EY - RJ
Praia de Botafogo, 370
Botafogo, Rio de
Janeiro.
CEP: 22250-909

Tel: +55 21 3263 7000
Fax: +55 21 3263 7002
ey.com.br

Independent Assurance Report

To the Management of CERTISIGN CERTIFICADORA DIGITAL - Certisign Trust Network – Certificate Authority:

Scope

We have examined Certisign Certificadora Digital - Certisign Trust Network (CERTISIGN-CA) management's assertion, that for its Certification Authority (CA) operations in Brazil, during the period of June 12th 2018 to September 10th 2018, for CAs as enumerated in the appendix A for SSL Baseline Requirements and Network Security Requirements, CERTISIGN - CA has:

- Disclosed its SSL certificate lifecycle management business practices in its:
    - Certification Practice Statement

  including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirement on the CERTISIGN - CA website, and provided such services in accordance with its disclosed practices

- Maintained effective controls to provide reasonable assurance that:
    - the integrity of keys and SSL certificates it manages is established and protected throughout their life cycles; and
    - SSL subscriber information is properly authenticated (for the registration activities performed by CERTISIGN – CA)

- Maintained effective controls to provide reasonable assurance that:
    - Logical and physical access to CA systems and data was restricted to authorized individuals;
    - The continuity of key and certificate management operations is maintained; and
    - CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity

- Maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

based on the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3. Certisign - CA's management is responsible for its assertion. Our responsibility it to express an opinion on management's assertion based on our examination.

EY - RJ
Praia de Botafogo, 370
Botafogo, Rio de
Janeiro.
CEP: 22250-909

Tel: +55 21 3263 7000
Fax: +55 21 3263 7002
ey.com.br

Certification authority's responsibilities

CERTISIGN - CA management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3.

Our independence and quality control

We have complied with the independence and other ethical requirements of the Code of Ethics for Professional Accountants issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care confidentiality and professional behavior.

The firm applies International Standard on Quality Control 1, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Auditor's responsibility

Our responsibility is to express an opinion on management's assertion based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion is fairly stated, and, accordingly, included:

1. obtaining an understanding of CERTISIGN - CA's SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of SSL certificates, and obtaining an understanding of CERTISIGN - CA's network and certificate system security to meet the requirements set forth by the CA/Browser Forum;
2. selectively testing transactions executed in accordance with disclosed SSL certificate lifecycle management practices;
3. testing and evaluating the operating effectiveness of the controls; and,
4. performing such other procedures as we considered necessary in the circumstances.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Relative effectiveness of controls

The relative effectiveness and significance of specific controls at CERTISIGN - CA and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

EY - RJ
Praia de Botafogo, 370
Botafogo, Rio de Janeiro.
CEP: 22250-909

Tel: +55 21 3263 7000
Fax: +55 21 3263 7002
ey.com.br

Building a better working world

Inherent limitations

Because of the nature and inherent limitations of controls, CERTISIGN - CA's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorized access to systems and information or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

Emphasis on matters

Certisign Certificadora Digital - Certisign Trust Network (CERTISIGN-CA) has reported a control deficiency on management's assertion. For this deficiency, we performed additional procedures and were able to obtain reasonable assurance that the risks associated were mitigated during the audit period.

Observation	Relevant Webtrust Criteria	Mitigating Procedure
The Certification Authority (CA) discloses on the respective Certification Practice Statement (CPS), Certificate Policy (CP) and certificates, that it operates OCSP (Online Certificate Status Protocol) responses. However, this service was not fully implemented by the CA prior to August 24, 2018.	PRINCIPLE 2 - Service integrity: 5.5 The CA maintains controls to provide reasonable assurance that the CA: • makes revocation information available via the cRLDistributionPoints and/or authority Information Access certificate extensions for Subordinate CA and Subscriber Certificates in accordance with the SSL Baseline Requirements Section 7.1.2. • for high-traffic FQDNs, distributes its OCSP responses in accordance with SSL Baseline Requirements. 5.6 The CA maintains controls to provide reasonable assurance that an online 24x7 Repository is provided that application software can use to automatically check the current status of all unexpired Certificates issued by the CA, and: • for the status of Subscriber Certificates: o If the CA publishes a CRL, then the CA shall update and reissue CRLs at least once every seven (7) days, and the value of the next Update field must not be more than ten (10) days beyond the value of the this Update field; and o The CA shall update information provided via an Online Certificate Status Protocol (OCSP) at least every four (4) days and OCSP responses must have a maximum expiration time of ten (10) days. • for the status of subordinate CA Certificates o The CA shall update and reissue CRLs at least (i) once every twelve (12) months and (ii) within 24 hours after revoking a Subordinate CA Certificate, and the value of the next Update field must not be more than twelve months beyond the value of the this Update field; and o The CA shall update information provided via an Online Certificate Status Protocol at least (i) every twelve (12) months and (ii) within 24 hours after revoking a Subordinate CA Certificate. • The CA makes revocation information available through an OCSP capability using the GET method	As part of our audit procedures, we were able to confirm that the CA started to operate OCSP responses in August 24, 2018. In addition, we verified through a detailed analysis of the complete list of certificates issued until August 24, 2018 – date when the CA started to operate OCSP responses - that certificates were issued only internally to CERTISIGN group as part of a "testing" period, with no impact to external customers.

EY - RJ
Praia de Botafogo, 370
Botafogo, Rio de Janeiro.
CEP: 22250-909

Tel: +55 21 3263 7000
Fax: +55 21 3263 7002
ey.com.br

	for Certificates issued in accordance with the SSL Baseline Requirements. 5.7 The CA maintains controls to provide reasonable assurance that the CA operates and maintains its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions. 5.9 The CA maintains controls to provide reasonable assurance that OCSP responses conform to RFC6960 and/or RFC5019, and are signed either: • by the CA that issued the Certificates whose revocation status is being checked, or • by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked (the OCSP signing Certificate must contain an extension of type id-pkix-ocsp-nocheck, as defined by RFC6960). 5.10 The CA maintains controls to provide reasonable assurance that OCSP responses by CA's which have not been technically constrained in accordance with SSL Baseline Requirements Section 7.1.5 do not respond with a "good" status for Certificates that have not been issued.	

Opinion

In our opinion, through the period of June 12th 2018 to September 10th 2018, CERTISIGN - CA management's assertion, as referred to above, is fairly stated, in all material respects, in accordance with WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3.

This report does not include any representation as to the quality of CERTISIGN - CA's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3 criteria nor the suitability of any of CERTISIGN - CA's services for any customer's intended purpose.

Use of the WebTrust seal

CERTISIGN - CA's use of the WebTrust for Certification Authorities – SSL Baseline with Network Security Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

FRANCESCO GIGLIO BOTTINO:83217258720

Digitally signed by FRANCESCO GIGLIO BOTTINO:83217258720
DN: cn=FRANCESCO GIGLIO BOTTINO:83217258720, c=BR, o=ICP-Brasil, ou=Autenticado por AR Vanguarda, email=francesco.bottino@br.ey.com
Date: 2018.12.20 10:52:05 -02'00'

Ernst & Young Auditores Independentes S.S.
Rio de Janeiro, Brazil.
December, 2018

Certisign Certificadora Digital - Certisign Trust Network (Certisign – CA) Management's Assertion

Certisign Certificadora Digital – Certisign Trust Network (CERTISIGN – CA) operates Certification Authority (CA) services for the CAs presented in the appendix A, in scope for SSL Baseline Requirements and Network Security and provides the SSL CA services.

Certisign Certificadora Digital - Certisign Trust Network (CERTISIGN-CA) has assessed its disclosures of its certificates and controls over its CA services. During our assessment, we noted the following observations that caused the relevant criteria to not be met:

Observation	Relevant Webtrust Criteria
The Certification Authority (CA) discloses on the respective Certification Practice Statement (CPS), Certificate Policy (CP) and certificates, that it operates OCSP (Online Certificate Status Protocol) responses. However, this service was not fully implemented by the CA prior to August 24, 2018. It is worth mentioning that in this period certificates were issued only internally to CERTISIGN group as part of a "testing" period, with no impact to external customers.	PRINCIPLE 2 - Service integrity: 5.5 The CA maintains controls to provide reasonable assurance that the CA: • makes revocation information available via the cRLDistributionPoints and/or authority Information Access certificate extensions for Subordinate CA and Subscriber Certificates in accordance with the SSL Baseline Requirements Section 7.1.2. • for high-traffic FQDNs, distributes its OCSP responses in accordance with SSL Baseline Requirements. 5.6 The CA maintains controls to provide reasonable assurance that an online 24x7 Repository is provided that application software can use to automatically check the current status of all unexpired Certificates issued by the CA, and: • for the status of Subscriber Certificates: o If the CA publishes a CRL, then the CA shall update and reissue CRLs at least once every seven (7) days, and the value of the next Update field must not be more than ten (10) days beyond the value of the this Update field; and o The CA shall update information provided via an Online Certificate Status Protocol (OCSP) at least every four (4) days and OCSP responses must have a maximum expiration time of ten (10) days. • for the status of subordinate CA Certificates o The CA shall update and reissue CRLs at least (i) once every twelve (12) months and (ii) within 24 hours after revoking a Subordinate CA Certificate, and the value of the next Update field must not be more than twelve months beyond the value of the this Update field; and o The CA shall update information provided via an Online Certificate Status Protocol at least (i) every twelve (12) months and (ii) within 24 hours after revoking a Subordinate CA Certificate. • The CA makes revocation information available through an OCSP capability using the GET method for Certificates issued in accordance with the SSL Baseline Requirements. 5.7 The CA maintains controls to provide reasonable assurance that

Este documento foi assinado digitalmente por Bernardo Stille Neto e Roni De Oliveira Franco.
Para verificar as assinaturas vá ao site https://www.portaldeassinaturas.com.br e utilize o código C8DA-6CB5-4F5B-857B.

	the CA operates and maintains its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions. 5.9 The CA maintains controls to provide reasonable assurance that OCSP responses conform to RFC6960 and/or RFC5019, and are signed either: • by the CA that issued the Certificates whose revocation status is being checked, or • by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked (the OCSP signing Certificate must contain an extension of type id-pkix-ocsp-nocheck, as defined by RFC6960). 5.10 The CA maintains controls to provide reasonable assurance that OCSP responses by CA's which have not been technically constrained in accordance with SSL Baseline Requirements Section 7.1.5 do not respond with a "good" status for Certificates that have not been issued.

CERTISIGN – CA management has assessed its disclosures of its certificate practices and controls over its SSL CA services. Based on the assessment, in providing its Certification Authority (CA) services in Brazil, throughout the period of June 12th 2018 to September 10th 2018, CERTISIGN - CA has:

- Disclosed its SSL certificate lifecycle management business practices in its:
  - Certification Practice Statement
    including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirement on the CERTISIGN - CA website, and provided such services in accordance with its disclosed practices

- Maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and SSL certificates it manages is established and protected throughout their lifecycles; and
  - SSL subscriber information is properly authenticated (for the registration activities performed by CERTISIGN – CA)

- Maintained effective controls to provide reasonable assurance that:
  - Logical and physical access to CA systems and data was restricted to authorized individuals;
  - The continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity

- Maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum based on the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3.

December, 2018
CERTISIGN CERTIFICADORA DIGITAL – Certisign Trust Network – Certificate Authority

Este documento foi assinado digitalmente por Bernardo Stille Neto e Roni De Oliveira Franco.
Para verificar as assinaturas vá ao site https://www.portaldeassinaturas.com.br e utilize o código C8DA-6CB5-4F5B-857B.

APPENDIX A

CA	CA Name	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	Hash SHA-2 Fingerprint
CERTISIGN ROOT CERTIFICATION AUTHORITY	CN = CERTISIGN ROOT CERTIFICATION AUTHORITY O = Certisign Certificadora Digital S.A. C = BR	613870caa793a166	sha512RSA	RSA (2048 Bits)	sha512	quarta-feira, 20 de dezembro de 2017 00:00:00	sábado, 20 de dezembro de 2042 00:00:00	5a11e3f7dfe9a92acc06041cb7375de4eb7f46d2	2811da9d4d306533d545a97cf61e1c1fecf1c8ac
CERTISIGN SSL CERTIFICATION AUTHORITY	CN = CERTISIGN SSL CERTIFICATION AUTHORITY O = Certisign Certificadora Digital S.A. C = BR	538d9b16e3d37d27	sha512RSA	RSA (4096 Bits)	sha512	quarta-feira, 20 de dezembro de 2017 00:00:00	segunda-feira, 20 de dezembro de 2027 00:00:00	3d65d2835103ad9bf7cb4a8c921c1ec7700932e5	72332bc31ca785ddb481216c083f80cb11942d1b
CERTISIGN SSL EV CERTIFICATION AUTHORITY	CN = CERTISIGN SSL EV CERTIFICATION AUTHORITY OU = http://www.certisign.com.br O = Certisign Certificadora Digital S.A. C = BR	22e793acd65dea16	sha512RSA	RSA (4096 Bits)	sha512	quarta-feira, 20 de dezembro de 2017 00:00:00	segunda-feira, 20 de dezembro de 2027 00:00:00	0003ff05acb4f2b0d790cd9adf2303324602ee72	96325a43e6dfff9fe29817ef677e779caef920a9
CERTISIGN CERTIFICATION AUTHORITY	CN = CERTISIGN CERTIFICATION AUTHORITY O = Certisign Certificadora Digital S.A. C = BR	1678f406eb41ad12	sha512RSA	RSA (4096 Bits)	sha512	quarta-feira, 13 de junho de 2018 01:00:00	terça-feira, 13 de junho de 2028 01:00:00	4d411a4b8d989e9546f900072a97ae4eb57f4dea	6204fbadd0292205f139d4a9c34c80fe589a33e9

Este documento foi assinado digitalmente por Bernardo Stille Neto e Roni De Oliveira Franco.
Para verificar as assinaturas vá ao site https://www.portaldeassinaturas.com.br e utilize o código C8DA-6CB5-4F5B-857B.

PROTOCOLO DE ASSINATURA(S)

O documento acima foi proposto para assinatura digital na plataforma Portal de Assinaturas Certisign. Para verificar as assinaturas clique no link: https://www.portaldeassinaturas.com.br/Verificar/C8DA-6CB5-4F5B-857B ou vá até o site https://www.portaldeassinaturas.com.br e utilize o código abaixo para verificar se este documento é válido.

Código para verificação: C8DA-6CB5-4F5B-857B

Hash do Documento

A19ABFFA3E893337E70AABE3A9261BFACFBDBE275492B8C2ED0F83FA80D115AE

O(s) nome(s) indicado(s) para assinatura, bem como seu(s) status em 19/12/2018 é(são) :

- Bernardo Stille Neto (Signatário) - 627.794.517-34 em 19/12/2018 16:33 UTC-02:00
  Tipo: Certificado Digital
- Roni De Oliveira Franco (Signatário) - 031.796.478-09 em 19/12/2018 18:28 UTC-02:00
  Tipo: Certificado Digital