

Bugzilla ID: 792377

Bugzilla Summary: Add CA Disig root certificates

CAs wishing to have their certificates included in Mozilla products must

- 1) Comply with the requirements of the Mozilla CA certificate policy (<http://www.mozilla.org/projects/security/certs/policy/>)
- 2) Supply all of the information listed in http://wiki.mozilla.org/CA:Information_checklist.
 - a. Review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices
 - b. Review the Potentially Problematic Practices at https://wiki.mozilla.org/CA:Problematic_Practices

General information about the CA's associated organization

| | |
|--------------------------------|--|
| CA Company Name | Disig |
| Website URL | http://www.disig.eu http://www.disig.sk |
| Organizational type | Private Corporation |
| Primark Market / Customer Base | Disig is a public Certification Service Provider, located in Slovakia. Disig focus its certification service mainly for Slovakian market for the customer from general public, private companies, governmental organization. |
| CA Contact Information | CA Email Alias: caoperator@disig.sk CA Phone Number:+421 2 20850140 Title / Department: Senior consultant at Information Security department |

Technical information about each root certificate

| Cert Name | CA Disig Root R1 | CA Disig Root R2 |
|--------------------------|---|--|
| Certificate Issuer Field | CN = CA Disig Root R1 O = Disig a.s. L = Bratislava C = SK | CN = CA Disig Root R2 O = Disig a.s. L = Bratislava C = SK |
| Certificate Summary | Will eventually replace the current CA Disig root certificate included in Mozilla products (Bugzilla #455878). This root will sign internally-operated intermediate certificates that will sign entity certificates for SSL, digital signature, sending/receiving e-mail, and code signing. | Root certificate for SHA2 CA chain hierarchy This root will sign internally-operated intermediate certificates that will sign entity certificates for SSL, digital signature, sending/receiving e-mail, and code signing. |
| Root Cert URL | http://www.disig.sk/rootcar1/cert/rootcar1.der | http://www.disig.sk/rootcar2/cert/rootcar2.der |
| SHA1 | 8E:1C:74:F8:A6:20:B9:E5:8A:F4:61:FA:EC:2B:47:56:51:1A:52:C6 | B5:61:EB:EA:A4:DE:E4:25:4B:69:1A:98:A5:57:47:C2:34:C7:D9:71 |
| Valid From | 2012-07-19 | 2012-07-19 |
| Valid To | 2042-07-19 | 2042-07-19 |
| Certificate Version | 3 | 3 |
| Signature Algorithm | SHA-1 | SHA-256 |
| Modulus | 4096 | 4096 |
| Test Website | https://testssl-valid-r1i1.disig.sk | https://testssl-valid-r2i1.disig.sk |

| | | |
|----------------------|--|--|
| CRL URL | http://www.disig.sk/rootcar1/crl/rootcar1.crl http://www.disig.sk/subcar1i1/crl/subcar1i1.crl (NextUpdate: 24 hours) | http://www.disig.sk/rootcar2/crl/rootcar2.crl http://www.disig.sk/subcar2i1/crl/subcar2i1.crl (NextUpdate: 24 hours) |
| CRL Frequency | CP section 4.4.3: immediate upon revocation, otherwise every 24 hours | |
| OCSP URL | http://rootcar1-ocsp.disig.sk/ocsp/rootcar1 http://subcar1i1-ocsp.disig.sk/ocsp/subcar1i1 No expiration time set. OCSP responder is on-line updated - max delay is 15 seconds from revocation. | http://rootcar2-ocsp.disig.sk/ocsp/rootcar2 http://subcar2i1-ocsp.disig.sk/ocsp/subcar2i1 No expiration time set. OCSP responder is on-line updated - max delay is 15 seconds from revocation. |
| Requested Trust Bits | Websites (SSL/TLS) Email (S/MIME) Code Signing | Websites (SSL/TLS) Email (S/MIME) Code Signing |
| SSL Validation Type | OV | OV |
| EV Policy OID(s) | Not Applicable. Not requesting EV treatment for this root. | |

CA Hierarchy information for each root certificate

| | | |
|----------------------------|---|---|
| CA Hierarchy | CA Disig Root R1 – CA Disig R011 (SSL certificates) – CA Disig R012 (e-mail certificates, digital signature certificates, code signing) | CA Disig Root R2 – CA Disig R011 (SSL certificates) – CA Disig R012 (e-mail certificates, digital signature certificates, code signing) |
| Externally Operated SubCAs | None, and none planned. | None, and none planned. |
| Cross-Signing | None, and none planned. | None, and none planned. |

Verification Policies and Practices

| | |
|--------------------------------------|--|
| Policy Documentation | CP (Slovak): http://www.disig.sk/_pdf/cp-disig.pdf CP (English): http://www.disig.eu/_pdf/cp-cadisig-eng.pdf CPS (Slovak): http://www.disig.sk/_pdf/cps_ra_cadisig.pdf CPS (English): http://www.disig.eu/_pdf/cps_ra_cadisig_eng.pdf |
| Audits | Audit Type: ETSI 102042 Auditor: Ing. Juraj Zelenay (juraj.zelenay@mpicons.sk) , Ing. Rastislav Machel (rastislav.machel@machel-cs.eu) Auditor Qualifications: http://www.isaca.sk/priprava-na-certifikaty/zoznam-drzitelov-certifikatov/ Audit Report and Management's Assertions: http://www.disig.sk/_pdf/Audit_Statement_2011_CA_Disig.pdf (2011.11.28) Email exchanged with Mr. Zelenay to confirm authenticity of audit statement. |
| Baseline Requirements (SSL) | CP section 1.3.3: CA Disig conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org . In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document. |
| Organization Verification Procedures | CP section 3.1.7: Authentication of organization identity CP section 3.1.8: Authentication of individual identity CPS section 3.1.7: Authentication of legal identity (organization) CPS section 3.1.8: Authentication of individual identity CPS section 3.1.9: Authentication of the component identity |

| | |
|------------------------------------|---|
| <p>SSL Verification Procedures</p> | <p>CP section 3.1.9: Authentication of the component identity CMA (Certificate Management Authority) has to guarantee that the certificate issued for hardware or software component (code signing) that is able to use the certificate, that the component identity and the public key are bonded together. For this reason the component has to be assigned to a specific person or to a person that is authorized to deal on behalf of a company that is administrating the component. (see section 5.2). Person is obliged to provide following information to CMA, as described in sections 3.1.10 and 5.2:</p> <ul style="list-style-type: none"> - identification of component (name for software component), - public key of the component (part of certificate request), - authorization of component and its characteristics (URL and application description for software component), - contact information, that CMA may, if necessary, to communicate with this person, <p>CMA will be verify the accuracy of any authorization (values of distinguishing name) to be listed in the certificate and verify the data submitted. Methods to implement this authentication and control data include:</p> <ul style="list-style-type: none"> - verify the identity of the person in accordance with the requirements of section 3.1.8, - verify the identity of the organization, which includes the component, in accordance with the requirements of section 3.1.7, - verify the competency of using data to be introduced in individual items of the certificate, with an emphasis on CommonName. (Note: The typical value of this item will be fully registered domain name.) <p>In the case of using the domain name is the condition that the second level domain is owned by an entity which is an applicant for a certificate for the server. Subject has to demonstrate to RA operator that it is the holder of the domain for which calls for issuance of the certificate. The existence of a domain and its owner has been verified through WHOIS services provided by the web top level domain sponsoring organization(e.g. for domain ".sk" is the sponsoring organization SK-NIC - www.sk-nic.sk; for domain ".eu" is the sponsoring organization EURid vzw/asbl established in Belgium for the domain ".com" is sponsoring organization VeriSign Global Registry Services based in the U.S.). Full domain name will be verified by sending an e-mail which will contain secret information to some unforeseeable e-mail accounts for the domain listed in the record obtained from the WHOIS service respectively on the e-mail from that domain for these possible accounts: admin, administrator, webmaster, hostmaster or postmaster. An applicant for a certificate for the domain shall send back verification information as proof of ownership of the domain within specified period of time. If from the data obtained from the above sources is not possible to reliably determine that the applicant is the owner of the domain or person acting on behalf of the owner of the domain, CA Disig refuses to issue a certificate to that request. Registration Authority verifies a written confirmation from independent sources on the Internet such as www.sk-nic.sk for SK domain respectively www.eurid.eu for EU domain, etc. In the case of registered IP addresses RA will not investigate whether the body - the applicant for a certificate for the server uses the registered IP address legitimately e.g. whether the registered IP address is the address segment, which is registered in the RIPE organization for the entity - the applicant for a certificate for the server. In this case, is automatically assumed that that subject - the applicant for a certificate for the server use in the application for the certificate registered IP address and applicant gave to CA Disig a solemn declaration that the IP address used lawfully and that he is aware of all the consequences and responsibility for any unauthorized use of the IP address. The CA Disig implements a process that prevents an OU attribute from including a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless the CA Disig has verified this information.</p> |
|------------------------------------|---|

| | |
|---|---|
| | <p>CPS section 3.1.9: Authentication of the component identity The existence of a domain and its owner has been verified through WHOIS services provided by the web top level domain sponsoring organization (e.g. for domain ".sk" is the sponsoring organization SK-NIC - www.sk-nic.sk; for domain ".eu" is the sponsoring organization EURid vzw/asbl established in Belgium for the domain ".com" is sponsoring organization VeriSign Global Registry Services based in the U.S.). Full domain name will be verified by sending an e-mail which will contain secret information to some unforeseeable e-mail accounts for the domain listed in the record obtained from the WHOIS service respectively on the e-mail from that domain for these possible accounts: admin, administrator, webmaster, hostmaster or postmaster.</p> <p>CPS section 4.1.2.2: RA procedure before issuing a SSL certificate</p> |
| Email Address Verification Procedures | <p>CP section 4.1.2: 9. In connection with the verification of an e-mail address in the request for certificate which is used to sign electronic messages (extension "Secure Email (1.3.6.1.5.5.7.3.4)") perform RA worker verification checks of e-mail addresses in the certificate request, via the responds to the e-mail, from which request was send. Verification is carried out so that to the e-mail address is sending a mail message containing secret unpredictable information (authentication information). An applicant for a certificate shall send back to the CA Disig verification information as evidence of control of the e-mail addresses. In case that the verification of e-mail address runs unsuccessfully, CA Disig refuses to issue the certificate. If the certificate request for issuing subsequent certificate is sent via e-mail and that e-mail is signed with the valid electronic signature and certificate was issued by CA Disig and e-mail in the request is identical with the sender e-mail, verifying od e-mail address is not required.</p> <p>CPS section 4.1.1.3: 2. In the case when certificate request sent in advance contains the same e- mail address as from which it was sent, the RA staff shall verify validity of this e-mail address. . Verification is carried out so that to the e-mail address is sending a mail message containing secret unpredictable information (authentication information). An applicant for a certificate shall send back to the CA Disig verification information as evidence of control of the e-mail addresses. The answer shall be send within a specified period of time sufficient for sending email. In case that the verification of e-mail address runs unsuccessfully, CA Disig refuses to issue the certificate. Detailed procedure is described in the RA working manuals and is also subject to the initial training of RA staff.</p> |
| Code Signing Subscriber Verification Procedures | <p>CP section 3.1.9: Authentication of the component identity CPS section 3.1.9: Authentication of the component identity Hardware or software component that will use certificates will be subject to certification and CA Disig SSL certificate respectively code-signing certificate (not a personal certificate) can be created. For this reason the component has to be assigned to a specific person or to a person that is authorized to deal on behalf of a company that is administrating the component. (see section 3.1.8 and 5.2).</p> |
| Multi-factor Authentication | <p>Audit statement: verified multi-factor auth in place for all accounts capable of directly causing cert issuance. CP and CPS section 5: Physical, procedural, and personnel security controls CP and CPS section 6: Technical Security Controls</p> |
| Network Security | <p>CP and CPS section 6.4: CA Disig computer equipment is used exclusively for the purposes of conducting certification activities. Information security of CA Disig system is regularly control for compliance with the requirement of ISO 17799 and ISO 13335.</p> |

Response to Mozilla's CA Recommended Practices (https://wiki.mozilla.org/CA:Recommended_Practices)

| | |
|---|---|
| Publicly Available CP and CPS | Yes. See above. |
| CA Hierarchy | Yes. See above. |
| Audit Criteria | See above. |
| Document Handling of IDNs in CP/CPS | Not applicable. CA Disig does not issue IDNs certificates |
| Revocation of Compromised Certificates | Yes. CPS section 4.4.1, Circumstances of revocation |
| Verifying Domain Name Ownership | Yes. See above. |
| Verifying Email Address Control | Yes. See above. |
| Verifying Identity of Code Signing Certificate Subscriber | Yes. See above. |
| DNS names go in SAN | Yes. Comment #2: All DNS names go into the SAN including DNS name from CN field |
| Domain owned by a Natural Person | Comment #2: If there be such application CA Disig will require proposed information (O and OU fields) in the SSL certificate request. During the next revision of current CP and CPS this part will be add to procedures for SSL certificate issuing. |
| OCSP | Yes. Tested. |

Response to Mozilla's list of Potentially Problematic Practices (https://wiki.mozilla.org/CA:Problematic_Practices)

| | |
|---|---|
| Long-lived DV certificates | SSL certs are OV. CP section 3.2: All CA Disig certificates are issued with the validity period maximum of 36 month e.g. 3 years. |
| Wildcard DV SSL certificates | Comment #2: CA Disig does not issue wildcard DV SSL certificates |
| Email Address Prefixes for DV Certs | If DV SSL certs, then list the acceptable email addresses that are used for verification. |
| Delegation of Domain / Email validation to third parties | Comment #2: Domain validation is performed by CA Disig staff only. Email validation is performed by CA Disig staff or external RA staff according written procedures "MP_ERA_2009_06 Overenie e-mailu v žiadostiach (E-mail validation)". |
| Issuing end entity certificates directly from roots | No. See above. |
| Allowing external entities to operate subordinate CAs | No. See above. |
| Distributing generated private keys in PKCS#12 files | No. CPS section 6.1.1: CA Disig essentially does not make a key pairs generation for the foreign entity |
| Certificates referencing hostnames or private IP addresses | CA Disig never issued SSL certificates for registered IP address |
| Issuing SSL Certificates for Internal Domains | No. |
| OCSP Responses signed by a certificate under a different root | No. Tested. |
| CRL with critical CDP Extension | No. Tested. |
| Generic names for CAs | CN includes CA name. |