

Mozilla - CA Program

Case Information			
Case Number	00000071	Case Record Type	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	Internet Security Research Group (ISRG)	Request Status	Ready for Public Discussion

Additional Case Information	
Subject	Include ISRG root certificate
Case Reason	

Bugzilla Information	
Link to Bugzilla Bug	https://bugzilla.mozilla.org/show_bug.cgi?id=1204656

General information about CA's associated organization			
CA Email Alias 1			
CA Email Alias 2			
Company Website	https://letsencrypt.org/	Verified?	Verified
Organizational Type	Non-Profit Organization	Verified?	Verified
Organizational Type (Others)		Verified?	Not Applicable
Geographic Focus	Global	Verified?	Verified
Primary Market / Customer Base	Offers server authentication certificates to the general public around the world.	Verified?	Verified
Impact to Mozilla Users	New CA.	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	<ul style="list-style-type: none"> - Publicly Available CP and CPS: Yes - CA Hierarchy: Yes - Audit Criteria: Yes - Document Handling of IDNs in CP/CPS: We do not currently issued for IDN, when we do we'll state how we handle homographic spoofing in our CPS. - Revocation of Compromised Certificates: Yes, CP section 4.9.1.2 - Verifying Domain Name Ownership: Yes, CP section 3.2.2 - Verifying Email Address Control: Not applicable, not requesting Email trust bit. - Verifying Identity of Code Signing Certificate Subscriber: Not applicable, not request Code signing trust bit. - DNS names go in SAN: Yes, CP section 3.1.1 	Verified?	Verified

- Domain owned by a Natural Person: We only issued DV certificates which do not include O or OU fields.
- OCSP: Yes
- Network Security Controls: We comply with recommendations.

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	
CA's Response to Problematic Practices	<ul style="list-style-type: none"> - Long-lived DV certificates: No. CP section 6.3.2 - DV-SSL certs valid up to 39 months. - Wildcard DV SSL certificates: No. CP section 3.1.1 - Wildcard names are not permitted. - Email Address Prefixes for DV Certs: CP section 3.2.2.2 - "admin," "administrator," "webmaster," "hostmaster," or "postmaster" - Delegation of Domain validation to third parties: Yes. CP section 8.1 - In any event, the CA, RAs, CSAs, and CMAs must certify annually that they have at all times during the period in question complied with the requirements of this Policy. - Issuing end entity certificates directly from roots: No - Allowing external entities to operate subordinate CAs: Yes, CP section 8.1 - Distributing generated private keys in PKCS#12 files: No - Certificates referencing hostnames or private IP addresses: CP section 3.2.2.5: The CA will not issue certificates for IP Addresses. - Issuing SSL Certificates for Internal Domains: CP section 3.2.2.3 - OCSP Responses signed by a certificate under a different root: No - SHA-1 Certificates: We have not and never will issue SHA-1 certificates. - Generic names for CAs: We use "Internet Security Research Group" and "Let's Encrypt". - Lack of Communication With End Users: We offer various email addresses for contact, and operate a support forum - Backdating the notBefore date: Compliant with recommendation/requirement 	<p>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.</p>	<p>Verified? Verified</p>

Root Case Record # 1

Root Case Information

Root Certificate Name	ISRG Root X1	Root Case No	R00000099
Request Status	Ready for Public Discussion	Case Number	00000071

Additional Root Case Information

Subject Include ISRG Root X1

Technical Information about Root Certificate

O From Issuer Field	Internet Security Research Group	Verified?	Verified
OU From Issuer Field		Verified?	Verified

Certificate Summary	ISRG Root X1 will be used to issue server authentication certificates. Initially there will be two intermediates, "Let's Encrypt Authority X1" and "Let's Encrypt Authority X2".	Verified?	Verified
Root Certificate Download URL	https://letsencrypt.org/certs/isrgrootx1.der	Verified?	Verified
Valid From	2015 Jun 04	Verified?	Verified
Valid To	2035 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://helloworld.letsencrypt.org/	Verified?	Verified
CRL URL(s)	CRL HTTP URL: http://crl.root-x1.letsencrypt.org/ CRL issuing frequency for subordinate end-entity certificates: We will not issue CRLs for end-entity certificates. CRL issuing frequency for subordinate CA certificates: At least once every six months.	Verified?	Verified
OCSP URL(s)	http://ocsp.root-x1.letsencrypt.org/ CP section 4.10.2: OCSP responses from this service must have a maximum expiration time of 10 days.	Verified?	Verified
Revocation Tested	https://certificate.revocationcheck.com/helloworld.letsencrypt.org no errors	Verified?	Verified
Trust Bits	Websites	Verified?	Verified
SSL Validation Type	DV	Verified?	Verified
EV Policy OID(s)	Not EV	Verified?	Not Applicable
EV Tested	Not requesting EV treatment	Verified?	Not Applicable
Root Stores Included In		Verified?	Verified
Mozilla Applied Constraints	None	Verified?	Verified

Digital Fingerprint Information

SHA-1 Fingerprint	CA:BD:2A:79:A1:07:6A:31:F2:1D:25:36:35:CB:03:9D:43:29:A5:E8	Verified?	Verified
SHA-256 Fingerprint	96:BC:EC:06:26:49:76:F3:74:60:77:9A:CF:28:C5:A7:CF:E8:A3:C0:AA:E1:1A:8F:FC:EE:05:C0:BD:DF:08:C6	Verified?	Verified

CA Hierarchy Information

CA Hierarchy	CA Hierarchy Diagram: https://bugzilla.mozilla.org/attachment.cgi?id=8660928	Verified?	Verified
Externally Operated SubCAs	There may be externally-operated subCAs in the future, but the CP/CPS requires that they be audited annually according to the	Verified?	Verified

CA/Browser Forum Baseline Requirements.

CP section 1.3: CAs (CAs who have cross-certified or are otherwise authorized to issue Certificates by the PMA)... The CA issues Certificates to Applicants, who may be individuals or organizations.

CP section 1.3.6.1: the CA may subcontract manufacturing and administrative functions to third party Certificate Manufacturing Authorities (CMAs) who agree to be bound by this Policy.

CP section 1.4.3: If the CA is cross-certifying with another external party, it cannot issue that entity a Subordinate Certificate unless it is compliant with the CA/B Forum Baseline Requirements

CP section 8.1: In any event, the CA, RAs, CSAs, and CMAs must certify annually that they have at all times during the period in question complied with the requirements of this Policy.

Cross Signing	Cross-signing with "DST Root CA X3" root that is owned by IdenTrust and included in NSS.	Verified?	Verified
Technical Constraint on 3rd party Issuer	External third parties who can directly cause the issuance of certificates in this hierarchy: subordinate CAs, Registration Authorities (RAs), Certificate Manufacturing Authorities (CMAs), and cross-certified CAs. No technical constraints. All subCAs will be publicly-disclosed and audited according to the CA/Browser Forum Baseline Requirements. CP section 1.3.3: the CA may subcontract registration and Identification and Authentication (I&A) functions to an organization that agrees to fulfill the functions of an RA in accordance with the terms of this Policy... Audit requirements are in section 8 of the CP.	Verified?	Verified

Verification Policies and Practices

Policy Documentation	Documents are in English.	Verified?	Verified
CA Document Repository	https://letsencrypt.org/repository/	Verified?	Verified
CP Doc Language	English		
CP	https://letsencrypt.org/documents/ISRG-CP-September-9-2015.pdf	Verified?	Verified
CP Doc Language	English		
CPS	https://letsencrypt.org/documents/ISRG-CPS-September-22-2015.pdf	Verified?	Verified

Other Relevant Documents	Subscriber Agreement: https://letsencrypt.org/documents/LE-SA-v1.0.1-July-27-2015.pdf	Verified?	Verified
Auditor Name	BrightLine	Verified?	Verified
Auditor Website	https://www.brightline.com/	Verified?	Verified
Auditor Qualifications	http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx	Verified?	Verified
Standard Audit	https://letsencrypt.org/documents/LE_WebTrustforCA.pdf	Verified?	Verified
Standard Audit Type	WebTrust	Verified?	Verified
Standard Audit Statement Date	9/9/2015	Verified?	Verified
BR Audit	https://letsencrypt.org/documents/LE_WebTrustforBR.pdf https://wiki.mozilla.org/CA:BaselineRequirements	Verified?	Verified
BR Audit Type	WebTrust	Verified?	Verified
BR Audit Statement Date	9/9/2015	Verified?	Verified
EV Audit	Not requesting EV treatment	Verified?	Not Applicable
EV Audit Type		Verified?	Not Applicable
EV Audit Statement Date		Verified?	Not Applicable
BR Commitment to Comply	CP and CPS section 1.1	Verified?	Verified
SSL Verification Procedures	<p>CP section 3.2.2: The issuance of a DV-SSL or Administrative Certificate will be based on I&A performed by the CA or RA using procedures that shall be documented in the CPS.</p> <p>CP section 3.2.2.2: For each Name listed in a DV-SSL Certificate, the CA shall confirm that, as of the date the Certificate was issued, the Applicant (or the Applicant's Parent Company, Subsidiary Company, or Affiliate, collectively referred to as "Applicant" for the purposes of this Section) either is the Domain Name Registrant or has control over the FQDN by: ...</p> <p>Verification against the Denied List: CP section 3.2.4.1, CPS section 3.2.4.2</p> <p>Verification against High Risk Certificate Requests: CP section 3.2.4.2, CPS section 3.2.4.3.</p> <p>CPS: ACME Automated Certificate Management Environment</p> <p>CPS section 3.2.4.1: A DV-SSL Certificate request identifying an electronic device as the subject of a Certificate can only be made by the machine that has previously been verified by the ACME client as being used by the Applicant requesting the DV-SSL Certificate. To verify the authenticity of a DV-SSL Certificate request for a FQDN, the Applicant responds to requests from the ACME</p>	Verified?	Verified

client from servers to verify requested changed to their domain as described in Section 3.2.2.2.

EV SSL Verification Procedures	Note requesting EV treatment	Verified?	Not Applicable
Organization Verification Procedures	<p>CP section 3.2.4: Validation of Authority For DV-SSL Certificates, demonstration of control over the device and domain may be conducted electronically and if used shall consist of validation of the information presented as described above. If the Applicant cannot demonstrate control, validation of authority will be verified through a check to an alternative source as listed in Section 3.2.2.</p> <p>For Administrative Certificates issued to individuals, the information submitted by the Applicant shall consist of at least the following items:</p> <ol style="list-style-type: none"> 1. Full name; and 2. Validation from the Human Resources department of the CA that confirms affiliation to the CA. <p>CP section 4.2.1: For Administrative Certificates issued to individuals, the CA shall provide a secure means of validating the identity of the Applicant; such means shall include satisfactory proof of identity from the Human Resources Department of the CA and proof of organizational affiliation with the CA.</p>	Verified?	Verified
Email Address Verification Procedures	Not requesting the Email trust bit.	Verified?	Not Applicable
Code Signing Subscriber Verification Pro	Not requesting the Code Signing trust bit.	Verified?	Not Applicable
Multi-Factor Authentication	CPS section 5 Two-factor auth is being used, Client Certificates and/or Hardware Tokens.	Verified?	Verified
Network Security	CPS section 6.7 We are in compliance with CA/B Forum Network and Certificate System Security.	Verified?	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	http://cert.int-x1.letsencrypt.org/	Verified?	Verified
--	---	-----------	----------