Bugzilla ID: 379152
Bugzilla Summary: Add Lithuanian National Root Certificates

CAs wishing to have their certificates included in Mozilla products must comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/) and must supply the information necessary to determine whether or not the policy's requirements have been satisfied.

General Information	**Data**
CA Name	UAB "Skaitmeninio sertifkavimo centras" (SSC)
Website URL (English version)	www.ssc.lt
Organizational type. (E.g., whether the CA is operated by a private or public corporation, government agency, academic institution or consortium, NGO, etc.)	national government CA private corporation
Primary market / customer base. (Which types of customers does the CA serve? Are there particular vertical market segments in which it operates? Does it focus its activities on a particular country or other geographic region?)	SSC, Skaitmeninio Sertifkavimo Centras, is the Lithuanian Government accredited commercial CA issuing certificates to Government institutions, public services, businesses and citizens. Primary geographical area(s) served: Lithuania, European Union

For Each Root CA whose certificate is to be included in Mozilla (or whose metadata is to be modified)

Info Needed	**Data** – Root A	**Data –** Root B	**Data** – Root C
Certificate Name	SSC Root CA A	SSC Root CA B	SSC Root CA C
Cert summary / comments	This root has four internally operated subordinate CAs: Class 1, Class 2, Qualified Class 3, and Qualified Class 3 VS.	This root is a special purpose CA that has no subordinate CAs. Root B is used for single-root certificates (SSL, Code Signing, OCSP, time stamping).	This root serves as a backup CA for Roots A and B. Just in case either of those two roots become unusable and become revoked. According to the government project that SSC is involved in, Root C will have to be tested in a specific project where they must demonstrate availability of its CRL and OCSP services. The project will accept Root C only if it is a Firefox built-in object. If Root A does get revoked and Root C gets put into service, then Root C will have four internally operated

			subordinate CAs: Class 1, Class 2, Qualified Class 3, and Qualified Class 3 VS.
root CA certificate URL	http://www.ssc.lt/cacert/ssc_root_a.crt	http://www.ssc.lt/cacert/ssc_root_b.crt	http://www.ssc.lt/cacert/ssc_root_c.crt
SHA-1 fingerprint	5a:5a:4d:af:78:61:26:7c:4b:1f:1e:67:58:6b:ae:6e:d4:fe:b9:3f	3e:84:d3:bc:c5:44:c0:f6:fa:19:43:5c:85:1f:3f:2f:cb:a8:e8:14	23:e8:33:23:3e:7d:0c:c9:2b:7c:42:79:ac:19:c2:f4:74:d6:04:ca
Valid from	12/27/2006	12/27/2006	12/27/2006
Valid to	12/28/2026	12/25/2026	12/22/2026
Cert Version	3	3	3
Modulus length	4096	4096	4096
CRL URL	http://crl.ssc.lt/root-a/cacrl.crl	http://crl.ssc.lt/root-b/cacrl.crl	http://crl.ssc.lt/root-c/cacrl.crl
CRL update frequency for end-entity certificates	CPS section 4.4.4: SSC QCA publishes its CRLs weekly. The CRL is also updated each time when a certificate issued by this CA is revocated.		
OCSP Responder URL	http://ocsp.ssc.lt:2560 http://www.ssc.lt/ocsp/		
CA Hierarchy Diagram	CA Hierarchy Diagram is on page 17 of the CPS.		
List or description of subordinate CAs operated by the CA organization associated with the root CA	From page 17 of the CPS: SSC Root CA A -> SSC Class 1 CA II -> SSC Class 2 CA II -> SSC Qualified Class 3 CA -> SSC Qualified Class 3 VS CA CPS section 1.4.7: Class 1 – Subject's identity has not been verified. Certificate can be used for email encryption only; in non-commercial transactions.	No subordinate CAs shown in diagram on page 17 of the CPS. SSC Root CA B is a special purpose CA that has no subordinate CAs. This root is used for single-root certificates: SSL, Code Signing, OCSP, time stamping	From page 17 of the CPS: SSC Root CA C -> SSC Class 1 CA II -> SSC Class 2 CA II -> SSC Qualified Class 3 CA -> SSC Qualified Class 3 VS CA These subordinate CAs are shown within dashed lines. The dashed lines indicate back-up CA functionality. Comment #23: Root C serves as a backup CA for Root A and B. Just in case any of these two roots

	Class 2 – Subject's identity has been verified. Can be used for all electronic transactions, except for signing electronic forms and documents. Can be used for SSL. Class 3 – Subject's identity has been verified and private key is stored in SSCD. This is the qualified certificate as defined by EU Directive and National el. Signature Law. Only Class 3 certificates are qualified electronic signatures.		become unusable and become revocated, then we switch to using C. According to the govenment project I mentioned in one of my messages above, Root C will have to be tested in a specific project where we should demonstrate availability of its CRL and OCSP services. Again, the project will accept Root C only if it is FireFox' built-in object.
For subordinate CAs operated by third parties, if any:	None	None	None
List any other root CAs that have issued cross-signing certificates for this root CA	None	None	None
Requested Trust Bits	Websites Email Code	Websites Email Code Comment #30: Although in practice this Root CA is mainly used for SSL, Code Signing, OCSP and time stamping purposes, the secure email has to be also enabled.	Websites Email Code
If SSL certificates are issued within the hierarchy rooted at this root CA certificate: • DV	SSL certs are IV/OV Identity verification is defined in CPS section 3.2. The verification procedure described relevant to the classes of certificates and not to the types of certificates (SSL, Code Signing etc.). The detailed [step by step] instructions relevant to the types of certificates are described in RA Operators Instructions Manual. Here is the translation of related identity verification requirements from the CPS (verified via Google Translate).		

• OV	Class 1 Certificates (used for email/encryption only): A person willing to order a certificate must fill in the Electronic Application Form. The identity verification is limited to email verification. (The order process is conducted by email). Class 2 Certificates (used for SSL, email, encryption): A person willing to order a certificate must fill in the Electronic Application Form. In order to verify applicant's identity SSC RA requests the applicant to present an ID that contain following information: Name, Surname Personal ID (applicable to citizens and residents of Lithuania) Date of Birth, validity date and document number of Residence Permit (Applicable to rezidents of Lithuania) Date of Birth, Passport or Travel document number, place and date of issue (Applicable to foreigners) Date of Birth, validity date, document number, place and date of issue of the Residence Permit (Applicable to foreigners rezidents of foerign countries) An authorization document as defined by the Civil Code, in case a person acting on behalf of another person. For legal entities SSC RA also verifies following information: The name of legal entity Legal status of the entity Location of legal entity Code of legal entity registration Document number and the date of issue of the Certificate of legal entity Registration Other Information from a third party or a public service Class 2 SSL certificates: SSC RA verifies that applicant is duly established, checks its legal status and applicant's authorization to order the SSL certificate on behalf of legal entity. Additionally SCC RA checks that the applicant has proper ownership or authorisation to use the Subject's domain name. Google Translate: "For all server certificates: SSC qca satisfied that the person requesting the certificate is set up, would be service station registered the Internet domain name of the owner or otherwise you will have the right to use the Internet domain." The Electronic Application Forms can be accessed here: https://repository.ssc.lt/?name=docs&act=list&group=5&L=lt&ssc_m=6,15 Class 3 Certificates (used as qualified electronic signatures): Identity is verified according to EU Directive and National el. Signature Law. Details are on pages 33 and 34 of the CPS.

Example certificate(s) issued within the hierarchy rooted at this root, including the full certificate chain(s) where applicable.	Sample url: https://www.dokumentai.lt/data/ Sample cert: https://www.ssc.lt/certs/noname_cert_a.pem	Sample cert: https://www.ssc.lt/certs/noname_cert_b.pem	Sample cert: https://www.ssc.lt/certs/noname_cert_c.pem
CP/CPS	(in Lithuanian language) PKI Disclosure Statement: http://repository.ssc.lt/files/viesa-info/pki_disclosure_v1-0-0%5BLT%5D.pdf Certificate Practices: http://repository.ssc.lt/files/cp/ssc_trusted_root_cp_v1-0-0%5BLT%5D.pdf Certificate Practices Statement: http://repository.ssc.lt/files/cps/ssc_trusted_root_cps_v1-0-0%5BLT%5D.pdf As defined in CPS 1.1., provisions set by the CPS are mandatory for the CA infrastructure as a whole. In certain cases service-specific CPSs can be created however they can't contradict to this CPS.		
AUDIT	Audit Type: ETSI TS 101 456 Auditor: Information Society Development Committee Under The Government Of The Republic Of Lithuania Auditor URL: http://www.ivpk.lt/main_en.php?cat=10&gr=4 http://epp.ivpk.lt/en/ Audit Document URL: http://www.ssc.lt/files/SSC%20CA%20Application%20to%20Trusted%20Root%20CA%20program.pdf (10/30/2008) According the Law on Electronic signatures, Information Sociate Development Committee of Lithuania is the official Government institution responsible for supervision of certification service providers. The Committee has developed official requirements to CAs issuing qualified certificates based on ETSI TS 101 456. Skaitmeninio sertifikavimo centras (SSC), has passed Government audit procedures. The status of the company as the qualiified CA can		

	also be checked through the Committee's web site: http://epp.ivpk.lt/en/providers/ Verifying Authenticity of Audit report: From main auditor website: http://www.ivpk.lt/main_en.php?cat=20&gr=2 Deputy Director Edmundas Žvirblis e.zvirblis@ivpk.lt **Email received from the auditor, IVPK:** Dear Kathleen Wilson, The document posted at http://www.ssc.lt/files/SSC%20CA%20Application%20to%20MS%20Trusted%20Root%20CA%20program.jpg was issued by the Information Society Development Committee under the Government of the Republic of Lithuania acting as Electronic Signature Supervision authority of Republic of Lithuania. You can find all Qualified certificate service providers registered in Lithuania at http://epp.ivpk.lt/en/providers/. Best regards, Vaidotas Ramonas Information Society Development Committee under the Government of the Republic of Lithuania Electronic Signature Supervision Division Chief Specialist. IT Security Officer E-mail.: v.ramonas@ivpk.lt

Review CPS sections dealing with subscriber verification (COMPLETE)
(section 7 of http://www.mozilla.org/projects/security/certs/policy/)

- Verify domain check for SSL
    - Google Translate from page 33 of CPS: "For all server certificates: SSC qca satisfied that the person requesting the certificate is set up, would be service station registered the Internet domain name of the owner or otherwise you will have the right to use the Internet domain."
    - Comments from SSC:
        - In CPS section 3.2 in regards to Class 2 SSL certificates: SSC RA verifies that applicant is duly established, checks its legal status and applicant's authorization to order the SSL certificate on behalf of legal entity. Additionally SCC RA checks that the applicant has proper ownership or authorisation to use the Subject's domain name.
        - The detailed [step by step] instructions relevant to the types of certificates are described in RA Operators Instructions Manual.

        - We additionally check the ownership of the domain name according to DNS (whois).
        - As we have explained earlier the identity verification is the same for all roots whether we deal with a physical entity or legal entity. This means that the same identity verification applies no matter which Root CA is involved. Appropriate verification procedures presented in Chapter 3 of the CPS (Page 29) more detailed procedures have been described in instructions manuals for the operating personnel.
- Verify the email account associated with the email address in the cert is owned by the subscriber. In addition to verification of subscriber's legal identity.
    - Comment #23: …the procedure of email address verification is still the same as for all other types of certificates. Applicant fills in the form on our web site, where he/she indicates the email address, selects the type of certificate and chooses a password. After that we offer the applicant to check his/her mailbox and click on the URL provided in the message. When he/she accesses his/her mailbox and clicks on the URL we prompt for the previously declared password. It's important to note, that for Class 2 and 3 certificates (Identity verified), we accept non-public domain name hosted email addresses only. And in case of legal entity we additionally check the ownership of the domain name according to DNS (whois). In latter case we might request the applicant to provide us with a proof of ownership other than whois (contract, order form, invoice etc.).
- Verify identity info in code signing certs is that of subscriber
    - Identity is verified for class 2 and class 3, as per CPS section 3.2. For class 3, identity is verified as per Identity is verified according to EU Directive and National el. Signature Law. Details are on pages 33 and 34 of the CPS.
- Make sure it's clear which checks are done for which context (cert usage)

Flag Problematic Practices (COMPLETE)
(http://wiki.mozilla.org/CA:Problematic_Practices)

- Long-lived DV certificates
    - SSL certs are IV/OV, not DV.
- Wildcard DV SSL certificates
    - SSL certs are IV/OV, not DV.
- Delegation of Domain / Email validation to third parties
    - No
- Issuing end entity certificates directly from roots
    - SSC Root CA A and C do not issue end entity certificates directly from roots.
    - **SSC Root B issues end-entity certificates directly.**
        - **Comment #30: Although still under consideration, but we are planning to issue single root SSL certs for various services.**
- Allowing external entities to operate unconstrained subordinate CAs
    - No sub-CAs operated by third parties.
- Distributing generated private keys in PKCS#12 files

    - No
- Certificates referencing hostnames or private IP addresses
    - No
- OCSP Responses signed by a certificate under a different root
    - Comment #30: Based on the actual usage, we have a single OCSP server running for all CAs. However as the number of eservices exploring PKI technologies reaches a certain level, each CA or group of CAs will have a separate OCSP server.
- CRL with critical CIDP Extension
    - CRLs downloaded into Firefox without error.

Verify Audits (COMPLETE)

- Validate contact info in report, call to verify that they did indeed issue this report.
    - COMPLETE – verified by internet and email exchange with the auditor.
- For EV CA's, verify current WebTrust EV Audit done.
    - N/A
- Review Audit to flag any issues noted in the report
    - None noted