SEGURTI *Consultoria e Auditoria Lda*

AUDIT REPORT 01/2019

Date of Issue: 07.10.2019

Version: 1.0

1. AUDIT FRAMEWORK

The audit 04/2019 covers the annual follow-up of the certified digital trust services of the SISP identified in paragraph 2 of this document.

The audit related with the present report was performed on July 8 - 10, 2019 and aimed at verifying the continued compliance of SISP operational practices during the period under review.

This period runs from the date of accreditation of the SISP for the trust services to be audited (November 16, 2018) up to the start-up date of the follow-up audit (July 8, 2019).

As a corollary to this audit, the SISP intends to demonstrate that it is in a position to continue to deserve, on the part of the supervisory body, the maintenance of its electronic certificate management activities associated with the trust services accredited by ARME to applicant holders in the Cabo Verdean territory.

2. TRUST SERVICES CONFORMITY ASSESSMENT REPORT

The present report has been prepared to comply with the requirements set forth in Article 35, paragraph 2 of the Regulatory Decree No. 18/2007, dated December 24, 2007, thus providing the evidence, findings, and declaration of conformity of SISP practices with the applicable legal and regulatory requirements.

The trust services included in the scope of this audit are:

TRUST SERVICE(s)	AEQ - Qualified electronic signature SEQ - Qualified electronic seal CAA - Advanced Signature Certificates and Authentication

3. IDENTIFICATION OF THE ORGANIZATION SUBJECT TO AUDIT

LEGAL NAME	Sociedade Interbancária e Sistemas de Pagamentos S.A.
ADDRESS	Achada Santo António C. P. 861 Praia Cabo Verde
ORGANIZATION REPRESENTATIVES	Top Management - Jair Silva Audit Coordinator – Alita Dias

4. IDENTIFICATION OF THE AUDIT TEAM

NAME	ROLE	ANAC/ARME Accreditation
Paulo Jorge Martins Borges	Lead Auditor	ANAC/ICP-CV/AUD02

5. IDENTIFICATION OF THE AUDITED TEAM

NAME	AUDITING TASK	PKI Working Team
Alita Dias	Head of Internal Audit (Coordinator)	Audit
Aurisa Barros	Internal Audit	Audit
João Cruz	Technical Coordinator	Security
Éder Monteiro	System Engineering	Systems
Gaudêncio Fernandes	System Engineering	Security and Management
Jair Silva	Top Management	Management
Leni Varela	Registration and validation of certificate applications	Registration
Jair Gonçalves	Certificate validation and issue	Registration and Management

6. LOCATIONS WHERE TRUST SERVICES OPERATIONS TAKE PLACE

SERVICE	LOCATION	ADDRESS
Registration and Validation ***(see Note 1)***	SISP	Achada Santo António C. P. 861 Praia - Cabo Verde
Backoffice	SISP	Achada Santo António C. P. 861 Praia - Cabo Verde
Issuance of Certificates	SISP	Achada Santo António C. P. 861 Praia - Cabo Verde
Dissemination of Certificates	SISP	Achada Santo António C. P. 861 Praia - Cabo Verde
Certificate Revocation Management	SISP	Achada Santo António C. P. 861 Praia - Cabo Verde
Revocation Status (OCSP and CRL)	SISP	Achada Santo António C. P. 861 Praia - Cabo Verde Achada Grande Praia - Cabo Verde

Note 1:

During the audit, the practice of registering and validating documents on the premises by a SISP customer was highlighted, but this situation was not identified as an external registration entity.

For that reason, ***these activities were not audited.***

It should be pointed out that if such situation persists, this registration body will have to be included in the scope of the next audit.

7. AUDIT PLAN and AUDIT DATES

The audit plan previously defined for this audit was jointly validated by the audit team and the audited team at the kickoff meeting held on July 8, 2019.

The audit work was carried out at the sites identified above, from 8 to 10 July 2019.

The audit scope is defined as including the trust services described in chapter 2 of the present report.

8. LEGAL FRAMEWORK OF THE AUDIT

This audit was conducted on the basis of the following official regulatory framework in force in Cabo Verde:

- Regulatory Decree 18/2007, of December 24, 2007
- Decree-Law 33/2007, of September 24, 2007
- Notice No. 001/CA/2008, of February 20, 2008
- Decree-Law 44/2009, of November 9, 2009

Relevant Note:

Particular attention should be drawn to the fact that the regulatory framework of the ETSI and CWA - CEN Workshop Agreement defined by Notice No. 001/CA/2008 is obsolete, having been replaced by standards which in turn are also for the most part already obsolete.

Thus, the implementation of the PKI was ensured by the audited entity with an approach supported by the latest standards and security requirements, which are included in the new European regulation eIDAS - ***e****lectronic* ***ID****entification,* ***A****uthentication and trust* ***S****ervices.*

Since the definition given in this notice indicates that its content should be complied with at least on the basis of the list of standards contained therein, and considering that the most recent standards meet these requirements, the auditor has allowed the audit to be carried out on this assumption, requiring appropriate checks in each case.

The standards considered as the reference for this audit are, in their latest version, those indicated in Chapter 10 d) of this report.

9. CHARACTERIZATION OF THE TRUST SERVICES

a. Description of the trust services

The Sociedade Interbancária e Sistemas de Pagamentos S.A., hereinafter referred to as **SISP**, aims to be a Trust Service Provider pursuant to paragraph 38 of the Regulatory-Decree no. 18/2007.

SISP intends to provide titleholders with the trusted services described in Chapter 1 of this report.

This Trust Service issues advanced and qualified certificates in which the electronic signature creation data and the validation data are located in a qualified signature/seal creation device (QSCD) in smartcard.

b. Identification of the trust services

SISP ROOT

Following accreditation of the SISP PKI by ARME in November 2018, a new certificate of signature of the SISP ROOT was generated:

FIELD	DESCRIPTION
Service type identifier	***To be identified by ARME***
Service name	N/A

DN	C=CV
	O=ICP-CV
	OU= ANAC-Agencia Nacional das Comunicacoes
	CN= Root Certification Entity of SISP 01

Certificate (base 64)	-----BEGIN CERTIFICATE----- MIIGnTCCBIWgAwIBAgIIJeaCO3vuWlgwDQYJKoZIhvcNAQELBQAwgYkxCzAJBgNV BAYTAkNWMQ8wDQYDVQQKDAZJQ1AtQ1YxLzAtBgNVBAsMJkFOQUMtQWdlbmNpYSBO YWNpb25hbCBkYXMgQ29tdW5pY2Fjb2VzMTgwNgYDVQQDDC9FbnRpZGFkZSBkZSBD ZXJ0aWZpY2FjYW8gUmFpeiBkZSBDYWJvIFZlcmRlIDAwMTAeFw0xODEyMTgwODM0 NTVaFw0zMDEyMTUwODM0NTVaMIGRMQswCQYDVQQGEwJDVjEPMA0GA1UECgwGSUNQ LUNWMT4wPAYDVQQLDDVTSVNQLVNvY2llZGFkZSBJbnRlcmJhbmNhcmlhIGUgU2lz dGVtYXMgZGUgUGFnYW1lbnRvczExMC8GA1UEAwwoRW50aWRhZGUgZGUgQ2VydGlm aWNhY2FvIFJhaXogZGEgU0lTUCAwMTCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCC AgoCggIBAORCJwdQMLOB8g1QGVkXZ1POEVKBwCr0GEn7riYgpYUGKnTzxmZZVra1 IcBOn3WtTsV9ItAhVxg0ZoKngYEAxDdipjHvWUUocGDOpatUGdQCT6Nepz4f8fkU LfzM2bmFRDOGJtlSAb8RVwQUMOGX1xGcn5Nu2o1IuJjEH85ANv/erPKcaUrAhwrP qZVltJue8QAM7WDivhszvKcbZwr4HYGV/mc8Q7f5ElwyE4yyJxS2IqdiOPpZcTm7 i1VZQR9iJq3WAp4x0tyUV4SPWz2QGYdqMDCBxpmsargpKmPHUPUAXFZ8fjM9xyTf /nvnzvYtRDVqo4MNINyk++eAFYzgvsuqwBMpu87gRxdmqHdnZ384hvCzEftv4F4m gPlSUj6fWTBfcNDuaetgv6BNnFC0hGXjTuQ+hdou0x7Erl2qAYFeYXjBRv8uEtPz 86002z7R7gPDy3zDc2veUKynJlpLcMI32w7My8XYZsXYBL/XU/DH4TWb3haJw4yy GaFZAfKhrwXbydB4CKoQus0R0MjEC5sXbMmjMcbqr9goFmTek6EIZfJg4B2VZtBK +bsczmYqwLAtvVEWrbM5xiSUtqRkfm0LHPaz4PFyoW8IkaOHttLXjE9rGpPt1JEy Qs71srRYNgYjLRTfuUDguXCvh8I0Y4RNC7DyRltXv0G1h/7VUuupAgMBAAGjgf4w gfswHQYDVR0OBBYEFNOK49Sm8NpIB4VkQ9A1zGyAT/CeMBIGA1UdEwEB/wQIMAYB Af8CAQEwHwYDVR0jBBgwFoAUKxVrrouYAyWCefRhh5hmnrxK3ygwVAYDVR0gBE0w SzBJBgRVHSAAMEEwPwYIKwYBBQUHAgEWM2h0dHA6Ly9wa2kuZWNyY3YuY3YvcHVi L3BvbC9lY19yYWl6X2RwY18wMDFfcHQuaHRtbDA/BgNVHR8EODA2MDSgMqAwhi5o dHRwOi8vcGtpLmVjcmN2LmN2L3B1Yi9jcmwvZWNfcmFpel9jcmwwMDEuY3JsMA4G A1UdDwEB/wQEAwIBBjANBgkqhkiG9w0BAQsFAAOCAgEAFm/P/0xkdyBEH8K9x40T

	b/opnt9tnkmOO5KSbvBUguvKX7rQJTqXEHN8kwAXiN6XEcvgVyVM6F53hFZJS0iS F/zu4xzIQUL5T8nym7JbVSmCWQ5IJG0QHTNOIVR2GQz83nITaI5UfjccinYkuUrS vb9lhjpAo89I8K0D3C3bJAU6NaGiCsowRulu/NsrPMvvC1V6N2AFrgYu1HF8wjUD diTuAQMc7GNNJIh+yzSCelRdP4+mj5HBuYM/XwG2wv+FHmoo9Ha+aRGFxJh3LTtY xpX8Of8jjQmd5laQfw5ZvISzLeVlyBWM9XGhr8H/fEJaTR6NukwoBxkNesTEWVIL KkQUtkKtjvjQvyePa/f+n3OZS4XEcn6HPowqOl0LNsj14HEHcvu3P0GyD4lW/sVA d40D7tYISpYXDhJpgCoiQCO5ZRPL3bHYP7dSfzRV8ftX3igmN4JvCI9jPONWPuzA SA0T3bwL2FTrsbv/xxiFZX4XYi1pdu4TCt3IcKwF3mNDBw2hZjnUI8x0Vg2D+Hf8 U4B4FLEKPA275fqvvXRnD8RDIzTxWuCFFjvvvUOPVnFQlj/5fcEszQZo9PT+cAxa rk81lDfqWmxBA6apv/h5gimLM9+ALgkjzQTv9LIq4r9Y/su43F+G4HsovxeKGpqG BV5z6MmVbupzqTIPoITGMQs= -----END CERTIFICATE-----

SISPCA01

SISPCA01 is the SubCA signed by SISP ROOT, which hosts the trust services within the framework of this audit.

The following information identifies the trust services that have been evaluated:

FIELD	DESCRIPTION
Service type identifier	***To be identified by ARME***
Service name	Qualified electronic signature Qualified electronic seal Advanced signature certificates and authentication

DN	C=CV
	O=ICP-CV
	OU=SISP-Sociedade Interbancaria e Sistemas de Pagamentos
	CN=Root Certification Entity of SISP 01

Certificate (base 64)	-----BEGIN CERTIFICATE----- MIIGozCCBIugAwIBAgIIFgXdtEGM7jYwDQYJKoZIhvcNAQELBQAwgZExCzAJBgNV BAYTAkNWMQ8wDQYDVQQKDAZJQ1AtQ1YxPjA8BgNVBAsMNVNJU1AtU29jaWVkYWRl IEludGVyYmFuY2FyaWEgZSBTaXN0ZW1hcyBkZSBQYWdhbWVudG9zMTEwLwYDVQQD DChFbnRpZGFkZSBkZSBDZXJ0aWZpY2FjYW8gUmFpeiBkYSBTSVNQIDAxMB4XDTE5 MDEwMzE3MjcxM1oXDTI1MDEwMTE3MjcxM1owgYoxKjAoBgNVBAMMIUVudGlkYWRl IENlcnRpZmljYWRvcmEgZGEgU0lTUCAwMTE+MDwGA1UECww1U0lTUC1Tb2NpZWRh ZGUgSW50ZXJiYW5jYXJpYSBlIFNpc3RlbWFzIGRlIFBhZ2FtZW50b3MxDzANBgNV BAoMBklDUC1DVjELMAkGA1UEBhMCQ1YwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAw ggIKAoICAQDm5oSdlwndxTX8XmYzYXr+7HaXvktJG8B40/N4VgNgE/O7a79xD81O ah58gEcJ1BArA41EJvMvQZ4bcgzkTz0Rgu45nEAhZYWl9eYL9JBXrhdxBqrtNQOf AxzJvrcak7vj21GTnJP0qY+E5Ys67amcO3g49AxNKEpSl5wRjwqLMYCnkTPKP6hs

```
MCiiFnIhtx/NU24Ht/cCwzW633+6OYJ09JUhIqfriQR5QIzv21d7vTtnEtMwdAqE
sjihf2bhdoDF6A+cG+ITjJnc/oIWVazMjWvW8qSzIKcrarKJL2y/P2/uLWZHpoDL
q9JSLPWVrhJAWwtsCirMTkglfjP/WsaudnCYaUrVdZTSpDSt9NgTAto7scrwKwRX
qWeVCia2I9qYyECAm9lhl5qx6I8zdYxqj2oMJR+/irpQJEfIY9Phor1WVLmSURo6
rDCvE/ahmKYDV5WBCC5NIGpgICTNWo+XwPwMgAIDCfF1WMRaZK1Lug+82Wx/FTLi
ZLtwCy64fWVRwhVpV501MW8NPOLlIiHrIdAeZK9EFczUqO6fjZuoRmv1pm6dl3Yk
q9aN9Jir8dSTejaiVn95WFBNKjjrbeRa3jFBfKtaRLpmmZVbteRYsNZXpT+mTT0s
kUwC/yxAhOiBYXgIh+aUMyIMfIBzhWBFC7risbb8D8xNZQynNYtV/QIDAQABo4IB
AjCB/zAdBgNVHQ4EFgQU5QQU1lHoDima4m1y61C30GsTl0cwEgYDVR0TAQH/BAgw
BgEB/wIBADAfBgNVHSMEGDAWgBTTiuPUpvDaSAeFZEPQNcxsgE/wnjBlBgNVHSAE
XjBcMCwGB2CBBAEBAgMwITAfBggrBgEFBQcCARYTaHR0cHM6Ly9wa2kuc2lzcC5j
djAsBgdggQQBAgIDMCEwHwYIKwYBBQUHAgEWE2h0dHBzOi8vcGtpLnNpc3AuY3Yw
MgYDVR0fBCswKTAnoCWgI4YhaHR0cDovL2NybC5zaXNwLmN2L3Npc3Byb290Y2Eu
Y3JsMA4GA1UdDwEB/wQEAwIBBjANBgkqhkiG9w0BAQsFAAOCAgEAbLoZp0tLQTnT
/BDB/IYjU6QbZNvE92w1kWvH8p6hRLo8bMBSe2aCY1C18UP9NuMm0XIL+xueXCTk
0h1mtR5J/JV/weP6IsOYJ4kAvIH1XNlzn4TeBMSU1JmGOx/k8GDklvzdisobrpVG
aZDhwKes/0pqcnkzX0qjGoWSAV2oWuEkZ/PSos+RNG55TYW2q7qXh3fR1vLK3JO6
AmVxfXp8zVTVEPOlXxVgnoQJGBAmTEJivcK8xktlfeVzrXD8p1xn8Twns2pr63iD
nXfoeZ55T/TBxj3SQ/TcwHY6HbQ1Li8ZEYqN/ZsoCXyZnN81CHD100rxNMqcdd5i
eSZzVSxqe7CXXfpb6CzwDf6C+qzWGHxcC80g6PfamWwr5fNTP36cX0UKyymiEiz6
itKem8mFTdBSaVqqAuD84uBO3ePRGzyvIh6PgYgzO7/h0TOelQHTJt8N24tU1A49
9ChtxOtAKlfRQ7yVxaCr5fUpsvwvIm6h314Cv8WXgSykl44WMAAli/s9ruZlqkpL
1NTqs1kdCKSL6CpGruKSdwxR9J/0IBUDXizuJ+6y88Yai1h2eehz+57buTqukjU6
skhdHuM0GebxDEBmcpR5AeZKHHYaHrhiiH6ibGkpTiUWsgPCZrcrROBU/TKyhD8b
fhOYuAAACnGQEQ8EjMybiNR717sS2Fo=
-----END CERTIFICATE-----
```

10.AUDIT EVIDENCES

a. Documentation assessed

The following SISP documents have been analyzed:

Base	Version	Activity	Type of process	Process	Area
PLRC001	5.0	Statement as to the Certification Practices of SISP Root Certification Entity	Execution	PR001 Customer Relations	GPS
PLRC002	2.0	Statement as to the Certification Practices of SISPCA01 Subordinate Certification Entities	Execution	PR001 Customer Relations	GPS
PLRC003	5.0	Certification Policy of SISP Root Certification Entity	Execution	PR001 Customer Relations	GPS
PLRC004	2.0	Certification Policy of SISPCA01 Subordinate Certification Entity	Execution	PR001 Customer Relations	GPS
PTOP033	4.0	Operation Manual of the PKI of SISP	Execution	PR002 Operations	GOP
PTOP034	2.0	Manual of Procedures for Life-Cycle Management of Digital Certificates	Execution	PR002 Operations	GOP
PLSI010	3.0	Security Plan of the SISP Certification Entity	Support	PS004 Information Systems	IS
PTSI033	2.0	Manual of Procedures for cryptographic key management in the PKI of SISP	Support	PS004 Information Systems	IS
PTSI034	2.0	Operation of Registration Units of End Users	Support	PS004 Information Systems	IS
PTRC007	1.0	Activity Termination Plan for the PKI of SISP	Execution	PR001 Customer Relations	GPS
PTSI035	2.0	Certificate Profile Management Procedures for the PKI of SISP	Support	PS004 Information Systems	IS
MD004	2.0	List of Employee Working Groups for the PKI of SISP	Support	PS004 Information Systems	IS

Forms					
FRRC001	1.0	Digital Certificate Issuing Contract	Execution	PR001 Customer Relations	GPS
FRRC002	1.0	Service Provision Agreement for the Registration Entity	Execution	PR001 Customer Relations	GOP
FRRC003	1.0	Trust Staff Appointment Sheet for the Registration Entity	Execution	PR002 Operations	GPS
FRRC004	1.0	Application Form for the Issuance of Individual Digital Certificate	Execution	PR001 Customer Relations	GPS
FRRC005	1.0	Application Form for the Issuance of Qualified Digital Certificate intended to represent Legal Entities	Execution	PR001 Customer Relations	GPS
FRRC006	1.0	Application Form for the Issuance of Qualified Digital Certificate – Electronic Seal	Execution	PR001 Customer Relations	GPS
FRRC007	1.0	Application Requesting Revocation of Digital Certificate	Execution	PR001 Customer Relations	GPS
FRRC008	1.0	Application Form for the Registration of Subordinate Certification Entity	Execution	PR001 Customer Relations	GPS
FRRC009	1.0	Application Form for the Revocation of a Subordinate Certification Entity	Execution	PR001 Customer Relations	IS
FRSI001	1.0	Check-list for Security Requirements of Registration Entities	Support	PS004 Information Systems	IS
FRSI002	1.0	PKI Key Ceremony Sheet	Support	PS004 Information Systems	IS
Complementary					
PLSI004	3.0	Change Management Policy	Support	PS004 Information Systems	IS
PLSI003	2.0	Password Policy	Support	PS004 Information Systems	IS
PTSI013	1.0	Incident Management Procedure	Support	PS004 Information Systems	IS

PLSI002	4.0	Access Control Policy	Support	PS004 Information Systems	IS
PLSI009	2.0	Disposal and Destruction Policy	Support	PS004 Information Systems	IS
PLSI006	1.0	Information Classification Policy	Support	PS004 Information Systems	IS
PLSI008	3.0	Data Retention Policy	Support	PS004 Information Systems	IS
PTSI003	3.0	Emergency Response Plan and Incident Handling	Support	PS004 Information Systems	IS
PTSI047	1.0	Business Continuity Plan	Support	PS004 Information Systems	IS
MSI003	6.0	Vulnerability Scan Manual	Support	PS004 Information Systems	IS

A few aspects that support the identification of improvement actions should be considered:

- A number of forms were identified without version indication;
- Completed forms with erasures were identified without being duly justified by a member of the audit working group;
- Cases of use of signatures or initials have been identified without defined rules;
- A case of authorization and validation by the same employee has been detected;
- Cases have been recorded where forms introduce changes (e.g. in the case of ceremonies) which are not being managed by the change management process.

b. Certificates issued by the trust services

The following specimen certificates were issued with the purpose of analyzing the certificate profiles for each trust service:

SERVICE	No. OF CERTIFICATES ISSUED	CERTIFICATE PROFILE
Qualified electronic signature	**19 certificates** including the serial number: • 1102e9c3858e45dd • 12eb67404b0ec94c • 25abf47eb0edf411 • 3522b8708c441fb • 6f3cdba9b04003b0 • 380894ed82aadb98 • f1b025b0d3e8f00 • 52f9de3d9eef0ba0 • 275477b5242dca7f • 36dd5d28b5d56fda • 5908b3580df79b27 • 37d95333a0e3eed5 • bbd509bbe72d87 • 7259452088d17229 • 89d1394cc497efc • 270a6fce95f7999e • a6227e43e921bb3 • 52df72a2f0d28ece • 6cbbc2742e4da96b	PERIL_CERT_AQ_01
Qualified electronic seal	**1 certificate** with the serial number: • 13b804bba71ab7de	PERIL_CERT_SE_01
Advanced authentication signature	**8 certificates** with the serial number: • 4eae4b1f333e5604 • e297ce7ca2e9b69 • 2972d0271a8b84f8 • 1ce8d719a198008a • 2bb2dd29523ce63c • 422d1dfa14846853 • 4af48c67f13ae3ae • e9f91ca7710e8c9	PERIL_CERT_AU_01

A certificate of signature was also issued for the OCSP with the serial number 66643217a4d23275.

Integrity tests were conducted involving the following components:

- Holder validation request portal
- Portal for issuing the certificate application
- EJBCA
- OCSP and CRL

All tests were successfully performed.

However, consideration must be given to the fact that there is no tool enabling the systematization of the collection of these statistics, nor that they are periodically monitored by internal audit.

This situation provides an opportunity for improvement.

c. Working Groups

A few changes in the working groups have been identified, namely:

- Aurisa Barros – Internal Audit
- Adélcio Rosa – Security Administration
- Various Registry Administrators

Records of acceptance, competency check and training are adequate for these changes.

Nevertheless, it should be noted that the current physical conditions for the receipt and validation of holder identification are rather deficient and should therefore consider the use of a secure Video ID solution.

d. Computer Architecture

The PKI system architecture is presented on page 28 of the "SISP PKI Operating Manual".

Following review of the said architecture, the following aspects should be considered:

- A date/version must be added in order to use representation outside the context of the manual;
- Communications systems in use should be represented;
- Redundancy of the SISP Root, which has not yet been made available on the alternative site, should be included.

e. Incident Management

Failure to generate the quarterly CRL of SISP Root was identified in March 2019 without any incidents whatsoever.
This situation gives rise to the identification of a "non-conformity", which in case of recurrence may be rated as high impact.

The following points emerge from the analysis of the incident management documentation:

- Although document PTS013 is called a "procedure" it actually consists of a process;
- It is outdated, for example AOC no longer exists. There are several inconsistencies in external references to other documents;
- There are no "lessons learned", no link to the improvement action plan;
- The differentiation between incident resolution and incident closure is not clearly identified.

This situation provides an opportunity for improvement.

f. Business Continuity Management

In addition to the points that are associated with the analysis of the Non-Compliance identified in the 2018 audit, the following issues must also be considered:

- There is still no operational redundancy of the "root" of the SISP;
- The OCSP and the CRL are published at one IP address only.

  The solution adopted by SISP, which consists of using VMWARE replication for virtual machines in the alternative location that are not "online" allows for the existence of lags that were not considered in risk analysis.
  It is recommended that intensive tests be performed to confirm that the risk of synchronization failure is properly managed, otherwise they should start publishing these services in 2 different IP addresses.
- The document reference list of the Business Continuity Plan does not identify ETSI standards;
- HSM on the alternative site is offline, with manual reset.

  Taking into account that backups are completed every 24 hours, service replacement and integrity tests should be performed at the alternate site/location so as to verify if this solution is suitable for the objectives set by the BCP.

  It is important to note that the objective of using an alternative site/location also includes returning to normal service mode.

g. Reference Standards

In view of the note contained in Chapter 8 of this audit, the following standards (in their latest version) have been considered in this assessment as complementary references for compliance analysis:

Reference	Abbreviated Title
eIDAS Regulations	REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market, and repealing Directive 1999/93/EC.
EN 319 403	Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers
EN 319 411-1	Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements
EN 319 411-2	Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
EN 319 412-1	Certificate Profiles; Part 1: Overview and common data structures
EN 319 412-2	Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons

EN 319 412-3	Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
EN 319 412-4	Certificate Profiles; Part 4: Certificate profile for web site certificates issued to organizations
EN 319 412-5	Certificate Profiles; Part 5: QCStatements

h. Annexes

There are no annexes to be attached to this audit report.

11. ANALYSIS OF THE STATUS OF THE PREVIOUS AUDIT CORRECTIVE ACTION PLAN

Following the audit work to the CAP carried out in August 2018 as regards the audit awarded in March 2018, eight (8) "low impact non-conformities" were detected.

This audit focused its attention on the analysis of the evidence generated by the SISP from the implementation of these corrective actions and its assessment as to compliance with the requirements identified upon detecting such "non-conformities".

This analysis results in the table below:

NON-CONFORMITY ID	DESCRIPTION	STATUS OF IMPLEMENTATION CONFORMITY
NC.BI.1	A Business Continuity Plan is not yet in place that includes the use of an alternative site for processing PKI operations.	The document PTSI047, in its version 1.0, was presented as evidence. ***However, although its structure is fit for the purpose, the content is not suitable for a PKI infrastructure, so the NC remains open.***
NC.BI.2	The alternative site for processing PKI operations is not yet established and operationalized.	The alternative site is in place, but it has not yet been possible to demonstrate its readiness and effectiveness for operation purposes. A test to the use of services at the alternative site should be performed, and the return to normal mode inserted in the Business Continuity Plan as well. ***Accordingly, the NC is considered to be unresolved.***
NC.BI.3	The implementation of the NTP component of the PKI still presents the following failures: • Monitoring of accuracy is not yet complete, from Stratum 2 to Stratum 0; • The alternative site appliance is not yet operational.	NC successfully implemented.
NC.BI.4	Tests for internal and external vulnerabilities of the PKI infrastructure at the main and alternative sites have not yet been conducted. The corresponding service provision contract should be submitted in due course.	Tests were carried out in January 2018 and repeated in April 2019. The issues found in the OCSP and the CRL were resolved, while the Primekey appliance was subject only to tests. Not all components of the PKI architecture were tested. The results of the tests were not analyzed by the internal audit and did not result in improvement actions. Vulnerability resolution deadlines were not met. ***Therefore, the NC maintains a pending status.***
NCBI.5	There is no procedure to manage the stoppage in certificate issuing in case of accuracy failure with the UTC.	NC successfully implemented.
NCBI.6	There is still no adequate procedure for managing the capacity of the infrastructure components of the PKI services.	NC successfully implemented.
NCBI.7	Need to resolve all security controls at the main and alternative sites.	NC successfully implemented.
NCBI.8	The version of the EJBCA in use is 6.14, not currently holding FIPS 140-2 level 3 and CC EAL4+ security certificate.	***The NC was not resolved, thus still remains pending.***

Relevant Note:

A low impact non-conformity kept open following more than 2 audits may result in a high impact non-conformity declaration, depending on the evidence of inability to meet requirements.

12. NON-CONFORMITIES IDENTIFIED IN THE PRESENT AUDIT

Taking into account the compliance analysis carried out, the audit team identifies the following non-conformities, organized according to their impact.

The practical significance of each type of non-conformity is presented below:

> ***High Impact Non-Conformity*** – clear violation of a requirement due to the lack of supporting evidence, incorrect interpretation or gross negligence in implementation.
> This is a decision that prevents the operation of the trusted service(s) in the production environment.
>
> ***Low Impact Non-Conformity*** – violation of a requirement, due to poor supporting evidence, failure of supporting documentation, or incorrect practice caused by documental commitments.
> Separately, it may not prevent the operation of the trusted service(s) in a production environment.
> However, jointly with others of the same type, it may lead to such a decision.

a. High impact

No situations were found that could configure "high impact non-conformities".

b. Low impact

The situations which meet the criteria for defining 'high impact non-conformities' are set out in the table below.

It should be noted that these are "non-conformities" which are carried over from the initial audit of April 2018, and will remain so until SISP generates evidence of their full and effective resolution.

NON-CONFORMITY ID	LEGAL OR REGULATORY REFERENCE	JUSTIFICATION
NC.BI.1 2018	RD 18/2007 Article 33 paragraph 2)	A Business Continuity Plan including the use of an alternative site for processing PKI operations is not yet in place. ***Note**: This is a result of the previous audit.*
NC.BI.2 2018	RD 18/2007 Article 33 paragraph 2)	The alternative site for processing PKI operations is not yet in a demonstrated state of readiness, through tests integrated with the Business Continuity Plan. At this stage it is recommended to consider the use of the "root" redundancy of the SISP. ***Note**: This is a result of the previous audit.*
NC.BI.4 2018	PLRC001 version 3.0 Statement of Practices of the SISP Root Certification Entity ISO 27001 A.12.6	Vulnerability tests were partially and incorrectly conducted, although the methodology adopted (PCI DSS) is adequate. Specifically: • The analysis of results was not carried out in internal audit • No opportunities for improvement have been identified and integrated into the overall PKI improvement plan • The vulnerabilities identified were not addressed in a timely manner and should therefore have been put into the risk analysis • No tests were made to the NTP system • No tests were made to the application portals (WEB and registration entity) • All tests must be carried out on the production platform, though they may be conducted on a test platform prior to this intervention ***Note**: This is a result of the previous audit.*
NCBI.8 2018	ETSI 319 411 6.5.2 Private key protection and cryptographic module engineering controls	The version of the EJBCA in use is 6.14, and it does not currently hold FIPS 140 and EAL4+ security certificates. ***This NC has not yet been resolved and may become critical and be considered as high impact!*** ***Note**: This is a result of the previous audit.*
NCBI.1 2019	ETSI 319 401 7.8 Network Security REQ-7-8-07	There is still no redundancy of the SISP Root on the alternative site for processing PKI operations
NCBI.2 2019	ETSI 319 401 7.8 Network Security REQ-7-8-12	There is still no redundancy of communications and security system at the alternative site for processing PKI operations
NCBI.3 2019	ETSI 319 401 7.9 Incident Management REQ-7-9-12	Failure to issue the quarterly CRL of SISP Root was identified without any incidents.
NCBI.4 2019	RD 18/2007 Article 33 paragraph 2)	The redundancy of the OCSP and the CRL services has not been demonstrated in a prompt and effective way.

NCBI.5 2019		Holder validation tasks are being performed at a SISP customer without being set up as an 'external registration entity', and as such their operators are not identified as registry administrators.

13.OPPORTUNITIES FOR IMPROVEMENT IDENTIFIED IN THIS AUDIT

The table below presents the opportunities for improvement that have been identified and which are not mandatory.

However, it is emphasized that an opportunity for improvement is signaled as a preventive measure of possible non-conformity situations and, as such, its applicability should be assessed.

Important Note:

There was no audit time to review the implementation of improvement opportunities.

It is up to the audited institution to decide on its adoption according to the definition of objective specified above.

ID OF THE IMPROVEMENT ACTION	DETAILED DESCRIPTION	OBJECTIVE
IO.1 2019	Review the vulnerability analysis manual in order to place the execution criteria and the results analysis at the beginning of the document	Highlighting the criteria for the analysis of the risk of vulnerabilities and their integration with risk management
IO.2 2019	Segregate the VLAN "Outside" from the internal zone of the Main Site of the SISP, taking the opportunity to constitute an area of Cyber-security protection according to the standard ISO 27032	Network Security and Cybersecurity Responses
IO.3 2019	Develop a Cybersecurity strategy for the PKI, according to ISO 27032 and the NIST Framework	Cybersecurity Readiness and Compliance
IO.4 2019	Create a tool for the extraction and analysis of certificate issuing statistics, carrying out a periodic and sample analysis of their compliance in internal audit	Internal audit support
IO.5 2019	Review the list of documents to ensure that they all contain the version indication	Minimize operating errors
IO.6 2019	Create/review the change management process, ensuring that all interventions in the PKI are carried out according to its operational and decision-making determinations	Minimize operating errors

IO.7 2019	Ensure that the practice of erasures in formal PKI documents is avoided, and where necessary duly justified by internal audit	Minimize operating errors
IO.8 2019	In relation to incident management, there are several points to consider in this improvement: (a) designate the document by process rather than procedure (b) bring its definition into line with the standard ISO 27035 (c) Add the steps required for incident "resolution" and "closure" d) Add the step on "lessons learned" and the link to the improvement action plan e) Manage the timeframe of the incident	Minimize business continuity losses
IO.9 2019	Create procedures for the safe destruction of tokens	Minimize the abuse of certificate use support
IO.10 2019	Regulating the practices of using the system's formal documents in order to avoid: • The unregulated use of signatures and initials • Authorization and validation by members of different groups • Validation by security audit in all cases • - The use of document numbering	Minimize operating errors and safety failures
IO.11 2019	Consider the possibility of integrating an eIDAS certified "Video ID" solution for the remote validation of the identity of the holders responsible for the certificate request	Effectiveness of the holder validation procedure and minimization of transaction errors

14. AUDIT DECISION

The SISP intends to provide digital trust services as defined by the Regulatory Decree no. 18/2007.

In order to provide the trust services submitted to the audit, it uses a standardized set of functions/processes, such as: the registration and validation of titleholders, the generation of keys and issuance of certificates, management of availability of the status of certificates and the respective revocations.

The trust services are performed by trained and formally authorized employees.

The physical environment in which these services operate is suitable for the regulatory compliance objectives.

The technical environment of the PKI is considered safe as a result of the analysis of audit evidence. However, there are still issues of non-compliance and improvements to be made.

The certificates issued in the period under review showed full compliance with the ETSI standards identified in this report as reference.

Five "low impact non-conformities" were identified, which will also have to be resolved within the time limits defined by ARME, alongside with 4 other "low impact non-conformities" that are carried over from the previous year's audit results.

In addition, 11 improvement actions were identified, which require analysis and consideration by the SISP in what concerns their acceptance and implementation.

The conformity of the audited trust service should be considered, at this point in time, as positive, but conditional.

This compliance assessment shall be reviewed by conducting a new audit to verify the implementation of the corrective actions defined by the SISP and approved by the auditor for the non-conformities indicated.

15. AUDIT CLOSING NOTES

a. DIVERGENCES

In case there are differences of opinion between the SISP and the audit team, for which it was not possible to reach an audit consensus, these are recorded in the present report and referred to ARME for clarification, evaluation and decision.

However, up to the conclusion of this report no differences have been identified between the organization and the audit team.

b. ACKNOWLEDGEMENTS

The audit team is grateful for the pleasant working environment provided, the excellent commitment of its employees and the support provided by SISP, thus ensuring the proper conditions for the success of this audit.

c. CONFIDENTIALITY

SEGURTI and its entire audit team shall ensure the confidentiality of all information to which it had access during the execution of all audit activities.

SEGURTI and its entire audit team reserve the right to make confidential information available to ARME's representatives, when formally requested to do so, for the purposes determined by the certification process and within the scope of its competencies.

d. SUBSEQUENT STEPS

The SISP should send this report to ARME, which will determine the need to present a CAP - Corrective Action Plan and the identification of a maximum execution time depending on the type of Non-Conformities identified.

The Auditor will thus have the opportunity to analyze the CAP submitted by the SISP and agree or not with this proposal, before being considered as good for execution.

The Auditor signs this report of his own free will and conscience.

	NAME	DATE	SIGNATURE
Lead Auditor:	Paulo Borges	07-10-2019	Paulo Jorge Martins Borges Assinado de forma digital por Paulo Jorge Martins Borges Dados: 2020.03.11 19:48:36 Z