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.
CA Contact Information	CA Email Alias: disig@disig.sk CA Phone Number: + 421 2 208 50 140 Title / Department: CA Disig

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
CA Hierarchy	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.

Sub-CAs operated by 3rd parties	None
Cross-Signing	None
Requested Trust Bits	Websites Email Code Signing
If SSL certificates: DV, OV, and/or EV	OV
EV policy OID(s)	Not EV
CP/CPS	CA Disig CPS (Slovak – version 4.0): http://www.disig.sk/_pdf/cps_ra_cadisig.pdf CA Disig CP (Slovak – version 4.0): http://www.disig.eu/_pdf/cp-disig.pdf CA Disig CP (English – version 3.4): https://bug455878.bugzilla.mozilla.org/attachment.cgi?id=384717 Security Policy (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 Auditor: Scientia, a.s. (Sartorisova 21, 821 08 Bratislava 2) Auditor Website: http://www.scientia.sk/ Audit Report: https://bug455878.bugzilla.mozilla.org/attachment.cgi?id=418236 (2009.11.13) Lead Auditor: Ing. Rastislav Machel, CISSP Expert 1: Ing. Martin Mach, MCSE Expert 2: Ing. Martin Spal, CISA Comment #26: Due to the specific audit area, an responsible, experienced and independent auditor Mr. Machel (CISSP) was contracted, to perform the security audit with help of Mr. Mach (MCSE) – employee of Scientia company. Contact information: rastislav.machel@machel-cs.eu, martin.mach@scientia.sk Mr. Spal (CISA), as an employee under review Disig company, which operates the CA, worked in audit team just as a formal participant in order to supervise the conduct of the audit. He did not active participate on security audit performance. 12/17: Completed email exchange with Mr. Mach of Scientia. He sent an updated audit statement, which I attached to the bug. 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 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.
Organization Identity Verification	Google Translations from CPS 3.1.7 Authentication of identity of the legal person (organization) Certificate Subscriber acting on behalf of the legal person must provide corporate name, other identifier, if one exists (usually it's such. ID), address and proof of the existence of the legal person (usually an extract from the Commercial Register). RA verifies the data and the identity of the person except pouțívateľa (țiadajúcej person) certify the person has the right to act on behalf of the legal person in case the certificate. A legal person established in the Slovak Republic is proving its totoțnosť extract from the commercial register if necessary. other applicable corporate registry. It vyțadovaný plated original or certified copy of the original, not older than three months. The document must include the full business name, identifier (usually ID), location, name of the person / persons acting them as a legal person of action and the signing of a legal person. If subscriber is not a legal person established in the Slovak Republic, the subscriber must be verified in the same manner as above. Extract from the current register of legal entities must be officially preloțený into the Slovak language (except for organizations based in the Czech Republic). Natural persons under predloțeného extract from the Register for RA acting as a legal entity in the case of obtaining a certificate, they must prove their organization under Section 3.1.8. On behalf of the legal person Mote on RA to act as an authorized person pouțívateľa ie person who is the statutory (or more of such persons at the same time, if vyțaduje predloțený extract from the Commercial Register), where the legal entity Mote be represented by another person or legal entity. If a legal person representing the RA left, representing the natural or legal person must be consulted vțdy predloțiť certified extract from the Register of legal persons represented no older than three months. If a legal person left to represent the RA is a natural person, this represents a natural person must demonstrate its totoțnosť under section 3.1.8 and in addition must show a certified (by a notary or the registrar office) powers of

	text which is clearly evident Te representing individual Enabling is acting as a legal person to act in the matter on its behalf. If a legal person representing the RA allow another legal person representing the legal person other than the power of attorney (see previous paragraph) must prove his totoťnosť same way as a legal person is represented as poťadované above. Entity (natural or legal person), which represents the legal person in case of a legal person represented in the case of muteness ťiadnom represented by another entity. If Te entity to prove its dumbness totoťnosť extract from the commercial register (valid for non-commercial entities such as. Community, church, civic zdruťenie, foundation, public authority, etc.), such person shall be evidenced in writing in addition to its legality and totoťnosti (respectively. "ground") of its existence (and vyuťitím with reference to law or regulation which the body deals with that type). 3.1.8 Authentication of identity of physical persons Mote to be a natural person of age a citizen of the Slovak Republic or a foreign national. A natural person must demonstrate its ownership of two of the following personal documents: ID card, passport, driving license, birth certificate, a temporary residence permit (or residence) in the case of an alien firearms license sluťobný Card Poťaduje the same time that at least one of the documents submitted was a document which includes a photograph of the person. For predloťenia birth certificate, license or firearms license sluťobného must predloťiť also one of the following documents: ID card or passport. If a natural person representing the RA another natural person must also demonstrate a certified (by a notary or the registrar office) powers of text which is clearly evident te representing a natural person is acting Enabling an individual to act in the matter on its behalf. If the entity represents a natural person, other than full power (see previous paragraph) must be empowered to establish his legal person totoťnosť under Section 3.1.7. Entity (natural or legal person), which represents a natural person, in case of a natural person represented in the case of muteness ťiadnom represented by another entity.
Domain Name Ownership / Control	Comment #24: Article 3.1.9 of CA Disig CP and CPS was modified in the following way: “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. 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 sufficient for sending email. In the event that there is no e-mail address respectively there is no response from expected e-mail addresses because it does not exist, RA must take further steps to verify domain ownership for example use published contact data of domain registrar. 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, RA refuses to issue a certificate to that request.”

	CA Disig also issued detailed manual for its registration authorities how to proceed in verification of ownership/control of domain. The CP/CPS was updated and the same process as described above is used also for non-Slovak domains. Registration authorities are obliging exploit WHOIS services of top domain sponsoring organization which are listed at http://www.iana.org/domains/root/db/. Google Translation from updated CPS: 3.1.9 Authentication of identity component CMA must be guaranteed even in this case, the identity component and its public key are adequately bonded. Hardware or software component that will pouțívať certificates will be subject to certification and is therefor a moțné Disig CA certificate or server. Certificate for the software component. (meaning no personal certificate). In this case, the component must be assigned to natural or legal person (organization), which he manages (see Section 5.2). This person or organization must provide the following information to RA, as described in sections 3.1.8 and 5.2: the identification device (a software component name), device public key (contained in the Certificate țiadosti), authentication devices and their attributes (if any be listed on the certificate), contact details, the CMA may, if necessary, to communicate with this person in a software component, the purpose for which the certificate pouțívaný RA must authenticate the accuracy of any authorization (value poloțky distinguishing name) to be listed in the certificate and verifies predloțené data. Methods for implementing the authentication and control data include: verifying the identity of the person in accordance with poțiadavkami section 3.1.8, verifying the identity of the organization, which includes the component, in accordance with poțiadavkami section 3.1.7, pouțitia eligibility verification data to be included in each poloțkách certificate, with an emphasis on content poloțky CommonName. A typical value of poloțky the full domain name. The existence of a domain and its owner has been verified by sluțby provided WHOIS Web top level domain (eg domain ". Com" is the controller SK-NIC - www.sk-nic.sk; for the domain. Eu is the administrator EURid vzw / asbl established in Belgium for the domain. "com" is manager 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 sluțby WHOIS. Țiadateľ a certificate for the domain must send back a verification information as proof of ownership of the domain specified period of time sufficient for sending email. If Te is not available țiadna e-mail address respectively. the expected e-mail addresses received verification information back RA because it does not exist, RA must take further steps to verify domain ownership, eg.

	Posted vyuțiť domain registrar contact information. With the data obtained from the above sources is moțné reliably determine the owner of Te țiadateľ respectively. person acting on behalf of the owner of the domain, RA refuses to issue the certificate țiadosť.
Email Address Ownership / Control	Comment #24: CP and CPS were modified in the following way: (CP) Article 4.1.1. "Request for a certificate for signing and encryption of electronic mail shall be send to the relevant RA in advance electronically from e-mail address which is included in the request for certificate in the field „E-mail". E-mail addresses of RA CA Disig are available on the Disig web site" (CP) Article 4.1.2 Item 1: "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." (CP) Article 4.1.2 Item 3: "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" (CP) Article 4.1.2 Item 4: "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 request for a certificate, 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. 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." (CPS) Article 4.1.1.1: "Send electronically certificate request to the RA - RA e-mail addresses are available on the Disig website (see 1.4). Certificate request decided for signing and encryption of electronic mail extension "Secure Email (1.3.6.1.5.5.7.3.4)" shall be send from an e-mail address specified in the certificate request." (CPS) Article 4.1.1.2: "Note: Customer must be able to identify on the RA RequestId indication value (as numeric string proceeded by the string "disigweb" that uniquely identifies the generated certificate request) of the certificate request. Application for a certificate for signing and encryption of electronic mail shall be send to the RA electronically in advance (see 4.1.1.1)." (CPS) Article 4.1.1.3 Item 1: "RA staff verify if electronically sent certificate request from an applicant (it is compulsory for certificates with extension "Secure Email (1.3.6.1.5.5.7.3.4)"), was sent from the same e-mail addresses, what is in the certificate request. If the differences observed refuses to issue the certificate."

	(CPS) Article 4.1.1.3 Item 12: “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.” CA Disig also issued detailed working manual for its registration authorities how to proceed in verification of ownership/control of e-mail address. Google translation from updated CPS: 4. Operational requirements 4.1 Requiring Certificate When žiadateľ Certificate požiada the certificate žiadateľ and RA must perform the following steps: Verify and record the identity žiadateľa (under section 3.1) Žiadateľ must have generated key pair (public and private key) for každý him požadovaný certificate to prove te public key pair is key private key owned žiadateľom Certificate (under Section 3.1.6) Provide sufficient documentation to verify any particulars to be given to the certificate All communication between zložkami CA žiadosti on the certificate and the certificate issuing process has to be authenticated and protected from modification using mechanisms appropriate požiadavkám data to be protected použitím previously issued certificates. Any electronic transmission of shared secrets must be made encrypted. 4.1.1 A detailed procedure for obtaining a personal certificate and certificate of legal person 4.1.1.1 Preparing to visit RA Customer (žiadateľ Certificate) take the following steps: They will get acquainted with this procedure, possibly with the principles and instructions for obtaining a certificate. Generate on your computer using compliant browser žiadosť new certificate via the web site of Disig (see URL section 1.4) and uloží it to the appropriate medium (HDD, USB drive, floppy, etc..). Prepare your chosen documents totožnosti respectively. other necessary documents, for example. Extract from the commercial register (we recommend to verify the validity of documents) under the provisions of Part 3 Visits by appointment RA (phone, email). Žiadosť electronically transmit the certificate to be issued at the RA - RA e-mail addresses are available on the website of Disig. (see 1.4). Žiadosť a certificate for signing and encryption of electronic mail must be sent from email addresses appearing in the Certificate žiadosti in položke E-mail.

	4.1.1.2 Visit RA A customer at an agreed time comes to RA, taking with them and identify respectively. predloţí: Ţiadosť a certificate in electronic form (generated by the browser) Selected papers totoţnosti respectively. other necessary documents, for example. Extract from the Commercial Register, credentials, etc.. under the provisions of Part 3 Penati appropriate amount, if not previously agreed another form of payment for the certificate. 4.1.1.3 Procedure for RA ţiadosti sent electronically 1. RA worker verify electronically sent ţiadosť for a certificate of ţiadateľa (compulsory licenses for enlargement Secure Email (1.3.6.1.5.5.7.3.4) "), was sent the same e-mail addresses, what is in ţiadosti the certificate is issued. If the differences observed refuses to issue the certificate. 2. If te ţiadosť sent in advance of issuing the certificate contains the same e-mail address from which it was sent, the RA shall verify the worker checks the e-mail address. Verification is carried out by Te on the e-mail address send a mail message containing a secret unpredictable information (authentication information). Ţiadateľ the certificate must be sent back verification information as evidence of control of the e-mail addresses. The answer must be sent within a specified period of time sufficient for sending email. If te check e-mail addresses run unsuccessfully, CA Disig refuses to issue the certificate. Detailed procedure is described in the manuals for workers and the RA is also subject to the initial training of staff RA. 3. For contractual partners Disig who sent ţiadosti to issue a certificate with the contracted domain ownership verification e-mail address does not.
Identity of Code Signing 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.

Potentially Problematic Practices	http://wiki.mozilla.org/CA:Problematic_Practices
	• Long-lived DV certificates
	  o SSL certs are OV
	  o 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.
	• Wildcard DV SSL certificates
	  o SSL certs are OV
	• Delegation of Domain / Email validation to third parties
	  o Based on the feedback provided from the first round of public discussion, Disig has performed the following actions:
	  ▪ CA Disig issued detailed manual for its registration authorities how to proceed in verification of ownership/control of domain.
	  ▪ CA Disig also issued detailed working manual for its registration authorities how to proceed in verification of ownership/control of e-mail address.
	  ▪ The scope of compliance audit performed during November 2009 was extended to include Mozilla root inclusion requirements.
	• Issuing end entity certificates directly from roots
	  o This root issues end-entity certs directly.
	  o Result from first discussion: It is noted that the CA Disig root certificate does not have subordinate CAs.However, as per previous discussions, this alone does not prevent a root certificate from being included. No action required from CA.
	  o 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).”
	• Allowing external entities to operate unconstrained subordinate CAs
	  o No. This root does not have subordinate CAs.
	• Distributing generated private keys in PKCS#12 files
	  o 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.
	  o CP Section 3.1: Application for a certificate received by CA Disig must comply with the standard PKCS # 10 or SPKAC

	• Certificates referencing hostnames or private IP addresses
	  o There used to be information in section 3.1.9 of the CP (see the old English translation) which indicated private IP addresses were allowed. This information about IP addresses has been removed from the new (version 4.0) CP.
	• OCSP Responses signed by a certificate under a different root
	  o N/A
	• CRL with critical CIDP Extension
	  o CRLs downloaded into Firefox without error
	• Generic names for CAs
	  o Root name is not generic.