Bugzilla ID: 455878
Bugzilla Summary: Add CA Disig root certificate into browser

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, as per http://wiki.mozilla.org/CA:Information_checklist.

General Information	**Data**
CA Name	Disig
Website URL	http://www.disig.eu
Organizational type	Public Corporation
Primary market / customer base	Disig is a public Certification Service Provider, located in Slovakia. Disig is a member of international ASSECO Group, one of the strongest software houses in the CEE region. Asseco is a leader in selected IT segments in countries across Central and Eastern Europe.

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

Info Needed	**Data**
Certificate Name	CA Disig
Cert summary / comments	This root has no subordinate CAs, issuing end-entity certs for SSL, email, and code signing directly.
The root CA certificate URL	http://www.disig.eu/ca/cert/ca_disig.der
SHA-1 fingerprint.	2a:c8:d5:8b:57:ce:bf:2f:49:af:f2:fc:76:8f:51:14:62:90:7a:41
Valid from	2006-03-21
Valid to	2016-03-21
Cert Version	3
Modulus length / key length	2048
Test Website	https://kb.asseco.com
CRL	http://www.disig.eu/ca/crl/ca_disig.crl http://www.disig.sk/ca/crl/ca_disig.crl NextUpdate: 24 hours
OCSP	Not Applicable
List or description of subordinate CAs operated by the CA organization associated with the root CA.	This root has no subordinate CAs. From Disig: Our company is running only Root CA, because until now we have been providing a small number of certificate types. In the future we are planning to deploy a hierarchy of CA's where there will be one Root CA and several Sub CA. Each of these Sub CA will be responsible for issuing a specific type of certificates. Audit has proven that security measures applied to protect our CA are more than sufficent.

Subordinate CAs operated by third parties	None
Cross-Signing	None
Requested Trust Bits	Websites Email Code Signing
If SSL certificates are issued within the hierarchy rooted at this root CA certificate: DV, OV, and/or EV	OV CP section 3.1.7 Authentication of organization identity CP section 3.1.8 Authentication of individual identity
EV policy OID(s)	Not EV
CP/CPS	CA Disig CP (English): https://bug455878.bugzilla.mozilla.org/attachment.cgi?id=384717 CP CA Disig (in Slovak): http://www.disig.eu/_pdf/cp-disig.pdf Security Policy (in Slovak): http://www.disig.eu/_pdf/bp-disig.pdf Disig’s Certification Authority Website: http://www.disig.eu/index.php?id=ca&L=1
AUDIT	Audit Type: ETSI TS 102 042 Date of Report: 31.5.2008 (Expected completion of next audit 30.7.2009) Audit Report: http://www.disig.sk/_pdf/Audit_report_CA_statement.pdf The audit team members were: Lead Auditor: Mgr. Jan Cesnak, CISA auditor (license no. 650230) Expert 1: Ing. Rastislav Machel, CISSP Expert 2: Ing. Martin Spal Assoc. Professor Ladislav Hudec, PhD, CISA auditor (license no. 9921170) Auditor: Independent Team of Auditors managed by Mr. Jan Cesnak Audit Website: http://www.asint.sk/isaca/index.php?option=com_content&task=view&id=43&Itemid=56 From: Dept: Certification <certification@isaca.org> Date: Friday, November 14, 2008, 2:07 PM I have checked my records and can confirm that Mr. Jan Cesnak is CISA certified. From: Jan Cesnak <jan.cesnak@scientia.sk> Subject: RE: Verifying Authenticity of Audit report posted on Disig's website Date: Friday, November 21, 2008 according to your request, I can verify, that the audit report statement located at http://www.disig.sk/_pdf/Audit_report_CA_statement.pdf is authentic.

	Issues noted in audit report: "However, the security audit revealed some minor findings that are listed in the audit report, the audit team found no evidence of violating the Certification Authority policies, practices or procedures that could have material impact on the security of the certification services."

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

- Verify domain check for SSL
  - CP Section 3.1.9 Authentication of the component identity: 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. Ownership shows via written confirmation issued by authorized domain registration authority e.g. SKNIC is the national registration of top level Slovakian domains (www.sk-nic.sk). 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.
- 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.
  - CP Section 4.1.2 Procedure for registration of an applicant on the RA:
    - RA staff checked the completeness and accuracy of the data received in the certificate request. RA staff considering meaningfulness of all items taken into accounts (please see section 3.1.2) - violation of the principle of meaningfulness may be a reason for refusing to issue the certificate. Request for issuance of personal certificates for signing and encryption of electronic mail must be send electronically to the appropriate RA from addresses, which is included in the request in the field E-mail.
    - The applicant for a certificate shall satisfactorily demonstrate to the RA all the elements which entered into certificate request.
    - RA must verify whether electronically transmitted certificate request was sent by the applicant from the same e-mail address, which is located in the certificate request. In the case of the differences observed may refuse to issue the certificate
    - In connection with the verification of e-mail address make RA validation such way that will send e-mail response to e-mail, from which request was send.
- Verify identity info in code signing certs is that of subscriber
  - 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:
    - 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,

- 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:
  - 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.

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

- 1.1 Long-lived DV certificates
  - SSL certs are OV
  - CP Section 3.2: CA Disig certificates are issued with the validity of one year (usually 365 days), unless otherwise agreed by separate written agreement with the applicant.
- 1.2 Wildcard DV SSL certificates
  - SSL certs are OV
- 1.3 Issuing end entity certificates directly from roots
  - **This root issues end-entity certs directly.**
  - From Disig: "Our company is running only Root CA, because until now we have been providing a small number of certificate types. In the future we are planning to deploy a hierarchy of CA's where there will be one Root CA and several Sub CA. Each of these Sub CAs will be responsible for issuing a specific type of certificates. Audit has proven that security measures applied to protect our CA are more than sufficient. This was also one of the reasons that convinced company Microsoft to add our Root CA certificate into their store (MS update will be issued on November 25, 2008)."
- 1.4 Allowing external entities to operate unconstrained subordinate CAs
  - No. This root does not have subordinate CAs.
- 1.5 Distributing generated private keys in PKCS#12 files
  - No. CP section 3.1.6 Method to prove possession of private key: RA will require the applicant for the certificate confirmed that it possesses the private key that corresponds to a public key contained in the certificate request.
  - CP Section 3.1: Application for a certificate received by CA Disig must comply with the standard PKCS # 10 or SPKAC
- 1.6 Certificates referencing hostnames or private IP addresses
  - CP Section 3.1.9 Authentication of the component identity**: In the case of registered IP addresses** RA will 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.
- 1.7 OCSP Responses signed by a certificate under a different root
  - N/A
- 1.8 CRL with critical CIDP Extension
  - CRLs downloaded into Firefox without error

Verify Audits (Sections 8, 9, and 10 of http://www.mozilla.org/projects/security/certs/policy/)

- Validate contact info in report, call to verify that they did indeed issue this report.
  - Complete – verified auditor, and confirmed with auditor that the audit letter is authentic.
- For EV CA’s, verify current WebTrust EV Audit done.
  - N/A
- Review Audit to flag any issues noted in the report
  - “However, the security audit revealed some minor findings that are listed in the audit report, the audit team found no evidence of violating the Certification Authority policies, practices or procedures that could have material impact on the security of the certification services.”