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
List any other root CAs that have issued cross-signing certificates for this root CA	None
Requested Trust Bits • Websites (SSL/TLS) • Email (S/MIME) • Code Signing	Websites Email Code Signing
If SSL certificates are issued within the hierarchy rooted at this root CA certificate: DV, OV, and/or EV	OV
EV policy OID(s)	Not EV
CP/CPS	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 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 CA Disig practice was audited by the independent team of auditors as is required by national legislation given by Article 25 of 215 Act of 15 March 2002 on electronic signature and on amendment of some acts as amended by Act No. 679/2004 Coll., Act No. 25/2006 Coll. and Act No. 275/2006 Coll.

	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 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 page 27, section 3.1.9 [Translation provided by Disig]: Applicant shell proves to the Registration Authority that he is an owner of the domain for which he is requesting certificate. Ownership is established by written certification from authorized registry e.g. Slovak Top Level Domain Registry (www.sk-nic.sk) etc. Registration Authority shell verify this written certification from independent source on Internet e.g www.sk-nic.sk for Slovak domain; www.eurid.eu for European domain etc.
        - Google Translation of the corresponding paragraph: In the case pouțitia domain name is the condition that the domain second level included the subject who is țiadateľom on the certificate for the server. The entity must show RA, Te is drțiteľom domain for which the issue țiada certificate. Prove ownership of the written confirmation of Authorized registration authority of your domain name eg. SK-NIC is the national registrar top level domains (www.sk-nic.sk). Registration Authority verifies a written confirmation from independent sources on the Internet such as. www.sk-nic.sk domain SK respectively. www.eurid.eu Domain EU etc..
        - Note: The typical value of this poloțky will complete the domain name or registered IP address.
- 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 page 34, section 4.1.2 point 3 and 4 [Translation provided by Disig]: Applicant shell send certificate request for a certificate to be used for digitally signing and/or encrypting email messages to the CA Disig registration authority (RA) via e-mail. Registration authority shell check if the request for particular applicant was sent from the same e-mail address as is inside his request. If there is

difference RA may refuse issue certificate. In addition to this check, RA performs confirmation of the applicant's e-mail address through an answer to e-mail address from which request was sent.

- Google Translation of Section 4.1.2: Procedure for registration of an applicant for a certificate to the RA
  - 1. RA worker checked the completeness and accuracy of data received ţiadosti certificate. When considering the values of all the worker takes poloţiek RA the meaningfulness of these values (bliţšie see section 3.1.2) - breach of meaningfulness principle möte be a reason for refusing to issue certificate. Ţiadosť the issue a personal certificate designated for signing and encryption of electronic mail must be sent RA electronically to the appropriate address of which will be indicated in ţiadosti certificate in poloţke E-mail.
  - 2. Ţiadateľ certificate to the RA must satisfactorily demonstrate all data that has entered into various poloţiek ţiadosti certificate.
  - 3. RA must verify whether the electronic transmission ţiadosť on the issue of the certificate of ţiadateľa was sent from the same e-mail address, which is located in ţiadosti the issue of the certificate. In the case of the differences observed möte refuse edition certificate.
  - 4. In connection with the verification e-mail made worker confirm the validity of RA e-mail response to e-mail, which was sent ţiadosť.
  - 5. Through a CA Disig be automatically verify the public key contained in the certificate predloţenej ţiadosti ut not previously issued certificate. If it was, RA ţiadosť certificate refuses For safety reasons, to accept, since ut once certified public key muteness pouţitý be in another certificate.
  - 6. The worker shall notify the RA ţiadateľa certificate bearing the words "Treaty on the issue of pouţívaní a certificate and sluţieb CA Disig. Consent ţiadateľa with this text contract is a condition for issuing the certificate.
  - 7. RA Vlotho worker in a CA certificate ţiadosť poţadované and other data. In the case of the Te ţiadosti certificate for some reason is not moţné make the certificate, the CA shall notify the RA, including the presentation of the relevant reason, which then notifies ţiadateľa certificate. Ţiadateľ certificate in this case must submit a new ţiadosť certificate.
  - 8. In the case of the downstream ţiadosti certificate shall proceed in accordance with Chapter 3.2.

- Verify identity info in code signing certs is that of subscriber
  - Applicant for the certificate presents: name of software component, URL and application description (this can be understood as the declaration on word of honor). Also he is signing the declaration on word of honor that the content of contract complies with the provided documents.
  - Google Translation of CP Section 3.1.7, Authentication of identity legal person: Legal person established in the Slovak Republic is proving its totoţnosť extract from the Commercial Register or. other existing register of legal persons. It vyţadovaný / and the original or certified copy of the original, not the older than three months. Evidence must include full name, identifier (usually ICO), established, name-plated person acting / them legal person and the way the case for the signing of a legal person. If Te is not a legal person established in the territory of Slovak Republic, its totoţnosť be verified in the same manner as described above. List of valid register of legal persons shall be officially preloţený in the English language (except for organizations based in the Czech Republic).

- If Te legal person muteness prove his statements totoţnosť from the commercial register (valid for non-entities such as. municipality, Church, civic zdruţenie Foundation, a national body, etc.), that legal person, in writing, except to prove the legality of his totoţnosti (resp. "Reason") of its existence (with vyuţitím a reference to the law or other regulation which the body of the type of deals).
- Google Translation of CP Section 3.1.8, Authentication of identity of physical persons: CMA must be guaranteed, te ţiadateľa identity certificate and its public key is adequately integrated. Kaţdá CMA shall specify in its CPS procedures ţiadateľa to authenticate the identity of the certificate. CA will record this
  kaţdý process for the certificate in written or electronic form. Documentation on the identification must include at least:
  - identity of the person who carries out the identification,
  - unique identification numbers of predloţených licenses dokladujúcich
  - authenticated identity of the person
  - date and site of the identification.
- The documentation of the identification document must be personally signed ţiadateľom, in the presence of the person conducting the authentication of identity, including ţiadateľa identifying information on the certificate. Ţiadateľom certificate möte be age Slovak Republic or a citizen of a foreign national. Verification of identity performed CMA on the basis of these predloţenia Data:
  - full name and surname,
  - residence (in the case, Te is given in the document)
  - identification number (citizen and a citizen of the Czech Republic Czech Republic)
  - date of birth (other national)
  - Card number totoţnosti,
  - totoţnosti card issuer,
  - Date license totoţnosti.
  - Other poţiadavky for initial registration ţiadateľa (drţiteľa) are described in detail Chapter 3.1.10 and 3.1.11.
- Google Translation of Section 3.1.11, Examination of documents submitted to the RA worker checked on the predloţených documents include the following:
  - Personal documents of natural persons:
    a) compliance of the data referred to in ţiadosti with the provisions of the Personal documents, particularly the name and residence;
    b) the validity predloţeného document
    c) physical age (ie age 18 years),
    d) consistency between the photograph and your personal view of the owner Personal document
    e) compliance in the document that is predloţených whether the data in one document not the data in another document.
  - Extracts from the Commercial Register or. a register of legal persons:
    a) a dump - there must be older than 3 months
    b) acting as a legal entity - ie, whether it has physica lperson, which predloţili the statement, the right to act (sign) for the legal person
    c) the form of statements - original or official (notary / registry) a certified copy extract.

- Consent to the issuance of the certificate:
  a) the authority to act for the company - the person signing the consent must be authorized to represent the employer. Eligibility is checked by extract from OR respectively. another designated register (or the outset documents, credentials, a letter of appointment). With signing person is not registered in this statement must predložiť another document on the basis of möte which act as a company (usually a notary authenticated credentials).
  b) The - as far as the agreement of the period of validity, controls the this figure.
- Full power:
  a) verification of the mandate (notary / registry)
  b) consistency of the data listed in the proxy, defining, representing physical respectively. legal person, with the data provided on the personal papers representing a natural person, respectively. with those set out in the statement of business or. another register representing a legal person,
  c) the scope of the mandate - that is whether the mandate authorized or empowered to physical požadovanému person to act on behalf of RA in the Enabling natural or legal persons,
  d) any time limit. other conditions specified in the proxy
- Sworn statements:
  a) the authority to sign - the person signing the declaration must be authorized to represent the legal person. Eligibility is checked by an extract from OR respectively. a register of legal persons. As signatory is not registered in this statement, the other predložiť evidence on which möte act as a company (usually notary certified credentials)
  In the case of any reasonable doubt about the potential totožnosti customer, for example, in the case of the deficiencies found in the predložených documents respectively. predložení incomplete evidence, the worker registration RA žiadateľa deny. Služba issue of the certificate in this case will be dismissed.

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

- 1.1 Long-lived DV certificates
  - SSL certs are OV
- 1.2 Wildcard DV SSL certificates
  - SSL certs are OV
- 1.3 Issuing end entity certificates directly from roots
  - This root does not have subordinate CAs. It 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
  - N/A

- 1.5 Distributing generated private keys in PKCS#12 files
  - No
- 1.6 Certificates referencing hostnames or private IP addresses
  - Google Translation of paragraph on page 27 of CP: In the case of registered IP addresses pouțitia RA will consider whether the entity -- țiadateľ certificate for the server pouțíva the registered IP address that is legitimately whether the registered IP address is the address segment, which is organization registered in the RIPE for the body - țiadateľa the certificate for the server. In this case, is automatically assumed by Te, Te body - țiadateľ certificate for the server pout in țiadosti certificate registered IP address, given CA Disig solemn declaration, the IP te pouțíva lawfully and Te is aware all the consequences and responsibility for any unauthorized pouțívanie the IP address.
- 1.7 OCSP Responses signed by a certificate under a different root
  - N/A
- 1.8 CRL with critical CIDP Extension
  - CRL 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."