PRESIDENCY OF THE COUNCIL OF MINISTERS
NATIONAL SECURITY AUTHORITY

Compliance Declaration 05/2016

WE HEREBY DECLARE THAT THE COMPANY:

MULTICERT, Serviços de Certificação Electrónica, S.A.

FOR THE FOLLWING CERTIFICATION AUTHORITY SERVICES:

- Issuing and management of Qualified Digital Certificates
- Timestamping Authority

IS IN COMPLIANCE, RESPECTIVELY, WITH THE TECHNICAL SPECIFICATIONS:

- ETSI TS 101 456 V 1.4.3 (2007-05)
- ETSI TS 102 023 v 1.2.2 (2008-10)

AUDIT REPORT:

- Delivered to the National Accreditation Authority GNS (Autoridade Nacional de Segurança) March 31th 2015, and valid for 12 months.

The National Accreditation Authority endorses this compliance declaration actung as the Portuguese Supervisory and Accreditation Body for all Electronic Signature and PKI subjects.

Lisboa, 20 de Maio de 2015

A Autoridade Nacional de Segurança

José
Deolindo
Torres Sobral

Assinado de forma digital por José Deolindo Torres Sobral
DN: c=PT, o=Gabinete Nacional de Segurança, ou=Gabinete Nacional de Segurança, cn=José Deolindo Torres Sobral
Dados: 2016.05.25 12:38:44 +01'00'

(José Torres Sobral)

PRESIDENCY OF THE COUNCIL OF MINISTERS
NATIONAL SECURITY AUTHORITY

Compliance Declaration 05/2015

Audit requirements and results

I. Audit Requirements for Issuance of Qualified Digital Certificates.

The audit requirements are defined in the technical specification ETSI TS 101 456 V1.4.3 (2007-05): "Electronic Signatures and Infrastructures (ESI); Policy Requirements for certification authorities issuing qualified certificates", Version 2.4.1, 2013-02, European Telecommunications Standards Institute.

The applicable ETSI certification policy is: **QC+SSCD**

The audit object is the following MULTICERT´s Certification Authority services:

- **Issuing and management of Qualified Certificates**

Audit result:

- The audit object fulfils the applicable requirements from the audit criteria.
- All requirements for a CA Practice according to chapter 7 of the rules and standards together with the therein demanded measures are implemented in terms of the selected Certificate Policy (QC+SSCD).
- The audited CA also takes the responsability for the norm requirements fulfilment
- The CA provides the certification services according to the definitions of the Certificate Practice Statement.

Summary of the audit requirements for ETSI TS 101 456

The ETSI TS 101 456 specification contains the following requirements:

1 Certification Practice Statement (CPS)

The CA has a presentation of its practices and policies.

2 Public Key Infrastructure – Key Management life cycle

- The CA ensures that CA keys are created under controlled conditions.
- The CA ensures that private CA Keys are treated confidentially and that their integrity is maintained.
- The CA ensures that the integrity and authenticity of the (published) CA public keys together with all associated parameters are preserved.
- The CA doesn't not generate nor store private signature keys of the certification owner (subject).

3 Public Key Infrastructure – certificate management life cycle

- The CA ensures that the subjects are properly identified and authenticated, and that the subject certificate requests are complete, accurate and duly authorized.
- The CA ensures that requests for certificate issued to a subject who already previously been are complete, accurate and duly authorized.
- The CA ensures that it issues certificates securely to maintain their authenticity.
- The CA ensures that the terms and conditions are made available to subscribers and relying parties.
- The CA ensures that certificates are made available as necessary to subscribers, subjects and relying parties.
- The CA ensures that certificates are revoked in a timely manner based on authorized and validated certificate revocation requests.
- The CA ensures that all subjects are informed for all change of status of their certificates.
- The CA ensures the CRL issuance as least daily.

4 CA Management and Operation

- The CA ensures that the applied administrative and management methods are appropriate and correspond to acknowledged standards.
- The CA ensures that the objects and information worthy of protection receive an appropriate protection.
- The CA ensures that the employees and the hiring procedures amplify and support the CA company´s trustability.
- The CA ensures that physical access to critical services is controlled and that the physical risks for the objects worthy of protection are minimized.
- The CA ensures that the CA systems are operated safely, according to specification.
- The CA ensures that the access to the CA systems is restricted to appropriate, authorized persons.
- The CA is to use trustworthy systems and products that are protected against modifications.
- The CA ensures that in case of a catastrophe the operation is restored as soon as possible.
- The CA ensures that in case of a cessation of the CA operation the potential interference of users (subscriber) and relying parties is minimized and that the continued maintenance of records that are required as proof of certification in legal proceedings is given.
- The CA ensures that statutory requirements are met.
- The CA ensures that all relevant information of a certificate is recorded for a reasonable period of time, especially for the purpose of proof of certification in legal proceedings.

5. Organization

The CA ensures that its organization is reliable.

6. Additional requirements

The CA allows third parties to check and test their certificates.

II. Audit Requirements for Time-Stamping Authorities.

The audit requirements are defined in the technical specification ETSI TS 102 123 V1.2.2 (2008-10): "Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities", Version 1.2.2, 2008-10, European Telecommunications Standards Institute.

The audit object is MULTICERT´s Time-Stamping Authority.

Audit result:

- The audit object fulfils the applicable requirements from the audit criteria.
- All requirements for a TSA Practice according to chapter 7 of the rules and standards together with the therein demanded measures are implemented.
- The audited Authority also takes the responsability for the norm requirements fulfilment
- The Time-Stamping Authority provides services according to the definitions of its Certificate Practice Statement.

Summary of the audit requirements for ETSI TS 102 123

The ETSI TS 102 123 specification contains the following requirements:

1 Practice and Disclosure Statements

The CA has a presentation of its practices and policies.

2 Key Management life cycle

- The TSA ensures that CA keys are created under controlled conditions.
- The TSA ensures that private CA Keys are treated confidentially and that their integrity is maintained.
- The TSA ensures that the integrity and authenticity of the TSU signature verification (public) keys and any associated parameters are maintained during its distribution to relying parties.
- The life-time of TSU's certificate is not longer than the period of time that the chosen algorithm and key length is recognized as being fit for purpose.
- The TSA ensures the security of cryptographic hardware throughout its lifecycle.

3 Time-stamping

- The TSA ensures that time-stamp tokens are issued securely and include the correct time.
- The TSA ensures that its clock is synchronized with UTC within the declared accuracy.

4 TSA Management and Operation

- The TSA ensures that administrative and management procedures are applied which are adequate and correspond to recognized best practice.
- The TSA ensures that its information and other assets receive an appropriate level of protection.
- The TSA ensures that personnel and hiring practices enhance and support the trustworthiness of the TSA's operations.
- The TSA ensures that physical access to critical services is controlled and physical risks to its assets minimized.
- The TSA ensures that the TSA system components are secure and correctly operated, with minimal risk of failure.
- The TSA ensures that TSA system access is limited to properly authorized individuals.
- The TSA uses a trustworthy system that are protected against modification.
- The TSA ensures, in the case of events which affect the security of the TSA's services, including compromise of TSU's private signing keys or detected loss of calibration, that relevant information is made available to subscribers and relying parties.
- The TSA ensures that potential disruptions to subscribers and relying parties are minimized as a result of the cessation of the TSA's time-stamping services, and in particular ensures continued maintenance of information required to verify the correctness of time-stamp tokens.
- The TSA ensures compliance with legal requirements.
- The TSA shall ensure that all relevant information concerning the operation of time-stamping services is recorded for a defined period of time, in particular for the purpose of providing evidence for the purposes of legal proceedings.

5. Organization

The TSA ensures that its organization is reliable.