AUDIT REPORT 03/2019

Date of Issue: 07.30.2019

Version: 1.0

1. COMPLIANCE ASSESSMENT REPORT OF TRUST SERVICES

The Sociedade Interbancária e Sistemas de Pagamentos S.A., hereinafter referred to as **SISP**, operates as a Trust Services Provider in accordance with No. 38 of the Regulatory Decree 18/2007 on trust services.

This report has been prepared taking into account the provisions set forth in no. 35 of the Regulatory Decree no. 18/2007, dated 24 December 2007, the first audit to be carried out to this organization for the trust service identified below and, as such, represents the primary report on the access to the activity of this service.

TRUST SERVICE(s)	WEB – Qualified Website Authentication Certificates

2. IDENTIFICATION OF THE AUDITED ORGANIZATION

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

3. IDENTIFICATION OF THE AUDIT TEAM

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

4. IDENTIFICATION OF THE AUDITED TEAM

NAME	AUDIT ROLE	PKI Working Group
Alita Dias	Internal audit coordinator	Audit
Aurisa Barros	Internal audit	Audit
João Cruz	Technical Coordinator	Security
Éder Monteiro	Systems Engineering	Systems
Gaudêncio Fernandes	Systems Engineering	Security and Management
Jair Silva	Top management	Management

5. LOCATIONS WHERE TRUST SERVICE OPERATIONS TAKE PLACE

SERVICE	SITE	ADDRESS
Registration and Validation	SISP	Achada Santo António C. P. 861 Praia - Cabo Verde
Backoffice	SISP	Achada Santo António C. P. 861
Certificate Issuance	SISP	Praia - Cabo Verde
Certificate Dissemination	SISP	Achada Santo António C. P. 861
Certificate Revocation Management	SISP	Praia - Cabo Verde
Revocation Status (OCSP and CRL)	SISP	Achada Santo António C. P. 861

6. AUDIT PLAN and AUDIT DATES

The audit plan previously defined for this audit was validated between the audit team and the audited team at the kick-off meeting held on July 10, 2019.

The audit work took place at the locations identified above on 10 - 12 July 2019.

The scope of the audit is defined as including the trust service of qualified Website authentication.

7. AUDIT REGULATORY FRAMEWORK

The present audit has been 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 09, 2009

Relevant Note:

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

*Thus, the implementation of the PKI was executed by the audited entity based on an approach embracing the latest standards and security requirements similar to the new European regulations eIDAS - **E**lectronic **ID**entification, **A**uthentication and trust **S**ervices.*

Whereas the SISP option derives from the definition of a profile for issuing certificates of type EV - Extended Validation, the requirements issued in formal documents by the CAB/Forum - Certification Authority Browser Forum will also be taken into account.

Since the definition indicated in this notice points out that its content must 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 allowed the audit to be carried out under this assumption, requiring appropriate checks in each case.

8. CHARACTERIZATION OF THE TRUST SERVICES

a. Description of the trust services

This trust service issues qualified EV-type web-authentication certificates, whose issuance profile despite being compliant with ETSI 319 422, and as such called 'qualified' due to the use of their QCStatment, is not considered to be an eIDAS service and therefore does not contain their attributes or features.

EV-type certificates will be issued in accordance with version 1.7.0 EV SSL Certificate Guidelines of the CAB/Forum.

The SubCA to be used will be the one already supporting SISP accreditation as a TSP - Trusted Service Provider.

b. Architecture of PKI systems

The architecture of networks and systems that supports the components of this trust service is the same as that used by the TSP for the remaining certified trust services, and, therefore, all findings and follow-up audit results presented in the Report no. 01/2019 shall apply.

c. NTP service architecture of the PKI

The system architecture of the NTP services that supports the components of this trusted service is the same as that used by the TSP for the other certified trusted services, and, therefore, all findings and follow-up audit results presented in the Report no. 01/2019 shall apply.

d. Identification of the trust services

The trusted Website authentication service is implemented in a shared SubCA known as SISPCA01.

This SubCA is signed by SISP "root".

The assessed trust service is described in the table below:

FIELD	DESCRIPTION
Service type identifier	***To be defined by ARME***
Service name	Website 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 q9JSLPWVrhJAWwtsCirMTkgIfjP/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-----

9. EVIDENCE COLLECTED FOR AUDIT ANALYSIS

a. Documentation assessed

The following SISP documents have been analyzed:

Base	Version	Activity	Process Type	Process
PLRC002	2.0	Statement of Practices of the Subordinate Certification Entity SISPCA01	Execution	PR001 Customer Relations
PLRC004	2.0	Certificate Policy of the Subordinate Certification Entity SISPCA01	Execution	PR001 Customer Relations
FRRC011	1.0	Application Form for the Issue of Qualified Digital Certificate – Web Authentication (SSL EV)	Support	PS004 Information Systems

b. Application Form

The following caveats result from the analysis of these documents:

- The option "personal" remains to be added to the type of organization
- The 'name of the organization' must be 'company name'.
- The "postal code" is missing as an option
- Usability notes placed in the "email" field should appear in the Statement of Practices and not in the form
- In section 3, it should be possible to place up to 10 domain names, depending on the statement of practices.
- The objective for each domain should also be added.

c. Portal for certificate issuing application forms

An analysis of the tool enabling the management of certificate issuing requests was carried out, which resulted in the following findings:

- Only 1 domain registration is available, rather than up to 10
- It should be ensured that only email domains defined by the statement of practices can be used
- The contact of the lead technician or technical manager must be mandatorily different from the person in charge of the entity applying for the certificate(s)
- Each of the entities in charge should be required to present criminal records
- Each of the entities in charge should be required to have the respective documents certified and/or notarized
- Loading and managing the CSR at registry administrator positions shall be protected by a SISP certificate of service
- The validation of the URLs associated with the domains does not produce validated registration

Taking into account the nature of this trusted service, consideration should be given to the possibility of identifying the identities of the main signatories through remote "Video ID" sessions in a secure mode.

d. Certificate issuing profile

The analysis of this document leads to the following findings:

- The OID of the "Signature" feature or attribute must start with 1.2 and not 2.16
- The OU attribute is optional and not mandatory
- The option "Private" is missing in the attribute "Subject Business"
- There can be no reference to "optional" fields in the "Certificate Policies" attribute
- There can be no reference to "optional" fields in the "CRL Distribution Point" attribute or feature
- The "Server Authentication" field is mandatory in the "Extended Key Usage" attribute
- All fields are mandatory in the “Authority Information Access” attribute or feature
- As for the “Qualified Certificate Statement” attribute:

- All fields are mandatory
- The OID related to the "QcType" is pre eIDAS.
  Whereas the national legislation of Cabo Verde is far outdated, a pre-eIDAS OID may be used.
- The comment text should be revised as it makes reference to obsolete ETSI standards, pre eDIAS (ETSI TS 101 862), depending on the OID indicated above.

These instructions were promptly complied with under the auditor's supervision, and, consequently, a specimen certificate was issued.

The issuing profile used for these tests is identified as:

- **Perfil_CERT_SSL_01**

The "End Entity" associated to this profile is identified as:

- **Perfil_ENDE_SSL_01**

After introducing the corrections detailed above, no further situations were detected that could constitute non-conformities.

e. Specimen Certificate

The issuing request registered on the portal under no. **#PSSL20190712003** was executed with the purpose of checking the certificate issuing profile.

The certificate issued has the following serial number: **3F9BD52FF5614792**.

Its analysis and application on a test platform have demonstrated its conformity.

f. Additional technical reference standards

The following standards have been considered in this assessment as complementary references for the 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, which repeals Directive 1999/93/EC.
EN 319 403 v2.2.2	Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers
EN 319 411-1 v1.1.1	Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements
EN 319 411-2 v2.1.1	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 v1.1.1	Certificate Profiles; Part 1: Overview and common data structures
EN 319 412-2 v2.1.1	Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
EN 319 412-3 v1.1.1	Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
EN 319 412-4 v1.1.1	Certificate Profiles; Part 4: Certificate profile for web site certificates issued to organizations
EN 319 412-5 v2.1.1	Certificate Profiles; Part 5: QCStatements
CAB-FORUM	CA-Browser-Forum-BR-1.7.0

g. Annexes

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

10. NON-CONFORMITIES

Taking into consideration the compliance assessment 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 trust service(s) in the production environment.

- ***Low Impact Non-Conformity*** – violation of a requirement, due to poor evidence to support it, failure of supporting documentation, or incorrect practice due to documental commitments.

  Separately, it may not impede the operation of the trust service(s) in a production environment.

  However, together with others of the same type, it may lead to such a decision.

a. High impact

No situations have been identified that could configure a high impact non-conformity or non-compliance.

b. Low impact

The following situations have been identified as low impact non-conformities:

ID OF THE NON-CONFORMITY	LEGAL OR REGULATORY REFERENCE	JUSTIFICATION
NC.BI.1 2019	N/A	The certificate application form must be corrected taking under consideration the audit findings set out in Chapter 9 b) of this audit report. The PKI operations manual shall be synchronized with these changes.
NC.BI.2 2019	N/A	The management portal for certificate applications must be corrected taking under consideration the audit findings set out in Chapter 9 d) of this audit report.
NC.BI.3 2019	EN 319 412-4 CA-Browser-Forum-BR-1.7.0	The certificate issuing profile must be corrected taking under consideration the audit findings set out in Chapter 9 d) of this audit report.

11. OPPORTUNITIES FOR IMPROVEMENT

The opportunities for improvement that have been identified and therefore are not mandatory, are outlined below.

Nevertheless, it should be 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.

ID OF THE IMPROVEMENT ACTION	DETAILED DESCRIPTION	OBJETIVE
IO.1	Consider 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 operating errors
IO.2	It is recommended that a memorandum be submitted to ARME in relation to the use of the OID of "Extended key Usage" pre-eIDAS or eIDAS in the characterization of the "qualification" of the web authentication certificates.	Support for better compatibility with the Cab/Forum requirements
IO.3	Evidence records of validation of URLs associated with the identified domains should be created, with the guarantee of a "two-man rule".	Improved procedure security and audit support

12.AUDIT DECISION

The SISP intends to provide digital trust services pursuant to the provisions set forth in the Regulatory Decree no. 18/2007.

Three "low impact non-conformities" have been identified, which will have to be resolved within the timeframes defined by ARME.

Three improvement actions were also identified, which should be analyzed and considered by the SISP in terms of their acceptance and implementation.

At this stage, the conformity of the audited trust service should be considered as positive but conditional.

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

13. AUDIT CLOSING NOTES

a. DIFFERENCES OF OPINION

In case there are differences of opinion between the SISP and the audit team, for which it was not possible to reach a consensus during the audit works, these shall be recorded in the present report and referred to the ARME for further 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 ANAC's (National Communications Authority) 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 shall forward the present 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 the proposal, before being considered as good for execution.

e. COMPLETION OF THE AUDIT REPORT

The auditor willfully and impartially signs the present report.

	NAME	DATE	SIGNATURE
Lead Auditor:	Paulo Borges	30-07-2019	Paulo Jorge Martins Borges Assinado de forma digital por Paulo Jorge Martins Borges Dados: 2020.03.25 18:09:43 Z