CERTISIGN	TÍTULO: **Subordinate CAs Operated by Third Parties For External Use – Mozilla** **Certisign Information**	DATA : **03/19/2009**

1. Sub-CA Company Name

   [Certisign] Certisign Certificadora Digital S.A.

2. Sub-CA Corporate URL

   [Certisign] http://www.certisign.com.br

3. Sub-CA cert download URL

   [Certisign] http://icp-brasil.certisign.com.br/repositorio/certificados/AC_Certisign_Multipla_G3.cer

4. General CA hierarchy under the sub-CA.

   [Certisign] End-Entity Certificates.

5. Sub-CA CP/CPS Links

   [Certisign] http://icp-brasil.certisign.com.br/repositorio/dpc

6. The section numbers and text (in English) in the CP/CPS that demonstrate that reasonable measures are taken to verify the ownership of the domain name and email address for end-entity certificates chaining up to the root, as per section 7 of our Mozilla CA certificate policy.
   - domain ownership/control
   - email address ownership/control
   - digitally signing code objects -- entity submitting the certificate signing request is the same entity referenced in the certificate

[Certisign] 3.1.11.2. Procedures for identification purposes of an equipment or application

For equipment certificates or application certificates that use URL in Common Name, is verified if the certificate applicant detain the domain name register with the relevant agency, or if it has titular domain authorization for using that name. In this case it's showed evidential documentation (term of authorization term of domain or similar) properly signed by the titular of domain.

(http://icp-brasil.certisign.com.br/repositorio/dpc/AC_Certisign_Multipla/DPC_AC_Certisign_Multipla_v3.0.pdf)

7. Identify if the SSL certificates chaining up to the sub-CA are DV and/or OV. Some of the potentially problematic practices only apply to DV certificates.
   - DV: Organization attribute is not verified. Only the Domain Name referenced in the certificate is verified to be owned/controlled by the subscriber.
   - OV: Both the Organization and the ownership/control of the Domain Name are verified.

   [Certisign] SSL certificates that chains up to the sub-CA are OV.

8. Review the CP/CPS for Potentially Problematic Practices. Provide further info when a potentially problematic practice is found.

[Certisign]

- Long-lived DV certificates

Not applicable. Certisign does not issue DV certificates. All production certificates are OV.

3.1.11. Authentication of Equipment Identify or Equipment Application

3.1.11.1. General Resolutions

3.1.11.1.1. Regarding certificates issued for equipment or application, the titular is the natural person or the legal entity that claims the certificate, who indicates the responsible for the private key.

3.1.11.1.2. If the titular be natural person, your identity is confirmed as written in the item 3.1.9.1 and it signs the titular term regarding the item 4.1.1.

(http://icp-brasil.certisign.com.br/repositorio/dpc/AC_Certisign_Multipla/DPC_AC_Certisign_Multipla_v3.0.pdf)

- Wildcard DV SSL certificates

Not applicable. Certisign does not issue Wildcard certificates.

7.1.4. Names Format

In an Equipment or application certificate, the CN identifier contains the correspondent URL or application name, and doesn't contain the E field.

(http://icp-brasil.certisign.com.br/repositorio/pc/AC_Certisign_Multipla/PC_A1_AC_Certisign_Multipla_v2.3.pdf)

- Delegation of Domain / Email validation to third parties

3.1.11. Authentication of Equipment Identify or Equipment Application

3.1.11.1. General Resolutions

3.1.11.1.1. Regarding certificates issued for equipment or application, the titular is the natural person or the legal entity that claims the certificate, who indicates the responsible for the private key.

3.1.11.1.2. If the titular be natural person, your identity is confirmed as written in the item 3.1.9.1 and it signs the titular term regarding the item 4.1.1.

(http://icp-brasil.certisign.com.br/repositorio/dpc/AC_Certisign_Multipla/DPC_AC_Certisign_Multipla_v3.0.pdf)

- Issuing end entity certificates directly from roots

Not applicable. Certisign's hierarchy are composed by an Intermediate CA.

- Allowing external entities to operate unconstrained subordinate Cas

Not applicable. All Certisign's subordinated CAs are operated by its Processing Center.

- Distributing generated private keys in PKCS#12 files

Not applicable. Each subscriber must generate its own private key.

6.1.1.Key Pair Generation

6.1.1.1. The cryptographic key pair is generated by the certificate titular, when it be a general person and generated by the responsible person, indicated by their legal representatives, when it be a legal entity.

(http://icp-brasil.certisign.com.br/repositorio/pc/AC_Certisign_Multipla/PC_A1_AC_Certisign_Multipla_v2.3.pdf)

- Certificates referencing hostnames or private IP addresses

Certisign Múltipla CA CP:

7.1.4. Names Format

In an Equipment or application certificate, the CN identifier contains the correspondent URL or application name, and doesn't contain the E field.

7.1.2.8 Certisign Múltipla CA Implements the extension Authority Information Access, not critical, including the access address to the On-line Certificate Status Protocol service (http://ocsp.certisign.com.br).

(http://icp-brasil.certisign.com.br/repositorio/pc/AC_Certisign_Multipla/PC_A1_AC_Certisign_Multipla_v2.3.pdf)

- OCSP Responses signed by a certificate under a different root

Not applicable. Certisign does not permit Indirect OCSP Responses.

- CRL with critical CIDP Extension.

Not applicable. Certisign doesn't issue certificates with CIDP extension.

7.1.2. Certificate Extensions

7.1.2.1. This item describes all the used extensions and your criticality.

7.1.2.2. Certificates issued by Certisign Multipla CA contains the following obligatory extensions:

a) CRL Distribution Points, not critical: contains the web addresses where can be found CRL from Certisign Multipla CA:

For certificates issued up to 10/31/2008

http://icp-brasil.certisign.com.br/repositorio/lcr/ACCertisignMultiplaV3/LatestCRL.crl

http://icp-brasil.outralcr.com.br/repositorio/lcr/ACCertisignMultiplaV3/LatestCRL.crl

http://repositorio.icpbrasil.gov.br/lcr/Certisign/ACCertisignMultiplaV3/LatestCRL.crl

For certificates issued from 11/01/2008

http://icp-brasil.certisign.com.br/repositorio/lcr/ACCertisignMultiplaG3/LatestCRL.crl

http://icp-brasil.outralcr.com.br/repositorio/lcr/ACCertisignMultiplaG3/LatestCRL.crl

http://repositorio.icpbrasil.gov.br/lcr/Certisign/ACCertisignMultiplaG3/LatestCRL.crl

(http://icp-brasil.certisign.com.br/repositorio/pc/AC_Certisign_Multipla/PC_A1_AC_Certisign_Multipla_v2.3.pdf)

- Generic names for CAs.

It's not a CPS requirements, but by internal procedure, Certisign always includes the term "Certisign" in their CAs.

9. If the root CA audit does not include this sub-CA, then for this sub-CA provide a publishable statement or letter from an auditor that meets the requirements of sections 8, 9, and 10 of our Mozilla CA certificate policy.

[Certisign] The root CA audit includes this sub-CA and it is done annually.

10. Provide information about the CRL update frequency for end-entity certificates. There should be a statement in the CP/CPS that the sub-CA must follow to the effect that the CRL for end-entity certificates is updated whenever a certificate is revoked, and at least every 24 or 36 hours.

[Certisign] Certisign Multipla CA CP/CPS implements CRL update frequency for end-entity certificates of 1 hour. In spite of using 1 hour, Certisign Multipla CRL is issued every 30 minutes.

Certisign Múltipla CA CP:

4.4.9 CRL Update Frequency

4.4.9.1. In this item is defined the CRL update frequency regarding end-entity certificates.

4.4.9.2. The CRL update frequency is 1 (one) hour.

(http://icp-brasil.certisign.com.br/repositorio/dpc/AC_Certisign_Multipla/DPC_AC_Certisign_Multipla_v3.0.pdf)