://www.dakks.de/en/content/accredited-bodies-dakks">http://www.dakks.de/en/content/accredited-bodies-dakks</a>	<b>Verified?</b>	Verified
<b>Standard Audit</b>	<a href="https://gdl.repository.ssc.lt/en/audit/2015/">https://gdl.repository.ssc.lt/en/audit/2015/</a>	<b>Verified?</b>	Verified
<b>Standard Audit Type</b>	ETSI TS 102 042	<b>Verified?</b>	Verified
<b>Standard Audit Statement Date</b>	7/4/2014	<b>Verified?</b>	Verified
<b>BR Audit</b>	<a href="https://www.tuvit.de/data/content_data/tuevit_en/6729UE_s.pdf">https://www.tuvit.de/data/content_data/tuevit_en/6729UE_s.pdf</a>	<b>Verified?</b>	Verified
<b>BR Audit Type</b>	ETSI TS 102 042	<b>Verified?</b>	Verified
<b>BR Audit Statement Date</b>	7/4/2014	<b>Verified?</b>	Verified
<b>EV Audit</b>	<a href="https://www.tuvit.de/data/content_data/tuevit_en/6729UE_s.pdf">https://www.tuvit.de/data/content_data/tuevit_en/6729UE_s.pdf</a>	<b>Verified?</b>	Verified
<b>EV Audit Type</b>	ETSI TS 102 042	<b>Verified?</b>	Verified
<b>EV Audit Statement Date</b>	7/4/2014	<b>Verified?</b>	Verified
<b>BR Commitment to Comply</b>	CPS section 1.4: SSC GDL CA conforms to the current versions of the [CABF-BR] and [CABF-EV]15. In the event of any inconsistency between this CPS and those Guidelines, the Guidelines take precedence over the CPS.	<b>Verified?</b>	Verified



<b>SSL Verification Procedures</b>	<p>DRAFT CPS v4.10 section 3.2.5: If the Subject of certificate is a service offered via a network, the Applicant must provide identifying information and an acceptable proof of ownership which shall include unique software or service name (e.g. DNS name), service attributes to be included in the certificate, if any, and owner's contact information.</p> <p>The CA shall validate that the Applicant is:</p> <ul style="list-style-type: none"> <li>(a) authorized to request a certificate for the service;</li> <li>(b) the real owner owner of the service (through an appropriate reliable 3rd party database);</li> <li>(c) able to demonstrate control of the domain (by manipulating DNS records and server configuration).</li> </ul> <p>Section 4: For digital assets whose identifiers are maintained by third parties (e.g. email addresses, domain names etc.) the RA verifies operational existence by directly accessing/using the resource (e.g. a server) or communicating through the resource (e.g. email address) and legal existence - by obtaining independent ownership conformation from the associated registrar.</p>	<b>Verified?</b>	Verified
<b>EV SSL Verification Procedures</b>	<p>CPS section 4.1: For EVCP and EVCP+ certificates extra verification measures are taken as defined in [CABF-EV] to ensure the Subscriber's legal, physical and operational existence. Proof of representation and authority to act on behalf of the Applicant has to be demonstrated in order to authenticate the signatures on EVCP and EVCP+ certificate application forms.</p> <p>The RA checks that the organization is the legal holder of its name by mapping the information provided in the Extended Validation certificate application with information of official Government Registers (Legal entity DB, TAX payers DB, Social Security DB) that confirms the existence of the organization.</p> <p>The RA checks the official postal address of the applicant along with Applicant's main business phone number.</p> <p>In case a technical contact is also the certificate requester with no approval rights, the certificate application form has to be signed by an authorized certificate approver, whose signature has to be verified. The RA communicates with the Certificate signer by phone to ensure validity of authorization. The RA may also communicate with the Certificate signer by postal mail sent to the applicant's place of business.</p>	<b>Verified?</b>	Verified
<b>Organization Verification Procedures</b>	<p>CPS sections 3.2.2 through 3.2.5. CPS section 4.1</p> <p>For each type of entities we verify physical, legal, operational existence and</p>	<b>Verified?</b>	Verified

for legal entities we also verify the relationship (representation/authorization) between a physical entity and associated legal entity.

The verification procedures above are applicable to all types of certificates issued by the CA (to the level of assurance required by appropriate certificate policy).

<b>Email Address Verification Procedures</b>	CPS section 3.2.6: Information about the Subject, including email address, is included in certificates only after it is reliably verified.  DRAFT CPS v4.10 section 4: For digital assets whose identifiers are maintained by third parties (e.g. email addresses, domain names etc.) the RA verifies operational existence by directly accessing/using the resource (e.g. a server) or communicating through the resource (e.g. email address) and legal existence - by obtaining independent ownership conformation from the associated registrar.	<b>Verified?</b>	Verified
<b>Code Signing Subscriber Verification Pro</b>	CPS sections 3.2.2 through 3.2.5, and 3.2.7	<b>Verified?</b>	Verified
<b>Multi-Factor Authentication</b>	CPS section 4.2: Application processing for EVCP and EVCP+ certificates is finished after a person other than the one who performed initial Application information verification conducts an extra cross correlation CPS section 5.	<b>Verified?</b>	Verified
<b>Network Security</b>	The CA's Security management documentation incorporates provisions of CA/B Forum "Network and Certificate System Security Requirements". An automatic procedure is run regularly to detect any "suspicious mis-issued" certificates including for high-profile domains. The certificate issuance system, that is not accessible from the public Internet, can be quickly shut down in case of any emergency alert. CPS section 6.7	<b>Verified?</b>	Verified

<b>Link to Publicly Disclosed and Audited subordinate CA Certificates</b>			
<b>Publicly Disclosed &amp; Audited subCAs</b>	<a href="https://gdl.repository.ssc.lt/en/repository/authority-certificates-and-crls/">https://gdl.repository.ssc.lt/en/repository/authority-certificates-and-crls/</a>	<b>Verified?</b>	Verified

## Root Case Record # 3

<b>Root Case Information</b>			
<b>Root Certificate Name</b>	SSC GDL CA VS Root	<b>Root Case No</b>	R00000050
<b>Request Status</b>	Ready for Public Discussion	<b>Case Number</b>	00000039

## Additional Root Case Information

Subject Include SSC GDL CA VS Root root

## Technical Information about Root Certificate

O From Issuer Field	Skaitmeninio sertifikavimo centras	Verified?	Verified
OU From Issuer Field	VS ROOT Services	Verified?	Verified
Certificate Summary	This root has one internally-operated Intermediate/Issuing CA: SSC GDL VS Class 2-4 QCA -- Issues QCs, SSL/TLS client (authentication/signing/encryption) certificates to Government and Public institutions only.	Verified?	Verified
Root Certificate Download URL	<a href="https://gdl.repository.ssc.lt/certs/rootvs.crt">https://gdl.repository.ssc.lt/certs/rootvs.crt</a>	Verified?	Verified
Valid From	2013 Jun 04	Verified?	Verified
Valid To	2033 Jun 04	Verified?	Verified
Certificate Version	3	Verified?	Verified
Certificate Signature Algorithm	SHA-256	Verified?	Verified
Signing Key Parameters	4096	Verified?	Verified
Test Website URL (SSL) or Example Cert	Example Cert: <a href="https://gdl.repository.ssc.lt/certs/test-v-vsclass2-4qca.cer">https://gdl.repository.ssc.lt/certs/test-v-vsclass2-4qca.cer</a>	Verified?	Verified
CRL URL(s)	<a href="https://gdl.repository.ssc.lt/crls/vsclass2-4qca.crl">https://gdl.repository.ssc.lt/crls/vsclass2-4qca.crl</a> NextUpdate for CRLs of end-entity certs: 7 days; CRL updates: please see section 4.9.7 of CPS	Verified?	Verified
OCSP URL(s)	<a href="http://vsclass2-4qca.ocsp.gdl.ssc.lt/">http://vsclass2-4qca.ocsp.gdl.ssc.lt/</a> Maximum expiration time of OCSP responses: 5 min.	Verified?	Verified
Revocation Tested	Not requesting Websites trust bit for this root.	Verified?	Not Applicable
Trust Bits	Email	Verified?	Verified
SSL Validation Type		Verified?	Not Applicable
EV Policy OID(s)	Not EV	Verified?	Not Applicable
EV Tested	Not applicable	Verified?	Not Applicable
Root Stores Included In	Microsoft	Verified?	Verified
Mozilla Applied Constraints	None	Verified?	Verified

## Digital Fingerprint Information

SHA-1 Fingerprint	D2:69:5E:12:F5:92:E9:C8:EE:2A:4C:B8:D5:5E:29:5F:EE:6B:2D:31	Verified?	Verified
SHA-256 Fingerprint	BC:2A:BB:C4:9A:68:14:37:0D:17:E4:71:14:1C:22:79:43:11:C4:DD:DF:25:67:BE:37:28:3A:89:43:92:E5:D3	Verified?	Verified

## CA Hierarchy Information

<b>CA Hierarchy</b>	This root has one internally-operated Intermediate/Issuing CA: SSC GDL VS Class 2-4 QCA -- Issues QCs, SSL/TLS client (authentication/signing/encryption) certificates to Government and Public institutions only.	<b>Verified?</b>	Verified
<b>Externally Operated SubCAs</b>	None, and none planned.	<b>Verified?</b>	Verified
<b>Cross Signing</b>	None, and none planned.	<b>Verified?</b>	Verified
<b>Technical Constraint on 3rd party Issuer</b>	CPS section 1.3.2: SSC PKI currently operates a RA which is a wholly owned division of SSC. Besides establishing enrollment procedures, identity verification, identification and authentication of applicants the RA also conveys the Root and CA public key certificates and performs other functions detailed in this CPS. * Currently SSC doesn't have third-party RAs, however may have registration partners in the future.	<b>Verified?</b>	Verified

## Verification Policies and Practices

<b>Policy Documentation</b>	Documents are provided in Lithuanian and English. Lithuanian: CP: <a href="https://gdl.repository.ssc.lt/lt/talpykla/dokumentai/sertifikato-taisykles-ssc-gdl-ca-v4.4.pdf">https://gdl.repository.ssc.lt/lt/talpykla/dokumentai/sertifikato-taisykles-ssc-gdl-ca-v4.4.pdf</a> CPS: <a href="https://gdl.repository.ssc.lt/lt/talpykla/dokumentai/sertifikavimo-veiklos-nuostatai-ssc-gdl-ca-v4.7.pdf">https://gdl.repository.ssc.lt/lt/talpykla/dokumentai/sertifikavimo-veiklos-nuostatai-ssc-gdl-ca-v4.7.pdf</a>  Documents SSC intends to change in the near future. <a href="https://gdl.repository.ssc.lt/en/repository/working-documents/">https://gdl.repository.ssc.lt/en/repository/working-documents/</a>  Draft CPS v4.10: <a href="https://gdl.repository.ssc.lt/en/repository/working-documents/certificate-practice-statement-v4.10.pdf">https://gdl.repository.ssc.lt/en/repository/working-documents/certificate-practice-statement-v4.10.pdf</a>	<b>Verified?</b>	Verified
<b>CA Document Repository</b>	<a href="https://gdl.repository.ssc.lt/en/repository/documents/">https://gdl.repository.ssc.lt/en/repository/documents/</a>	<b>Verified?</b>	Verified
<b>CP Doc Language</b>	English		
<b>CP</b>	<a href="https://gdl.repository.ssc.lt/en/repository/documents/certificate-policy-ssc-gdl-ca-v4.4.pdf">https://gdl.repository.ssc.lt/en/repository/documents/certificate-policy-ssc-gdl-ca-v4.4.pdf</a>	<b>Verified?</b>	Verified
<b>CP Doc Language</b>	English		
<b>CPS</b>	<a href="https://gdl.repository.ssc.lt/en/repository/documents/certificate-practice-statement-ssc-gdl-ca-v4.7.pdf">https://gdl.repository.ssc.lt/en/repository/documents/certificate-practice-statement-ssc-gdl-ca-v4.7.pdf</a>	<b>Verified?</b>	Verified
<b>Other Relevant Documents</b>	RPA: <a href="https://gdl.repository.ssc.lt/en/repository/documents/ssc-gdl-ca-rpa-v2.pdf">https://gdl.repository.ssc.lt/en/repository/documents/ssc-gdl-ca-rpa-v2.pdf</a>	<b>Verified?</b>	Verified
<b>Auditor Name</b>	TÜV Informationstechnik GmbH	<b>Verified?</b>	Verified

<b>Auditor Website</b>	<a href="https://www.tuvit.de/">https://www.tuvit.de/</a>	<b>Verified?</b>	Verified
<b>Auditor Qualifications</b>	<a href="http://portal.etsi.org/TBSiteMap/ESI/TrustServiceProviders.aspx">http://portal.etsi.org/TBSiteMap/ESI/TrustServiceProviders.aspx</a>	<b>Verified?</b>	Verified
<b>Standard Audit</b>	<a href="https://gdl.repository.ssc.lt/en/audit/2015/">https://gdl.repository.ssc.lt/en/audit/2015/</a>	<b>Verified?</b>	Verified
<b>Standard Audit Type</b>	ETSI TS 101 456	<b>Verified?</b>	Verified
<b>Standard Audit Statement Date</b>	7/4/2014	<b>Verified?</b>	Verified
<b>BR Audit</b>		<b>Verified?</b>	Not Applicable
<b>BR Audit Type</b>		<b>Verified?</b>	Not Applicable
<b>BR Audit Statement Date</b>		<b>Verified?</b>	Not Applicable
<b>EV Audit</b>		<b>Verified?</b>	Not Applicable
<b>EV Audit Type</b>		<b>Verified?</b>	Not Applicable
<b>EV Audit Statement Date</b>		<b>Verified?</b>	Not Applicable
<b>BR Commitment to Comply</b>		<b>Verified?</b>	Not Applicable
<b>SSL Verification Procedures</b>	Not requesting Websites trust bit for this root.	<b>Verified?</b>	Not Applicable
<b>EV SSL Verification Procedures</b>		<b>Verified?</b>	Not Applicable
<b>Organization Verification Procedures</b>	<p>CPS sections 3.2.2 through 3.2.5. CPS section 4.1</p> <p>For each type of entities we verify physical, legal, operational existence and for legal entities we also verify the relationship (representation/authorization) between a physical entity and associated legal entity.</p> <p>The verification procedures above are applicable to all types of certificates issued by the CA (to the level of assurance required by appropriate certificate policy).</p>	<b>Verified?</b>	Verified
<b>Email Address Verification Procedures</b>	<p>CPS section 3.2.6: Information about the Subject, including email address, is included in certificates only after it is reliably verified.</p> <p>DRAFT CPS v4.10 section 4: For digital assets whose identifiers are maintained by third parties (e.g. email addresses, domain names etc.) the RA verifies operational existence by directly accessing/using the resource (e.g. a server) or communicating through the resource (e.g. email address) and legal existence - by obtaining independent ownership conformation from the associated registrar.</p>	<b>Verified?</b>	Verified
<b>Code Signing Subscriber Verification Pro</b>	Not requesting Code Signing trust bit for this root.	<b>Verified?</b>	Not Applicable
<b>Multi-Factor Authentication</b>	CPS section 5.	<b>Verified?</b>	Verified

<b>Network Security</b>	<p>The CA's Security management documentation incorporates provisions of CA/B Forum "Network and Certificate System Security Requirements".</p> <p>An automatic procedure is run regularly to detect any "suspicious mis-issued" certificates including for high-profile domains.</p> <p>The certificate issuance system, that is not accessible from the public Internet, can be quickly shut down in case of any emergency alert.</p> <p>CPS section 6.7</p>	<b>Verified?</b>	Verified
-------------------------	--	------------------	----------

---

**Link to Publicly Disclosed and Audited subordinate CA Certificates**

<b>Publicly Disclosed &amp; Audited subCAs</b>	<a href="https://gdl.repository.ssc.lt/en/repository/authority-certificates-and-crls/">https://gdl.repository.ssc.lt/en/repository/authority-certificates-and-crls/</a>	<b>Verified?</b>	Verified
--	---	------------------	----------

---