

Mozilla - CA Program

Case Information			
Case Number	00000039	Case Record Type	CA Owner/Root Inclusion Request
CA Owners/Certificate Name	SSC, Skaitmeninio Sertifikavimo Centras	Request Status	Need Information from CA

Additional Case Information			
Subject	Root inclusion requested	Case Reason	New Owner/Root inclusion requested

Bugzilla Information	
Link to Bugzilla Bug	http://bugzilla.mozilla.org/show_bug.cgi?id=379152

General information about CA's associated organization			
Company Website	http://www.ssc.lt/	Verified?	Verified
Organizational Type	Private Corporation	Verified?	Verified
Organizational Type (Others)		Verified?	Not Applicable
Primary Market / Customer Base	The Trusted Service Provider (TSP) issues certificates to public institutions, private organizations and natural persons. The TSP focus its activities on EU market. QUESTION: Who does the term "TSP" refer to? Is SSC the TSP? Or does SSC have external TSPs?	Verified?	Need Clarification From CA
Impact to Mozilla Users	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.	Verified?	Verified

Response to Mozilla's list of Recommended Practices			
Recommended Practices	https://wiki.mozilla.org/CA:Recommended_Practices#CA_Recommended_Practices	Recommended Practices Statement	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.
CA's Response to Recommended Practices	Revocation of Compromised Certificates -- CPS section 4.9.1 Domain Owned by Natural Person -- according to ETSI QC profile	Verified?	Verified

OCSP -- All issued EE certs provide OCSP access info.

Response to Mozilla's list of Potentially Problematic Practices

Potentially Problematic Practices	https://wiki.mozilla.org/CA:Problematic_Practices#Potentially_problematic_CA_practices	Problematic Practices Statement	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.
CA's Response to Problematic Practices	Email Address Prefixes for DV Certs -- admin@, administrator@, webmaster@, hostmaster@, postmaster@ Distributing generated private keys in PKCS#12 files -- Where applicable, private keys are generated by the CA only on SSCD.	Verified?	Verified

Root Case Record # 1

Root Case Information

Root Case No	R00000048	Case Number	00000039
Request Status	Need Information from CA	Root Certificate Name	SSC GDL CA Root A

Additional Root Case Information

Subject Include SSC GDL CA Root A root

Technical Information about Root Certificate

O From Issuer Field	Skaitmeninio sertifikavimo centras	Verified?	Verified
OU From Issuer Field	CA ROOT Services	Verified?	Verified
Certificate Summary	This root has two internally-operated subordinate CAs that issue client (authentication, signing, and encryption) certificates.	Verified?	Verified
Root Certificate Download URL	https://gdl.repository.ssc.lt/certs/roota.crt	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: https://gdl.repository.ssc.lt/certs/test-v-class2-4qca.cer	Verified?	Verified
CRL URL(s)	https://gdl.repository.ssc.lt/crls/class2-4qca.crl NextUpdate for CRLs of end-entity certs: 7 days CRL updates: please see section 4.9.7 of CPS	Verified?	Verified

OCSP URL(s)	http://class2-4gca.ocsp.gdl.ssc.lt/ Maximum expiration time of OCSP responses: 5 min.	Verified?	Verified
Trust Bits	Code; 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		Verified?	Need Clarification From CA
Mozilla Applied Constraints	None	Verified?	Verified

Digital Fingerprint Information

SHA-1 Fingerprint	0C:20:09:A4:A8:8D:8B:42:02:18:52:50:54:0C:C4:2B:DF:B5:B0:89	Verified?	Verified
SHA-256 Fingerprint	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	Verified?	Verified

CA Hierarchy Information

CA Hierarchy	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.	Verified?	Verified
Externally Operated SubCAs	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.	Verified?	Verified
Cross Signing	None, and none planned.	Verified?	Verified
Technical Constraint on 3rd party Issuer	QUESTION: Can there be third-party RAs? If yes, what sorts of certs can they issue, and how are they constrained? 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.	Verified?	Need Clarification From CA

Verification Policies and Practices

Policy Documentation	Documents are provided in Lithuanian and English. Lithuanian:	Verified?	Verified
-----------------------------	--	------------------	----------

CP: <https://gdl.repository.ssc.lt/lt/talpykla/dokumentai/sertifikato-taisykles-ssc-gdl-ca-v4.4.pdf>

CPS: <https://gdl.repository.ssc.lt/lt/talpykla/dokumentai/sertifikavimo-veiklos-nuostatai-ssc-gdl-ca-v4.7.pdf>

CA Document Repository	https://gdl.repository.ssc.lt/en/repository/documents/	Verified?	Verified
CP Doc Language	English		
CP	https://gdl.repository.ssc.lt/en/repository/documents/certificate-policy-ssc-gdl-ca-v4.4.pdf	Verified?	Verified
CP Doc Language	English		
CPS	https://gdl.repository.ssc.lt/en/repository/documents/certificate-practice-statement-ssc-gdl-ca-v4.7.pdf	Verified?	Verified
Other Relevant Documents	RPA: https://gdl.repository.ssc.lt/en/repository/documents/ssc-gdl-ca-rpa-v2.pdf	Verified?	Verified
Auditor Name	TÜV Informationstechnik GmbH	Verified?	Verified
Auditor Website	https://www.tuvit.de	Verified?	Verified
Auditor Qualifications	http://portal.etsi.org/TBSiteMap/ESI/TrustServiceProviders.aspx	Verified?	Verified
Standard Audit	https://gdl.repository.ssc.lt/en/audit/2015/	Verified?	Verified
Standard Audit Type	ETSI TS 101 456	Verified?	Verified
Standard Audit Statement Date	7/4/2014	Verified?	Verified
BR Audit		Verified?	Not Applicable
BR Audit Type		Verified?	Not Applicable
BR Audit Statement Date		Verified?	Not Applicable
EV Audit		Verified?	Not Applicable
EV Audit Type		Verified?	Not Applicable
EV Audit Statement Date		Verified?	Not Applicable
BR Commitment to Comply		Verified?	Not Applicable
SSL Verification Procedures	Not requesting Websites trust bit for this root.	Verified?	Not Applicable
EV SSL Verification Procedures		Verified?	Not Applicable
Organization Verification Procedures	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).	Verified?	Verified

Email Address Verification Procedures	The CP/CPS needs to describe the procedures for verifying that the email address to be included in the certificate is owned/controlled by the certificate subscriber. https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Email_Address_Control	Verified?	Need Clarification From CA
Code Signing Subscriber Verification Pro	I could not find specific information about the verification procedures for code signing certificate subscribers. See https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Identity_of_Code_Signing_Certificate_Subscriber	Verified?	Need Clarification From CA
Multi-Factor Authentication	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 QUESTION: What about non-EV cert issuance? See BR #16.5	Verified?	Need Clarification From CA
Network Security	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	Verified?	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	https://gdl.repository.ssc.lt/en/repository/authority-certificates-and-crls/	Verified?	Verified
--	---	-----------	----------

Root Case Record # 2

Root Case Information

Root Case No	R00000049	Case Number	00000039
Request Status	Need Information from CA	Root Certificate Name	SSC GDL CA Root B

Additional Root Case Information

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

Technical Information about Root Certificate

O From Issuer Field	Skaitmeninio sertifikavimo centras	Verified?	Verified
OU From Issuer Field	CA ROOT Services	Verified?	Verified
Certificate Summary	This root has two internally-operated intermediate/issuing CAs, which sign SSL/TLS and CS certificates.	Verified?	Verified
Root Certificate Download URL	https://gdl.repository.ssc.lt/certs/rootb.crt	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	https://evssl.gdl.ssc.lt/	Verified?	Verified
CRL URL(s)	https://gdl.repository.ssc.lt/crls/nhca.crl https://gdl.repository.ssc.lt/crls/evca.crl http://gdl.repository.ssc.lt/crls/rootb.crl NextUpdate for CRLs of end-entity certs: 7 days CRL updates: please see section 4.9.7 of CPS	Verified?	Verified
OCSP URL(s)	http://nhca.ocsp.gdl.ssc.lt/ http://evca.ocsp.gdl.ssc.lt/ http://rootb.ocsp.gdl.ssc.lt/ Maximum expiration time of OCSP responses: 5 min.	Verified?	Verified
Trust Bits	Code; Email; Websites	Verified?	Verified
SSL Validation Type	OV; EV	Verified?	Verified
EV Policy OID(s)	0.4.0.2042.1.4 (ETSI EVCP) 0.4.0.2042.1.5 (ETSI EVCP+) 2.23.140.1.1 (CAB Forum) QUESTION: Do you need all of these in https://mxr.mozilla.org/mozilla-central/source/security/certverifier/ExtendedValidation.cpp ? Or just the first one?	Verified?	Need Clarification From CA
EV Tested	/ CN=SSC GDL CA Root B,OU=CA ROOT Services,O=Skaitmeninio sertifikavimo centras,C=LT "0.4.0.2042.1.4", "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 }, "MHExCzAJBgNVBAYTAkxUMSswKQYDVQQKEyJTa2FpdG1lbmluaW8gc2VydGlmaWth" "dmltbyBjZW50cmFzMRkwFwYDVQQLExBdQSBST09UIFNIcnZpY2VzMRowGAYDVQQD" "ExFTU0MgR0RMIENBIFJvb3QgQg==", "PoxPvOQpg4JNhFWO1TWAzw==", Success!	Verified?	Verified
Root Stores Included In		Verified?	Need Clarification From CA
Mozilla Applied Constraints	None	Verified?	Verified

Digital Fingerprint Information

SHA-1 Fingerprint	C8:60:A3:18:FC:F5:B7:13:0B:10:07:AD:7F:61:4A:40:FF:FF:18:5F	Verified?	Verified
SHA-256 Fingerprint	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	Verified?	Verified

CA Hierarchy Information

CA Hierarchy	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.	Verified?	Verified
---------------------	--	-----------	----------

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).

Externally Operated SubCAs	None, and none planned.	Verified?	Verified
Cross Signing	None, and none planned.	Verified?	Verified
Technical Constraint on 3rd party Issuer	Are there, or can there be, 3rd party Registration Authorities who can cause the issuance of certificates? If yes, please describe how they are constrained.	Verified?	Need Clarification From CA

Verification Policies and Practices

Policy Documentation	Documents are provided in Lithuanian and English. Lithuanian: CP: https://gdl.repository.ssc.lt/lt/talpykla/dokumentai/sertifikato-taisykles-ssc-gdl-ca-v4.4.pdf CPS: https://gdl.repository.ssc.lt/lt/talpykla/dokumentai/sertifikavimo-veiklos-nuostatai-ssc-gdl-ca-v4.7.pdf	Verified?	Verified
CA Document Repository	https://gdl.repository.ssc.lt/en/repository/documents/	Verified?	Verified
CP Doc Language	English		
CP	https://gdl.repository.ssc.lt/en/repository/documents/certificate-policy-ssc-gdl-ca-v4.4.pdf	Verified?	Verified
CP Doc Language	English		
CPS	https://gdl.repository.ssc.lt/en/repository/documents/certificate-practice-statement-ssc-gdl-ca-v4.7.pdf	Verified?	Verified
Other Relevant Documents	RPA: https://gdl.repository.ssc.lt/en/repository/documents/ssc-gdl-ca-rpa-v2.pdf	Verified?	Verified
Auditor Name	TÜV Informationstechnik GmbH	Verified?	Verified
Auditor Website	https://www.tuvit.de/	Verified?	Verified
Auditor Qualifications	http://portal.etsi.org/TBSiteMap/ESI/TrustServiceProviders.aspx	Verified?	Verified
Standard Audit	https://gdl.repository.ssc.lt/en/audit/2015/	Verified?	Verified
Standard Audit Type	ETSI TS 102 042	Verified?	Verified
Standard Audit Statement Date	7/4/2014	Verified?	Verified
BR Audit	https://www.tuvit.de/data/content_data/tuevit_en/6729UE_s.pdf	Verified?	Verified
BR Audit Type	ETSI TS 102 042	Verified?	Verified
BR Audit Statement Date	7/4/2014	Verified?	Verified
EV Audit	https://www.tuvit.de/data/content_data/tuevit_en/6729UE_s.pdf	Verified?	Verified
EV Audit Type	ETSI TS 102 042	Verified?	Verified
EV Audit Statement Date	7/4/2014	Verified?	Verified
BR Commitment to Comply	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.	Verified?	Verified

SSL Verification Procedures	<p>NEED: The following information needs to be in the CP/CPS (publicly available documentation). See https://wiki.mozilla.org/CA:BaselineRequirements#CA_Conformance_to_the_BRs and https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Domain_Name_Ownership</p> <p>==</p> <p>According to section 6.1 of the internal RA document: "For verification of the requested domain name, the database of the registrar responsible for this domain name is checked. In case that the applicant is not the holder of the requested domain name, an authorization letter from the domain holder is needed, to prove the applicants right to use that domain name. The information obtained is checked against the data on the CSR provided with the order. The two names must match".</p> <p>For new orders we always send out an authorization email to one of predefined email addresses indicated in section 11.1.1 p. 4. of "CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates".</p> <p>==</p>	Verified?	Need Clarification From CA
EV SSL Verification Procedures	<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*30, physical*31 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*32.</p> <p>30 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>31 The RA checks the official postal address of the applicant along with Applicant's main business phone number.</p> <p>32 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> <p>AlsoSSC has implemented a document as amendment to the RA policy which describes in detail how the verification of EV certificate requests has to be performed by the RA officer.</p>	Verified?	Verified
Organization Verification Procedures	<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>	Verified?	Verified
Email Address Verification Procedures	<p>The CP/CPS needs to describe the procedures for verifying that the email address to be included in the certificate is owned/controlled by the certificate subscriber.</p> <p>https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Email_Address_Control</p>	Verified?	Need Clarification From CA
Code Signing Subscriber Verification Pro	<p>I could not find specific information about the verification procedures for code signing certificate subscribers. See https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Identity_of_Code_Signing_Certificate_Subscriber</p>	Verified?	Need Clarification From CA
Multi-Factor Authentication	<p>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</p> <p>QUESTION: What about non-EV cert issuance? See BR #16.5</p>	Verified?	Need Clarification From CA
Network Security	<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>	Verified?	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	https://gdl.repository.ssc.lt/en/repository/authority-certificates-and-crls/	Verified?	Verified
-------------------------------------	---	-----------	----------

Root Case Record # 3

Root Case Information

Root Case No	R00000050	Case Number	00000039
Request Status	Need Information from CA	Root Certificate Name	SSC GDL CA VS Root

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	https://gdl.repository.ssc.lt/certs/rootvs.crt	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: https://gdl.repository.ssc.lt/certs/test-v-vsclass2-4qca.cer	Verified?	Verified
CRL URL(s)	https://gdl.repository.ssc.lt/crls/vsclass2-4qca.crl NextUpdate for CRLs of end-entity certs: 7 days; CRL updates: please see section 4.9.7 of CPS	Verified?	Verified
OCSP URL(s)	http://vsclass2-4qca.ocsp.gdl.ssc.lt/ Maximum expiration time of OCSP responses: 5 min.	Verified?	Verified
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		Verified?	Need Clarification From CA
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

CA Hierarchy	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
Externally Operated SubCAs	None, and none planned.	Verified?	Verified
Cross Signing	None, and none planned.	Verified?	Verified
Technical Constraint on 3rd party Issuer	Are there 3rd party Registration Authorities who can cause the issuance of certificates? If yes, please describe how they are constrained.	Verified?	Need Clarification From CA

Verification Policies and Practices

Policy Documentation	Documents are provided in Lithuanian and English. Lithuanian: CP: https://gdl.repository.ssc.lt/lt/talpykla/dokumentai/sertifikato-taisykles-ssc-gdl-ca-v4.4.pdf CPS: https://gdl.repository.ssc.lt/lt/talpykla/dokumentai/sertifikavimo-veiklos-nuostatai-ssc-gdl-ca-v4.7.pdf	Verified?	Verified
CA Document Repository	https://gdl.repository.ssc.lt/en/repository/documents/	Verified?	Verified
CP Doc Language	English		
CP	https://gdl.repository.ssc.lt/en/repository/documents/certificate-policy-ssc-gdl-ca-v4.4.pdf	Verified?	Verified
CP Doc Language	English		
CPS	https://gdl.repository.ssc.lt/en/repository/documents/certificate-practice-statement-ssc-gdl-ca-v4.7.pdf	Verified?	Verified
Other Relevant Documents	RPA: https://gdl.repository.ssc.lt/en/repository/documents/ssc-gdl-ca-rpa-v2.pdf	Verified?	Verified
Auditor Name	TÜV Informationstechnik GmbH	Verified?	Verified
Auditor Website	https://www.tuvt.de/	Verified?	Verified
Auditor Qualifications	http://portal.etsi.org/TBSiteMap/ESI/TrustServiceProviders.aspx	Verified?	Verified
Standard Audit	https://gdl.repository.ssc.lt/en/audit/2015/	Verified?	Verified
Standard Audit Type	ETSI TS 101 456	Verified?	Verified

Standard Audit Statement Date	7/4/2014	Verified?	Verified
BR Audit		Verified?	Not Applicable
BR Audit Type		Verified?	Not Applicable
BR Audit Statement Date		Verified?	Not Applicable
EV Audit		Verified?	Not Applicable
EV Audit Type		Verified?	Not Applicable
EV Audit Statement Date		Verified?	Not Applicable
BR Commitment to Comply		Verified?	Not Applicable
SSL Verification Procedures	Not requesting Websites trust bit for this root.	Verified?	Not Applicable
EV SSL Verification Procedures		Verified?	Not Applicable
Organization Verification Procedures	<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>	Verified?	Verified
Email Address Verification Procedures	<p>The CP/CPS needs to describe the procedures for verifying that the email address to be included in the certificate is owned/controlled by the certificate subscriber.</p> <p>https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Email_Address_Control</p>	Verified?	Need Clarification From CA
Code Signing Subscriber Verification Pro	Not requesting Code Signing trust bit for this root.	Verified?	Not Applicable
Multi-Factor Authentication	<p>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</p> <p>QUESTION: What about non-EV cert issuance?</p> <p>See BR #16.5</p>	Verified?	Need Clarification From CA
Network Security	<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>	Verified?	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	https://gdl.repository.ssc.lt/en/repository/authority-certificates-and-crls/	Verified?	Verified
--	---	------------------	----------