

Independent Assurance Report

To the Management of CERTISIGN CERTIFICADORA DIGITAL – Certificate Authority:

Scope

We have been engaged, in a reasonable assurance engagement, to report on Certisign Certificadora Digital (CERTISIGN-CA) management's [assertion](#), that for its Certification Authority (CA) services in Brazil for AC Certisign and the subordinated CAs presented in the appendix A, during the period July 1st 2017 through June 30th 2018, CERTISIGN - CA has:

- Disclosed its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices in its Certification Practices Statement (CPS) and Certificate Policy (CP) documents:
 - For activity July 1, 2017 – September 7, 2017, the Symantec Trust Network (STN) - Certificate Policy - Version 2.8.23, located at <https://www.symantec.com/about/profile/policies/repository.jsp> and provided such services in accordance with its disclosed practices;
 - For activity September 8, 2017 – June 30, 2018, the Symantec Trust Network (STN) - Certificate Policy - Version 2.8.24, located at <https://www.symantec.com/about/profile/policies/repository.jsp> and provided such services in accordance with its disclosed practices;
 - For activity July 1, 2017 – October 9, 2017, the Certisign - Certification Practices Statement - Version 3.2, located at <http://vtn.certisign.com.br/repositorio> and provided such services in accordance with its disclosed practices.
 - For activity October 10, 2017 – June 30, 2018, the Certisign - Certification Practices Statement - Version 3.3, located at <http://vtn.certisign.com.br/repositorio> and provided such services in accordance with its disclosed practices.
- Maintained effective controls to provide reasonable assurance that:
 - CERTISIGN - CA's Certification Practice Statement is consistent with its Certificate Policy
 - CERTISIGN - CA provides its services in accordance with its Certificate Policy and Certification Practice Statement
- Maintained effective controls to provide reasonable assurance that:
 - The integrity of keys and certificates it manages is established and protected throughout their life cycles;
 - The integrity of subscriber keys and certificates it manages is established and protected throughout their life cycles;
 - The Subscriber information is properly authenticated (for the registration activities performed by CERTISIGN - CA); and
 - Subordinate CA certificate requests are accurate, authenticated, and approved
- 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 was maintained; and
- CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity.

in accordance with the [Webtrust Services Principles and Criteria for Certification Authorities, Version 2.1.](#)

Certification authority's responsibilities

CERTISIGN - CA's management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the [Webtrust Services Principles and Criteria for Certification Authorities, Version 2.1.](#)

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 responsibilities

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 key and certificate life cycle management business practices and its controls over key and certificate integrity, over the authenticity and privacy of subscriber and relying party information, over the continuity of key and certificate life cycle management operations, and over development, maintenance, and operation of systems integrity;
2. selectively testing transactions executed in accordance with disclosed key and certificate life cycle management business 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 our examination provides a reasonable basis for our opinion.

CERTISIGN - CA's makes use of external registration authorities for specific subscriber registration activities as disclosed in CERTISIGN - CA's business practices. Our examination did not extend to the controls exercised by the external registration authorities.

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.

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.

Opinion

In our opinion, through the period July 1st 2017 to June 30th 2018, CERTISIGN - CA management's assertion, as referred to above, is fairly stated, in all material respects, in accordance with [Webtrust Services Principles and Criteria for Certification Authorities, Version 2.1](#).

This report does not include any representation as to the quality of CERTISIGN - CA's services beyond those covered by the [Webtrust Services Principles and Criteria for Certification Authorities, Version 2.1](#) 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 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
DN: cn=FRANCESCO GIGLIO
BOTTINO:83217258720, c=BR, ou=CP-
Brasil, ou=Autenticado por AR Vanguarda,
email=francesco.bottino@br.ey.com
Date: 2019.03.21 15:30:52 -0300

March 21, 2019
Ernst & Young Auditores Independentes S.S.
Francesco Bottino
Partner

APPENDIX A

CA	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	Hash SHA-2 Fingerprint
CertiSign Autoridade Certificadora Classe 2 - G3	CN = Certisign Class 2 CA - G3 OU = Symantec Trust Network O = Certisign Certificadora Digital S.A. C = BR	5352527d85870697b6462627afa184bd	sha256RSA	(2048 Bits)	sha256	segunda-feira, 21 de setembro de 2015 21:00:00	segunda-feira, 21 de setembro de 2020 20:59:59	b1309b40941ac87935a43b13664702e420d05296	bea5661071dac98c61be6870b2a70a7a95b45d1623ee38025149967bffb6d8f9
Certisign Class 1 Consumer Individual Subscriber CA - G2	CN = VeriSign Class 1 Public Primary Certification Authority - G3 OU = (c) 1999 VeriSign, Inc. - For authorized use only OU = VeriSign Trust Network O = VeriSign, Inc. = US	635e079cacad196323ecc0f0caaf9a79b	sha256RSA	(2048 Bits)	sha256	terça-feira, 26 de outubro de 2010 21:00:00	segunda-feira, 26 de outubro de 2020 20:59:59	a2043150a66d8954c3ca0d8d40ae4d8474f72ece	71288cdc38f662246942beb3219ac6d0f04e93b7e35f935ce9e9ce71b83ed407
Certisign Class 2 Managed PKI Individual Subscriber CA - G2	CN = VeriSign Class 2 Public Primary Certification Authority - G3 OU = (c) 1999 VeriSign, Inc. - For authorized use only OU = VeriSign Trust Network O = VeriSign, Inc. C = US	2c8ceec51a1764dfd8544bb8a5ace5007	sha256RSA	(2048 Bits)	sha256	quarta-feira, 20 de outubro de 2010 21:00:00	terça-feira, 20 de outubro de 2020 20:59:59	f5391ca688480bd7535718287b6aff2adfc44e69	6282aaf5fedeb9da88e18b6901c4044c65d4b761428ea1283a4e7a12b12f69b4

Certisign Certificadora Digital (Certisign – CA) Management Assertion

Certisign Certificadora Digital (CERTISIGN – CA) operates Certification Authority (CA) services for AC Certisign and the subordinated CAs presented in the appendix A, and provides the following CA services:

- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution (using an online repository)
- Certificate revocation
- Certificate status information processing (using an online repository)
- Subscriber key management

The management of CERTISIGN - CA is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure, CA business practices management, CA environmental controls, CA key lifecycle management controls, subscriber key lifecycle management controls, certificate lifecycle management controls, and subordinate CA certificate lifecycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, even effective controls can only provide reasonable assurance with respect to CERTISIGN - CA's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

CERTISIGN – CA management has assessed its disclosures of its certificate practices and controls over its CA services. Based on the assessment, CERTISIGN – CA's management opinion, in providing its Certification Authority (CA) services in Brazil, through the period July 1st 2017 to June 30th, 2018, CERTISIGN - CA has:

- Disclosed its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices in its Certification Practices Statement (CPS) and Certificate Policy (CP) documents:
 - For activity July 1, 2017 – September 7, 2017, the Symantec Trust Network (STN) - Certificate Policy - Version 2.8.23, located at <https://www.symantec.com/about/profile/policies/repository.jsp> and provided such services in accordance with its disclosed practices;
 - For activity September 8, 2017 – June 30, 2018, the Symantec Trust Network (STN) - Certificate Policy - Version 2.8.24, located at <https://www.symantec.com/about/profile/policies/repository.jsp> and provided such services in accordance with its disclosed practices;
 - For activity July 1, 2017 – October 9, 2017, the Certisign - Certification Practices Statement - Version 3.2, located at <http://vtn.certisign.com.br/repositorio> and provided such services in accordance with its disclosed practices.
 - For activity October 10, 2017 – June 30, 2018, the Certisign - Certification Practices Statement - Version 3.3, located at <http://vtn.certisign.com.br/repositorio> and provided such services in accordance with its disclosed practices.

- Maintained effective controls to provide reasonable assurance that:
 - CERTISIGN - CA's Certification Practice Statement is consistent with its Certificate Policy
 - CERTISIGN - CA provides its services in accordance with its Certificate Policy and Certification Practice Statement
- Maintained effective controls to provide reasonable assurance that:
 - The integrity of keys and certificates it manages is established and protected throughout their life cycles;
 - The integrity of subscriber keys and certificates it manages is established and protected throughout their life cycles;
 - The Subscriber information is properly authenticated (for the registration activities performed by CERTISIGN - CA); and
 - Subordinate CA certificate requests are accurate, authenticated, and approved
- 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 was maintained; and
 - CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity.

In accordance with the [Webtrust Services Principles and Criteria for Certification Authorities, Version 2.1](#), including the following:

CA Business Practices Disclosure

Certification Practice Statement
Certificate Policy Management

CA Business Practices Management

Certificate Policy Management
Certification Practice Statement Management
CP and CPS Consistency

CA Environmental Controls

Security Management
Asset Classification and Management
Personnel Security
Physical and Environmental Security
Operations Management
System Access Management
Systems Development and Maintenance
Business Continuity Management
Monitoring and Compliance
Audit Logging

CA Key Lifecycle Management Controls

- CA Key Generation
- CA Key Storage, Backup, and Recovery
- CA Public Key Distribution
- CA Key Usage
- CA Key Life Cycle Management Controls
- CA Key Archival and Destruction
- CA Key Compromise
- CA Cryptographic Hardware Life Cycle Management
- CA-Key Escrow

Certificate Life Cycle Management Controls

- Subscriber Registration
- Certificate Renewal
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation

March 21, 2019

CERTISIGN CERTIFICADORA DIGITAL – Certificate Authority

Roni Franco

Bernardo Stille

APPENDIX A

CA	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	Hash SHA-2 Fingerprint
CertiSign Autoridade Certificadora Classe 2 - G3	CN = Certisign Class 2 CA - G3 OU = Symantec Trust Network O = Certisign Certificadora Digital S.A. C = BR	5352527d85870697b6462627afa184bd	sha256RSA	(2048 Bits)	sha256	segunda-feira, 21 de setembro de 2015 21:00:00	segunda-feira, 21 de setembro de 2020 20:59:59	b1309b40941ac87935a43b13664702e420d05296	bea5661071dac98c61be6870b2a70a7a95b45d1623ee38025149967bffb6d8f9
Certisign Class 1 Consumer Individual Subscriber CA - G2	CN = VeriSign Class 1 Public Primary Certification Authority - G3 OU = (c) 1999 VeriSign, Inc. - For authorized use only OU = VeriSign Trust Network O = VeriSign, Inc. = US	635e079cadd196323ecc0f0caaf9a79b	sha256RSA	(2048 Bits)	sha256	terça-feira, 26 de outubro de 2010 21:00:00	segunda-feira, 26 de outubro de 2020 20:59:59	a2043150a66d8954c3ca0d8d40ae4d8474f72ecec	71288cdc38f662246942beb3219ac6d0f04e93b7e35f935ce9e9ce71b83ed407
Certisign Class 2 Managed PKI Individual Subscriber CA - G2	CN = VeriSign Class 2 Public Primary Certification Authority - G3 OU = (c) 1999 VeriSign, Inc. - For authorized use only OU = VeriSign Trust Network O = VeriSign, Inc. C = US	2c8cec51a1764dfd8544bb8a5ace5007	sha256RSA	(2048 Bits)	sha256	quarta-feira, 20 de outubro de 2010 21:00:00	terça-feira, 20 de outubro de 2020 20:59:59	f5391ca688480bd7535718287b6aff2adfc44e69	6282aaf5fedeb9da88e18b6901c4044c65d4b761428ea1283a4e7a12b12f69b4

Este documento foi assinado digitalmente por Roni De Oliveira Franco e Bernardo Stille Neto. Para verificar as assinaturas vá ao site <https://www.portaldeassinaturas.com.br:443> e utilize o código 5EF1-EC6A-2F97-2564.

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/5EF1-EC6A-2F97-2564> ou vá até o site <https://www.portaldeassinaturas.com.br:443> e utilize o código abaixo para verificar se este documento é válido.

Código para verificação: 5EF1-EC6A-2F97-2564



Hash do Documento

050EE679F38183BDE310BE96A23175D0E378A6158345BB73973DCCFB5617B5B3

O(s) nome(s) indicado(s) para assinatura, bem como seu(s) status em 21/03/2019 é(são) :

- Roni De Oliveira Franco (Signatário) - 031.796.478-09 em
21/03/2019 14:02 UTC-03:00
Tipo: Certificado Digital
- Bernardo Stille Neto (Signatário) - 627.794.517-34 em 21/03/2019
16:04 UTC-03:00
Tipo: Certificado Digital

