Athens Stock Exchange (ATHEX)

Conformity assessment report - Provisioning of qualified certificates for website authentication

Regulation (EU) No 910/2014

August 14, 2017

Ernst & Young CertifyPoint B.V. ey.com
Cross Towers,
Antonio Vivaldistraat 150
1083 HP AMSTERDAM
The Netherlands

Ernst & Young CertifyPoint B.V.
Cross Towers, Antonio Vivaldistraat 150
1083 HP AMSTERDAM
The Netherlands
ey.com/certifypoint

VAT number: NL8113.07.335.B.01
Chamber of Commerce number: 24341681

<Accreditation pending>

Based on certification examination in conformity with defined requirements in ISO/IEC 17065:2012 and ETSI EN 319 403, and with the accredited EY eIDAS QTSP/QTS certification scheme v1.2, EY CertifyPoint gained reasonable confidence that

Athens Stock Exchange (ATHEX)
Avenue Athinon 101
104 42 Athens
Greece
protocol@athexgroup.gr
VATEL-099755108

The trust service provider and trust services:
The provisioning of qualified certificates for website authentication

Based on conformity assessment against the following requirements:

Requirements applicable to the trust service provider

Requirements from the eIDAS regulation:
Article 5.1, 13, 15, 19.1, 19.2, 20.1, 20.2, 20.3, 23, 24.2

Requirements from implementing acts:

- Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means
- Commission Implementing Decision (EU) 2015/1984 of 3 November 2015 on defining the circumstances, formats and procedures of notification
- Commission Implementing Regulation (EU) 2015/806 of 22 May 2015 on the form of the EU Trust Mark for Qualified Trust Services
- Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists
- Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognized by public sector bodies

Requirements applicable to the provisioning of qualified certificates for website authentication:

Requirements from the eIDAS regulation:
Article 24.1, 24.2e, 24.2h, 24.2i, 24.2k, 24.3, 24.4, 45.1

Are compliant with the requirements of EY eIDAS QTSP/QTS certification scheme v1.2 related to the regulation (EU) No 910/2014 of the European Parliament and of 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 (hereafter the eIDAS Regulation)

CONFIDENTIAL

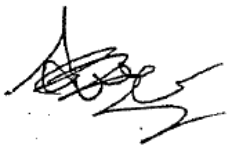
CONFORMITY ASSESSMENT REPORT

Client	: Athens Stock Exchange (ATHEX)
Address	: Avenue Athinon 101, 104 42 Athens, Greece
Contact	: protocol@athexgroup.gr
Product category	: Trust services
Trust service type(s)	: Provisioning of qualified certificates for website authentication
Date report	: August 14, 2017
Report Identification	: cp/AV/14.08.2017
Certification Body	: EY CertifyPoint
EY CertifyPoint Director	: Jatin Sehgal
EY CertifyPoint QA	: Mayank Joshi
Lead auditor	: Arvid Vermote
Auditors	: Ioannis Fragkoulopoulos
	: Ioannis Michalopoulos
	: Christophe Bonjean
Technical experts	: Nicholas Mandilaras
	: Konstantinos Varouxis
	: Evangelos Othon

EY CertifyPoint Director

Jatin Sehgal

Lead Auditor



Arvid Vermote

Table of contents

1 Introduction

1.1 Objectives

We were requested by

Athens Stock Exchange
Avenue Athinon 101
104 42 Athens
Greece
protocol@athexgroup.gr

To perform a conformity assessment of the trust service provider and the provided trust services based on the requirements defined in the EY eIDAS QTSP/QTS certification scheme v1.2 related to the eIDAS Regulation.

The scope of the conformity assessment been defined as covering "The provision of qualified certificates for website authentication" trust service.

1.2 Organization

1.2.1 Activities

Athens Stock Exchange is a trust service provider that operates trust services from Athens, Greece. The trust service provider activities include

- Operational management of the TSP
- Validation of subscriber information (both natural and legal persons) for all events related to certificate application and revocation.
- Certificate issuing activities
- Hosting of infrastructure and TSP issuing systems

1.2.2 Client team

The following table provides an overview of the titles and position of the client team members that have been contacted in the context of this conformity assessment.

Name	Team
Eleftheria Theologou	Digital Certification Services Manager
Stamatis Vamvakeris	PKI Software Administrator
Vassilis Papastogiannidis	PKI Infrastructure - Systems Administrator
Georgios Vasiliou	PKI Infrastructure – Network Administrator
Eirini Manolopoulou	Registration Services
Spyridon Skoularikis	Backup Administrator

1.2.3 Trust service hierarchy

The following table provides an overview of the trust service hierarchy related to the qualified trust services:

Qualified CA Details
CN = ATHEX Root CA G2, O = ATHENS STOCK EXCHANGE, C = GR Serial Number = 3e cf Subject Key Identifier = 47 a3 a6 04 9d 2d 96 e5
Qualified CA Details

Qualified CA Details
CN = ATHEX SSL Certificates CA G2, O = ATHENS STOCK EXCHANGE, C = GR Serial Number = 3e f8 Subject Key Identifier = 4c cd 5b ec 9a 03 92 2f

1.3 Scope

1.3.1 Sites

The following sites are in scope of the audit:

- Athens, Greece

1.3.2 Trust service

The scope of the conformity assessment been defined as covering "the provisioning of qualified certificates for website authentication" trust service.

The qualified certificates will be provided by the following certificate authorities (see appendix for detailed information of each certificate authority):

Qualified CA Details
CN = ATHEX SSL Certificates CA G2, O = ATHENS STOCK EXCHANGE, C = GR Serial Number = 3e f8 Subject Key Identifier = 4c cd 5b ec 9a 03 92 2f

The scope of conformity assessment is characterized by the "Service digital identifier" (cfr CID (EU) 2015/1505 and ETSI TS 119 612 v2.1.1) of the inspected trust service and the following candidate information relevant for inclusion in the national trusted list of the competent supervisory body of the territory in which Athens Stock Exchange is established.

Qualified certificates for website authentication will be provided by the following certificate authorities:

- O = ATHENS STOCK EXCHANGE
- CN = ATHEX SSL Certificates CA G2
- C = GR

Service type identifier = URI: http://uri.etsi.org/TrstSvc/Svctype/CA/QC

additionalServiceInformation = http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication

1.4 Requirements

The conformity assessment of the trust service provider and the trust services in scope was based on the requirements of the EY eIDAS QTSP/QTS certification scheme v1.2 related to the regulation (EU) No 910/2014 of the European Parliament and of 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 (hereafter the eIDAS Regulation), as indicated in the following table.

QTSP/QTS type	Normative requirements	Articles
Qualified trust service provider	Regulation (EU) No 910/2014	5.1, 13, 15, 19.1, 19.2, 20.1, 20.2, 20.3, 23.1, 23.2, 24.2
The provisioning of qualified certificates for website authentication	Regulation (EU) No 910/2014	24.1, 24.2e, 24.2h, 24.2i, 24.2k, 24.3, 24.4, 45.1

The following additional requirements were applicable to the trust service provider:

Requirements from implementing acts:

- Commission Implementing Decision (EU) 2015/1984 of 3 November 2015 on defining the circumstances, formats and procedures of notification
- Commission Implementing Regulation (EU) 2015/806 of 22 May 2015 on the form of the EU Trust Mark for Qualified Trust Services
- Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists
- Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognized by public sector bodies

1.5 Approach

We audited the (Q)TSP/(Q)TS regarding its compliance with the relevant requirements of the EY eIDAS QTSP/QTS certification scheme v1.2 related to the eIDAS Regulation in consideration of the requirements of the standards as identified and completed as specified in section 1.4 above.

During such audit, the compliance of the organizational and technical measures of the (Q)TSP/(Q)TS are assessed against the applicable requirements of EY eIDAS QTSP/QTS certification scheme v1.2. Our evaluation was twofold: design of controls and requirements (Stage 1) and evaluating the effectiveness and compliance to the controls to the requirements (Stage 2).

Stage 1 – Design check

The first stage of the assessment had following main objectives:

- To assess Athens Stock Exchange's system design documentation for all topics relevant to the assessment
- To review Athens Stock Exchange status and understanding regarding requirements of the relevant regulations, in particular with respect to the identification of key performance or significant aspects, processes, objectives and operation of the how these requirements are managed
- Undertake discussions with your core teams to determine the preparedness for the stage 2 assessment
- To collect necessary information regarding the scope of the trust services, processes and locations of Athens Stock Exchange, and related statutory and regulatory aspects and compliance
- To evaluate if the design of required controls is appropriate to the related requirements

Stage 2 – Operational effectiveness check

The purpose of the stage 2 assessment was to evaluate the implementation of required controls around Athens Stock Exchange's trust services. The evaluation included the following:

- Information and evidence about conformity to all requirements of the applicable regulations
- Performance monitoring, measuring, reporting and reviewing against key performance objectives and targets (consistent with the expectations as defined in the eIDAS regulation/ETSI standards)
- Operational control of Athens Stock Exchange to applicable processes
- Management responsibility for Athens Stock Exchange policies
- Links between the normative requirements, policy, performance objectives and targets (consistent with the expectations as defined in the standards), any applicable legal requirements, responsibilities, competence of personnel, operations, procedures and performance data.

1.6 Documentation

Throughout the conformity assessment, we requested and evaluated the following documents that were provided by the client:

- General information concerning and describing the trust service and the activities it covers;
- Description of the organizational structure of the TSP, including the use made and organizational structure of other parties (subcontractors) that provide parts of the trust services being audited;
- Description of the locations, size and functions (tasks and responsibilities) of roles/people involved in the trust services operational life-cycle processes, facility, management, technical security control processes (including other parties used, e.g. subcontractors) and also evidence of their competence or any analysis done for the same;

- Trust service policy (e.g. certificate policy) and Trust service practices statement (e.g. certification practices statement) and, where required, the associated documentation like IT network infrastructure plans with all relevant systems, manuals and instructions for the operation of the trust service;
- The risk assessment related documentation aimed to support demonstration of the requirement of eIDAS Art.19.1, including:
  - Information security risk analysis with risks and opportunities, and the actions taken to address them, related to all the interested parties;
  - Description of the risk assessment and treatment methodology;
- List of all internal documents supporting the declaration of the practices used by the TSP to provide the qualified trust services and the qualified trust service policy(ies)
- Policy Management Authority - PMA review;
- Internal/external audit reports or certifications;
- Independent reviews of information security;
- Security & personal data breach notification plan aimed to support demonstration of the requirement of eIDAS Art.19.2;
- Evidence of the detection of and reaction to security incidents, non-conformities identified during external or internal audits, including the corrective action taken for each;
- Network overview diagrams supporting segmentation and security measures;
- Detailed verification steps & guidelines documentation;
- Training materials for vetting staff;
- Arrangements to cover liability (certificate and evidence of payment);
- Information security policies and procedures, including but not limited to:
  - Key management;
  - Logical security;
  - Personnel security;
  - Physical security;
  - Backup and recovery;
  - Incident management;
  - Business continuity and disaster recovery;
  - Data protection and asset classification;
  - Change management;
- Procedures and controls in support of:
  - Publication and repository responsibilities;
  - Identification and authentication, when applicable;
  - Trust service life-cycle operational requirements;
  - Facility, management and operation controls;
  - Technical security controls;
- The termination plan of trust services (eIDAS Art.24.2.(i));
- Subscriber agreement and related terms and conditions.

1.7 Third parties

We noted that Athens Stock Exchange does not outsource the management or control of any of its information systems, networks or desktop environments to any other entity.

1.8 Timing

The conformity assessment was performed in two phases. The following table details the man/days on specific activities:

Activity	Stage 1	Stage 2	Total
Preparation	4	2	6
Documentation review	8		8
Assessment of Risk Analysis	6	8	14
On-site time	12	8	20
Audit reporting	4	4	8
Other (if Applicable)			
Total man/days:	**34**	**22**	**56**

An Intermediate surveillance audit during in-between years is required based on findings identified during this audit. The scope of the surveillance audits will be limited to a follow-up of the identified findings and assessment of changes to the trust service environment, if applicable.

The surveillance audit should be completed before 14/08/2018.

1.9 Classification of identified findings

The classification of potential findings is based on the guidelines illustrated in **Appendix – Classification of findings.**

2 Executive Summary

Based on the work performed during the conformity assessment, and given our experience reviewing private and public trust service provider implementations, during the course of our examination procedures, we did not note any deviation that would lead us to conclude that Athens Stock Exchange's TSP business practices was not in compliance with the requirements defined in the EY eIDAS QTSP/QTS certification scheme v1.2 related to the relevant eIDAS Regulation.

The assessment however demonstrated several areas of improvement. In total, 12 observations were identified during the current audit. Based on the classification model used, added in the appendix, the observations can be grouped as follows:

- 0 major non-conformities
- 6 minor non-conformities
- 6 opportunities for improvement

Rating	List of findings
Major non-conformity	No major non-conformities identified
Minor non-conformity	1. Incomplete CA key compromise procedure 2. Incomplete CA termination procedure 3. CA Root private key is online 4. Malware detection 5. Patch management 6. Vulnerability management
Opportunity for improvement	7. CA public key dissemination 8. Review of information security policy 9. TSP systems hardening 10. TSP systems monitoring 11. Certificates issued to TSP personnel 12. Website accessibility for persons with disabilities

The above findings, however, do not impact our opinion on the conformity of Athens Stock Exchange's trust services with the requirements defined in the EY eIDAS QTSP/QTS certification scheme v1.2 related to the eIDAS Regulation, as all those findings are either supported by compensating controls or are related to supporting processes or individual controls that does not result in a major finding.

The detailed report contains the approach taken during the conformity assessment and observations identified during the audit. For each of the findings, relevant sections of the compliance requirements were added. The appendix describes the classification scheme used for the identified findings.

3 Summary of document review

Based on our audit activities performed in stage 1, we are of the opinion that Athens Stock Exchange has provided us with sufficient insight in the establishment of the trust service.

4 Assessment of information security risk analysis

The EY eIDAS QTSP/QTS certification scheme v1.2 and the eIDAS Regulation requires that qualified and non-qualified trust service providers shall take appropriate technical and organizational measures to manage the risks posed to the security of the trust services they provide.

We evaluated the risk assessment performed by the TSP. The most recent risk assessment was completed 24th of June 2017, was performed at the application/service level and covers the registration, certificate generation, revocation management, revocation status information, dissemination and repository services. Additionally the extended environmental risks to the underlying infrastructure, physical and network security, loss of availability to critical hardware and applications, human resources and governance are addressed by the risk assessment.

Based on our evaluation we note that appropriate technical and organizational measures are present to appropriately manage the risks posed to the security of the in scope trust services provided by Athens Stock Exchange.

5 Findings

These findings cover the conformity assessment and are based on either general findings (covering more than one particular requirement) or findings uniquely related to specific eIDAS Regulation requirements.

5.1 Major non-conformities

No major non-conformities identified.

5.2 Minor non-conformities

5.2.1 Incomplete CA key compromise procedure

Article(s) of the regulation:

- Article 19.1

Relevant controls within supporting standards:

- [ETSI EN 319 401] Clause 7.11 (Business continuity management)
- [ETSI EN 319 411-1] Clause 6.4.8 (Compromise and disaster recovery)

Finding:

Detailed actions related to the (i) identification, (ii) confirmation and (iii) response of a root key compromise are not documented or not presented in the appropriate level of the detail (i.e. step-by-step activities with detailed (technical) instructions and workflows).

Expectation:

We expect a CA key compromise procedure that details the identification, confirmation and response to a key compromise scenario.

Conformance rationale

We confirmed that although the current procedure/plan can be further enhanced, TSP management are aware of the steps that need to be addressed to adequately identify, confirm and respond to an alleged, suspected or real key compromise event.

5.2.2 Incomplete CA termination procedure

Article(s) of the regulation:

- Article 24.2 a
- Article 24.2 i

Relevant controls within supporting standards:

- [ETSI EN 319 401] Clause 7.12 (TSP termination and termination plans)
- [ETSI EN 319 411-2] Clause 6.4.9 (Certification Authority or Registration Authority termination)
- [ETSI EN 319 411-1] Clause 6.4.9 (Certification Authority or Registration Authority termination)

Finding:

Within the TSP Termination Procedure, the termination and/or transfer of the trust service is not presented in the appropriate level of the detail (i.e. step-by-step activities with detailed (technical) instructions and workflows).

Expectation:

We expect a termination plan that details managerial and technical processes for terminating and transferring the TSP.

Conformance rationale:

We confirmed that although the current procedure/plan can be further enhanced with managerial and technical processes for terminating and transferring the TSP, TSP management are aware of the responsibilities and steps that need to take place in case of cessation of operations. Moreover, a contract is already in place in case such an event was to take place.

5.2.3 CA Root private key is online

Article(s) of the regulation:

- Article 19.1
- Article 24.2 e

Relevant controls within supporting standards:

- [ETSI EN 319 401] Clause 7.7 (Operation security)
- [ETSI EN 319 411-1] Clause 6.4.2 g (Physical security controls)

Finding:

The Root CA private key is currently online in the HSM, increasing the exposure of the Root CA and the likelihood of Root CA key compromise.

Expectation:

We expect a certificate hierarchy with an intermediate layer of subordinate issuing CAs and an offline Root CA, physically isolated from normal operations. This would reduce the likelihood of Root CA compromise and reduce the impact if issuing CA keys are compromised.

Conformance rationale:

We confirmed that only designated trusted personnel have access to the private key for use in signing subordinate CA certificates. Furthermore, the key length is appropriate to protect against compromise via a brute-force attack.

5.2.4 Malware detection

Article(s) of the regulation:

- Article 19.1
- Article 24.2 e

Relevant controls within supporting standards:

- [ETSI EN 319 401] Clause 7.7 (Operation security)

Finding:

There are no specific measures defined/implemented for prevention and detection of virus/malware software on servers supporting the trust service.

Expectation:

We expect specific measures to prevent, detect and deal with viruses/malware. For the purpose of uninterrupted operation of the infrastructure, it is typical to adopt solutions approved by the application vendor.

Conformance rationale:

We confirmed that there are no connections of the PKI infrastructure with the internal network apart from a secure connection with the backup server and a publishing of a CRL to a servant server and there are no connections to the outside world.

5.2.5 Patch Management

Article(s) of the regulation:

- Article 19.1
- Article 24.2 e

Relevant controls within supporting standards:

- [ETSI EN 319 401] Clause 7.7 (Operation security)

Finding:

Servers supporting the trust service are not provisioned nor is there a manual process to ensure security-related patches for the used operating system and software are timely installed.

Expectation:

We expect a process that ensures timely manual or provisioned installation of security patches.

Conformance rationale:

We confirmed that there are no connections of the PKI infrastructure with the internal network apart from a secure connection with the backup server and a publishing of a CRL to a servant server and there are no connections to the outside world.

5.2.6 Vulnerability Management

Article(s) of the regulation:

- Article 19.1
- Article 24.2 e

Relevant controls within supporting standards:

- [ETSI EN 319 401] Clause 7.8 g (Network Security)
- [ETSI EN 319 401] Clause 7.8 h (Network Security)

Finding:

No full (external/ internal, black/grey box), manual penetration testing exercise has been performed on the systems supporting the trust service.

Expectation:

We expect that penetration tests are performed on the systems supporting the trust service.

Conformance rationale:

We confirmed that automated vulnerability scans are performed and that there are no connections of the PKI infrastructure with the internal network apart from a secure connection with the backup server and a publishing of a CRL to a servant server and there are no connections to the outside world.

5.3 Opportunities for improvement

5.3.1 CA public key dissemination

Article(s) of the regulation:

- Article 24.2 e

Relevant controls within supporting standards:

- [ETSI EN 319 411-1] Clause 6.5.1 (Key Pair Generation and Installation)

Finding:

CA signature verification (public) keys are disseminated through the HTTP protocol instead of using the more secure HTTPS protocol.

Expectation:

We expect that the https protocol is implemented for disseminating CA signature verification (public) keys.

Conformance rationale

We confirmed that the trust service certificate details are publicly available to the (HTTPS enabled) corporate website so as to enable the crosschecking of public key data.

5.3.2 Review of information security policy

Article(s) of the regulation:

- Article 19.1

Relevant controls within supporting standards:

- [ETSI EN 319 401] Clause 6.3 (Information security policy)

Finding:

Currently, there is no formal procedure in place for the review of the information security policy. The last version of the policy is dated to 2014.

Expectation:

We expect regular, formal reviews of the information security are planned and executed.

Conformance rationale:

We confirmed that there have been no changes to the trust services offered by the TSP, to the TSP systems and application or to TSP operations that would mandate a change to the information security policy. As it stands, the information security policy adequately addresses the trust services.

5.3.3 TSP systems hardening

Article(s) of the regulation:

- Article 19.1
- Article 24.2 e

Relevant controls within supporting standards:

- [ETSI EN 319 401] Clause 7.7 (Operation security)
- [ETSI EN 319 401] Clause 7.8 (Network security)

Finding:

There is no formal policy/procedure for the hardening of TSP systems configuration.

Expectation:

We expect that a formal policy regarding the hardening of TSP systems is authored, executed and that systems configuration is periodically monitored. We expect the policy to include provisions on removing or disabling all accounts, applications, services, protocols, and ports that are not used in the TSP's operations.

Conformance rationale:

We confirmed that although a formal systems hardening policy is not in place, access to TSP systems is granted to appropriate TSP personnel and appropriate authentication schemes are in place.

Furthermore, no inappropriate/irrelevant applications are installed on the servers.

Finally, we confirmed that there are no connections of the PKI infrastructure with the internal network apart from a secure connection with the backup server and a publishing of a CRL to a servant server and there are no connections to the outside world.

5.3.4 TSP system monitoring

Article(s) of the regulation:

- Article 19.1
- Article 24.2 f

Relevant controls within supporting standards:

- [ETSI EN 319 401] Clause 6.3 (Information security policy)
- [ETSI EN 319 401] Clause 7.9 (Incident Management)

Finding:

System configurations are not monitored for integrity and there is security event monitoring of system audit logs.

Expectation:

We expect that system configuration integrity and system audit logs are monitored for integrity and malicious activity.

Conformance rationale:

We confirmed that although detective controls are not in place, following preventive controls are in place:

- Logs related to the cryptographic and certificate management actions are preserved in a way they cannot be tampered with and cryptographic devices do not allow disablement of logging activities.
- Administrative access is granted to appropriate individuals and authentication and physical access mechanisms are appropriate.

5.3.5 Certificates issued to TSP personnel

Article(s) of the regulation:

- Article 19.1

Relevant controls within supporting standards:

- [ETSI EN 319 401] Clause 6.2.2 q (Initial identity validation)

Finding:

Currently, the TSP issues certificates to its employees whilst this is not disclosed in the TSP's policies.

Expectation:

We expect the TSP to include in its policies that certificates are issued to the organization's personnel.

Conformance rationale:

We confirmed that appropriate initial identity validation procedures are in place for issuing certificates to internal employees.

5.3.6 Website accessibility for persons with disabilities

Article(s) of the regulation:

- Article 15

Relevant controls within supporting standards:

- [ETSI EN 319 401] Clause 7.13 b (Compliance)

Finding:

Accessibility guidelines have been taken into account for physical access to Athens Stock Exchange offices. Accessibility for persons with disabilities has not been evaluated for the organization's website. Persons with disabilities could communicate with Athens Stock Exchange through other electronic means such as e-mail or telephone.

Expectation:

We expect the main electronic communication means (i.e. the Athens Stock Exchange website) being accessible for persons with disabilities.

Conformance rationale:

We confirmed that Athens Stock Exchange offers alternative electronic communication means such as e-mail and telephone in case of communicating with persons with disabilities.

6 Conformity assessment

6.1 Requirements applicable to the trust service provider

6.1.1 Data processing and protection

i) Article 5.1

Relevant controls within supporting standards:

- [ETSI EN 319 401] Clause 7.13 a,c (Compliance)
- [ETSI EN 319 411-1] Clause 6.8.4 (Privacy of personal information)

Conformity statement:

We verified the conformity of the trust service provider with this article through document and record review, observation and interviews. We found the trust service provider to be in conformance with the article.

Activities performed:

- We reviewed TSP documentation related to
  - data privacy, processing and protection of personal data
  - Information ownership
  - Information classification

  The TSP has formal data privacy policy aligned to the relevant provisions of Greek Law (Law 2472/1997) on the protection of individuals and the protection of personal data as supplemented by the decisions of the Chairman of the Commission for Personal Data Protection, P.A. 207/1998 and 79/2000 and Article 8 of Law 2819/2000 and Law 2774/1999 and European law (Directives 95/46/EP and 97 /66/EP).
- We reviewed access to personal data on TSP systems and applications as well as to the physical records.
- We interviewed the Digital Certifications Services Manager on provisions on data privacy, processing and protection of personal data.

Documents reviewed:

- Certificate Practice Statement & Policy
- Data Privacy Policy
- Information Security Policy
- Data Classification Policy
- PKI Data Classification

Review of record(s):

- Employee access to PKI Certificate Management applications
- Employee access to PKI Certificate register

Observation(s):

- Provisions for Storage of physical Subscriber Agreements (as of now no certificates have been issued to customers)

Interview(s):

- Eleftheria Theologou (Digital Certifications Services Manager)
- Eirini Manolopoulou (Registration Services)

6.1.2 Liability and burden of proof

i) Article 13.1

Relevant controls within supporting standards:

- No other relevant controls

Conformity statement:

We verified the conformity of the trust service provider with this article through document review and interviews. We found the trust service provider to be in conformance with the article.

Activities performed:

- We reviewed TSP documentation regarding liability for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations under this Regulation.
- We reviewed insurance coverage (contract) to assess the TSP capacity for liability exposure.
- We interviewed the Digital Certifications Services Manager on the specific liability provisions.

Documents reviewed:

- Certificate Practice Statement & Policy
- Terms and Conditions
- Subscriber Agreement (template)
- Insurance Contract

Interview(s):

- Eleftheria Theologou (Digital Certifications Services Manager)

ii) Article 13.2

Relevant controls within supporting standards:

- [ETSI EN 319 401] Clause 6.2 (Terms and Conditions)
- [ETSI EN 319 411-1] Clause 6.9.4 (Terms and conditions)
- [ETSI EN 319 411-2] Clause 6.9.4 (Terms and conditions)

Conformity statement:

We verified the conformity of the trust service provider with this article through document review and interviews. We found the trust service provider to be in conformance with the article.

Activities performed:

- We reviewed TSP documentation regarding liability for limitations on the use of the services they provide and provisions that where those limitations are recognisable to third parties, trust service providers shall not be liable for damages arising from the use of services exceeding the indicated limitations.

  Moreover, we reviewed insurance coverage to assess the TSP capacity for liability exposure.
- We interviewed the Digital Certifications Services Manager on the limitations of the provided service.

Documents reviewed:

- Certificate Practice Statement & Policy
- Terms and Conditions
- Subscriber Agreement (template)
- Insurance Contract

Interview(s):

- Eleftheria Theologou (Digital Certifications Services Manager)

iii) Article 13.3

Relevant controls within supporting standards:

- [ETSI EN 319 401] Clause 6.2 (Terms and Conditions)
- [ETSI EN 319 411-1] Clause 6.9.4 (Terms and conditions)
- [ETSI EN 319 411-2] Clause 6.9.4 (Terms and conditions)

Conformity statement:

We verified the conformity of the trust service provider with this article through document review and interviews. We found the trust service provider to be in conformance with the article.

Activities performed:

- We reviewed TSP documentation in respect to articles 13.1 and 13.2 regarding liability according to the national rules.

  Moreover, we reviewed insurance coverage to assess the TSP capacity for liability exposure.
- We interviewed the Digital Certifications Services Manager on the limitations of the provided service.

Documents reviewed:

- Certificate Practice Statement & Policy
- Terms and Conditions
- Subscriber Agreement (template)
- Insurance Contract

Interview(s):

- Eleftheria Theologou (Digital Certifications Services Manager)

6.1.3 Accessibility for person with disabilities

i) Article 15

Relevant controls within supporting standards:

- [ETSI EN 319 401] Clause 7.13 b (Compliance)

Finding(s):

We identified an opportunity for improvement relating to accessibility for persons with disabilities. Refer to section 5 – Findings, Opportunities for improvement "Website accessibility for persons with disabilities".

Conformity statement:

We verified the conformity of the trust service provider with this article through observation. Based on the presence of compensating controls for the identified non-conformity and the items under opportunity for improvement, we found the trust service provider to be in conformance with this article.

Activities performed:

We have performed an onsite inspection on accessibility for physical access to Athens Stock Exchange offices. Accessibility for persons with disabilities has not been evaluated for the organization's website.

Observation(s):

Physical Access for persons with disabilities to TSP offices

6.1.4 Security requirements applicable to trust service providers

i) Article 19.1

Relevant controls within supporting standards:

- [ETSI EN 319 401] Clause 5 (Risk assessment)
- [ETSI EN 319 401] Clause 6.2.2 (Initial identity validation)
- [ETSI EN 319 401] Clause 6.3 (Information security policy)
- [ETSI EN 319 401] Clause 7.1.1 (Organization reliability)
- [ETSI EN 319 401] Clause 7.2 (Human resources)
- [ETSI EN 319 401] Clause 7.3 (Asset management)
- [ETSI EN 319 401] Clause 7.4 (Access control)
- [ETSI EN 319 401] Clause 7.5 (Cryptographic controls)
- [ETSI EN 319 401] Clause 7.6 (Physical and environmental security)
- [ETSI EN 319 401] Clause 7.7 (Operation security)
- [ETSI EN 319 401] Clause 7.8 (Network security)
- [ETSI EN 319 401] Clause 7.9 (Incident management)
- [ETSI EN 319 401] Clause 7.10 (Collection of evidence)
- [ETSI EN 319 401] Clause 7.11 (Business continuity management)
- [ETSI EN 319 411-1] Clause 6.4.2 (Physical Security Controls)
- [ETSI EN 319 411-1] Clause 6.4.3 (Procedural controls)
- [ETSI EN 319 411-1] Clause 6.4.4 (Personnel controls)
- [ETSI EN 319 411-1] Clause 6.4.8 (Compromise and disaster recovery)
- [ETSI EN 319 411-1] Clause 6.8.6 (Representations and warranties)
- [ETSI EN 319 411-1] Clause 6.9.1 (Organizational)
- [ETSI EN 319 411-2] Clause 6.8.6 (Representations and warranties)

Finding(s):

1) We identified a minor non-conformity relating to the CA key compromise procedure/plan. Refer to section 5 – Findings, Minor non-conformities "Incomplete CA key compromise procedure".
2) We identified a minor non-conformity relating to the CA Root private key being online. Refer to section 5 – Findings, Minor non-conformities "CA Root private key is online".
3) We identified a minor non-conformity relating to Malware detection. Refer to section 5 – Findings, Minor non-conformities "Malware detection".
4) We identified a minor non-conformity relating to patch management. Refer to section 5 – Findings, Minor non-conformities "Patch Management".
5) We identified a minor non-conformity relating to vulnerability management. Refer to section 5 – Findings, Minor non-conformities "Vulnerability Management".
6) We identified an opportunity for improvement relating to the review of the information security policy. Refer to section 5 – Findings, Opportunities for improvement "Review of information security policy".
7) We identified an opportunity for improvement relating to TSP systems hardening. Refer to section 5 – Findings, Opportunities for improvement "TSP systems hardening".

8) We identified an opportunity for improvement relating to TSP systems monitoring. Refer to section 5 – Findings, Opportunities for improvement "TSP systems monitoring".

9) We identified an opportunity for improvement relating to Certificates issued to TSP personnel. Refer to section 5 – Findings, Opportunities for improvement "Certificates issued to TSP personnel".

Conformity statement:

We verified the conformity of the trust service provider with this article through document review, record review, observation and interviews. Based on the presence of compensating controls for the identified non-conformities and the item under opportunity for improvement, we found the trust service provider to be in conformance with this article.

Activities performed:

- We reviewed TSP documentation as to the appropriateness of technical and organisational measures to manage the risks posed to the security of the trust services they provide.
- We reviewed records of technical measures at the application and network level, physical access which was also reviewed by observation, organisational measures including HR screening processes, identity validation, incident management, IT operations including backup, secure handling & destruction of data and provisions to transfer obligation for information maintenance in case of cessation of operations.

  We reviewed the TSP procedures, plan in case of cessation of operations as well as the contract with the related party to transfer obligation for information maintenance in case of cessation of operations.

  We reviewed the TSP CA key compromise procedure/plan.
- We interviewed TSP personnel as per areas identified above.

Documents reviewed:

- Certificate Practice Statement & Policy
- Information Security policy
- Risk assessment
- Physical security policy
- Information Security Policy
- Data Privacy Policy
- Data Classification Policy
- PKI Data Classification
- Terms and conditions
- Incident Management procedure
- Network diagram
- HR screening
- Athens Stock Exchange cryptography standards
- Business continuity manual
- Contract to transfer obligations to a reliable party for maintaining all information necessary to provide evidence of the operation of the TSP
- Procedure for the destruction of assets & related contract with reliable party

Review of record(s):

- Employee access to PKI Certificate Management applications

- Employee access to PKI Certificate register
- Employee Access to PKI spaces and access logs
- Backup records
- Incident Management records
- Complaints and disputes
- Insurance contracts
- Firewall ruleset
- Routers configurations
- Vulnerability assessment
- Risk assessment
- Cryptographic units, algorithms, key sizes, validity periods
- Qualified Signature Creation devices
- X.509 Certificates (CA, subCAs, SSL test certificate) specifications including QCStatements
- CRLs specifications
- OCSP service
- Subscriber Agreement (template)
- Certificate Management (creations, renewals, suspensions, revocations)
- Validity of Identity

Observation(s):

- Physical Access provisions

Interview(s):

- Eleftheria Theologou (Digital Certifications Services Manager)
- Stamatis Vamvakeris (PKI Software Administrator)
- Vassilis Papastogiannidis (PKI Infrastructure - Systems Administrator)
- Georgios Vasiliou (PKI Infrastructure – Network Administrator)
- Eirini Manolopoulou (Registration Services)
- Spyridon Skoularikis (Backup Administrator)

ii) Article 19.2

Relevant controls within supporting standards:

- [ETSI EN 319 401] Clause 7.9 e, f (Incident management)

Conformity statement:

We verified the conformity of the trust service provider with this article through document review, record review and interviews. We found the trust service provider to be in conformance with the article.

Activities performed:

- We reviewed TSP documentation as to provisions for notification to the supervisory body and other relevant bodies of any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein.
- We reviewed the related Incident Management software application.
- We interviewed the Digital Certifications Services Manager and assessed that commitment as to the above.

Documents reviewed:

- Certificate Practice Statement & Policy
- Incident Management procedure
- Information Security policy
- Terms and conditions

Review of record(s):

- Incident Management records

Interview(s):

- Eleftheria Theologou (Digital Certifications Services Manager)

6.1.5 Supervision of qualified trust service providers

i) Article 20.1

Relevant controls within supporting standards:

- No other relevant controls

Conformity statement:

We verified the conformity of the trust service provider with this article through interviews. We found the trust service provider to be in conformance with the article.

Activities performed:

We interviewed the Digital Certifications Services Manager and have identified that the TSP has in its plans to be audited as per the regulation every 24 months or if any event requires a new assessment.

Interview(s):

- Eleftheria Theologou (Digital Certifications Services Manager)

ii) Article 20.2

Relevant controls within supporting standards:

- No other relevant controls

Conformity statement:

We verified the conformity of the trust service provider with this article through interviews. We found the trust service provider to be in conformance with the article.

Activities performed:

We interviewed the Digital Certifications Services Manager and have identified that the TSP recognises and accepts that requirement to be subject to an audit or an ad-hoc conformity assessment if the supervisory body requests it.

Interview(s):

- Eleftheria Theologou (Digital Certifications Services Manager)

iii) Article 20.3

Relevant controls within supporting standards:

- No other relevant controls

Conformity statement:

We verified the conformity of the trust service provider with this article through interviews. We found the trust service provider to be in conformance with the article.

Activities performed:

We interviewed the Digital Certifications Services Manager and have identified that the TSP recognises and accepts the fact that where the supervisory body requires the qualified trust service provider to remedy any failure to fulfil requirements under this Regulation and where that provider does not act accordingly, and if applicable within a time limit set by the supervisory body, the supervisory body, taking into account, in particular, the extent, duration and consequences of that failure, may withdraw the qualified status of that provider or of the affected service it provides and inform the body referred to in Article 22(3) for the purposes of updating the trusted lists referred to in Article 22(1).

Interview(s):

- Eleftheria Theologou (Digital Certifications Services Manager)

6.1.6 EU trust mark for qualified trust services

i) Article 23.1

Relevant controls within supporting standards:

- No other relevant controls

Conformity statement:

We verified the conformity of the trust service provider with this article through an interview. We found the trust service provider to be in conformance with the article.

Activities performed:

We interviewed the Digital Certifications Services Manager and have identified that the TSP recognises and accepts that they may use has the EU trust mark to indicate in a simple, recognisable and clear manner the qualified trust services they provide, after the supervisory body verifies whether the trust service provider and the trust services provided by it comply with the requirements laid down in this Regulation, and in particular, with the requirements for qualified trust service providers and for the qualified trust services they provide. Moreover, the TSP recognises the allowed uses and graphical depictions of the EU trust mark.

Interview(s):

- Eleftheria Theologou (Digital Certifications Services Manager)

ii) Article 23.2

Relevant controls within supporting standards:

- No other relevant controls

Conformity statement:

We verified the conformity of the trust service provider with this article through interviews We found the trust service provider to be in conformance with the article.

Activities performed:

We interviewed the Digital Certifications Services Manager and have identified that the TSP recognises and accepts that when using the EU trust mark for the qualified trust services referred to in Article 23.1, the TSP shall ensure that a link to the relevant trusted list is made available on their website. Moreover, the TSP recognises the allowed uses and graphical depictions of the EU trust mark.

Interview(s):

- Eleftheria Theologou (Digital Certifications Services Manager)

iii) Article 23.3

Relevant controls within supporting standards:

- No other relevant controls

Conformity statement:

We verified the conformity of the trust service provider with this article through interviews. We found the trust service provider to be in conformance with the article.

Activities performed:

We interviewed the Digital Certifications Services Manager and have identified that the TSP recognises and accepts that they may use has the EU trust mark to indicate in a simple, recognisable and clear manner the qualified trust services they provide, after the supervisory body verifies whether the trust service provider and the trust services provided by it comply with the requirements laid down in this Regulation, and in particular, with the requirements for qualified trust service providers and for the qualified trust services they provide. Moreover, the TSP recognises the allowed uses and graphical depictions of the EU trust mark.

We interviewed the Digital Certifications Services Manager and have identified that the TSP recognises and accepts that when using the EU trust mark for the qualified trust services referred to in Articles 23.1 and 23.2, the TSP recognises and accepts the requirement to abide to the specifications with regard to the form, and in particular the presentation, composition, size and design of the EU trust mark for qualified trust services as provided in implementing acts by the Commission.

Interview(s):

- Eleftheria Theologou (Digital Certifications Services Manager)

6.1.7 Requirements for qualified trust service providers

i) Article 24.2 a

Relevant controls within supporting standards:

- [ETSI EN 319 401] Clause 7.12 (TSP termination and termination plans)

Finding(s):

1) We identified a minor non-conformity relating to the CA Termination procedure/plan. Refer to section 5 – Findings, Minor non-conformities "Incomplete CA termination procedure".

Conformity statement:

We verified the conformity of the trust service provider with this article through document review and interviews. We found the trust service provider to be in conformance with the article.

Activities performed:

- We reviewed TSP documentation relating to communication to the supervisory body of any change in the provision of its qualified trust services and an intention to cease those activities.
- We reviewed the contracts with other parties for the secure handling & destruction of data and provisions to transfer obligation for information maintenance in case of cessation of operations.
- We interviewed the Digital Certifications Services Manager on the above.

Documents reviewed:

- Certificate Practice Statement & Policy
- Procedure for communication with supervisory body
- Contract to transfer obligations to a reliable party for maintaining all information necessary to provide evidence of the operation of the TSP
- Procedure for the destruction of assets & related contract with reliable party

Interview(s):

- Eleftheria Theologou (Digital Certifications Services Manager)

ii) Article 24.2 b

Relevant controls within supporting standards:

- [ETSI EN 319 401] Clause 7.1.2 (Segregation of duties)
- [ETSI EN 319 401] Clause 7.2 (Human resources)
- [ETSI EN 319 411-1] Clause 6.4.4 (Personnel controls)

Conformity statement:

We verified the conformity of the trust service provider with this article through document review, record review, observation and interviews. We found the trust service provider to be in conformance with the article.

Activities performed:

- We have reviewed TSP documentation on employee controls on screening and competencies.
- We have reviewed records of the periodical screening process including resubmission of employee criminal records and employee trainings.
- We interviewed the Digital Certifications Services Manager on the above.

Documents reviewed:

- HR screening
- Employee training
- PKI roles

Review of record(s):

- Employee training
- Employee access to PKI Certificate Management applications
- Access Logs to PKI spaces

Observation(s):

- HR screening

Interview(s):

- Eleftheria Theologou (Digital Certifications Services Manager)

iii) Article 24.2 c

Relevant controls within supporting standards:

- [ETSI EN 319 401] Clause 7.1.1 c (Maintain sufficient financial resources/ obtain appropriate liability insurance)

Conformity statement:

We verified the conformity of the trust service provider with this article through document review and interviews. We found the trust service provider to be in conformance with the article.

Activities performed:

- We reviewed TSP documentation with regard to the risk of liability for damages in accordance with Article 13, maintain sufficient financial resources and/or obtain appropriate liability insurance, in accordance with national law.
- We reviewed insurance coverage (contract) to assess the TSP capacity for liability exposure.

  Moreover, we reviewed publicly available Financial Statements to assess the current financial state of the TSP.
- We interviewed the Digital Certifications Services Manager on the specific provisions.

Documents reviewed:

- Terms and conditions
- Insurance Contract
- Review of publicly available Financial Statements

Interview(s):

- Eleftheria Theologou (Digital Certifications Services Manager)

iv) Article 24.2 d

Relevant controls within supporting standards:

- [ETSI EN 319 401] Clause 6.1 (Trust Service Practice (TSP) statement)
- [ETSI EN 319 401] Clause 6.2 (Terms and Conditions)
- [ETSI EN 319 411-1] Clause 6.9.4 (Terms and conditions)
- [ETSI EN 319 411-2] Clause 6.9.4 (Terms and conditions)

Conformity statement:

We verified the conformity of the trust service provider with this article through document review and interviews. We found the trust service provider to be in conformance with the article.

Activities performed:

- We reviewed TSP documentation regarding the requirement before entering into a contractual relationship, inform, in a clear and comprehensive manner, any person seeking to use a qualified trust service of the precise terms and conditions regarding the use of that service, including any limitations on its use.
- We interviewed the Digital Certifications Services Manager on related provisions.

Documents reviewed:

- Certificate Practice Statement & Policy
- Terms and conditions
- Subscriber Agreement (template)

Interview(s):

- Eleftheria Theologou (Digital Certifications Services Manager)

v) Article 24.2 e

Relevant controls within supporting standards:

- [ETSI EN 319 401] Clause 7.7 (Operation security)
- [ETSI EN 319 401] Clause 7.8 (Network security)
- [ETSI EN 319 411-2] Clause 6.1 (Publication and Repository Responsibilities)
- [ETSI EN 319 411-2] Clause 6.4.5 (Audit Logging Procedures)
- [ETSI EN 319 411-2] Clause 6.4.6 (Records Archival)
- [ETSI EN 319 411-2] Clause 6.5.1 (Key Pair Generation and Installation)

Finding(s):

1) We identified a minor non-conformity relating to the CA Root private key being online. Refer to section 5 – Findings, Minor non-conformities "CA Root private key is online".
2) We identified a minor non-conformity relating to Malware detection. Refer to section 5 – Findings, Minor non-conformities "Malware detection".

3) We identified a minor non-conformity relating to patch management. Refer to section 5 – Findings, Minor non-conformities "Patch Management".
4) We identified a minor non-conformity relating to vulnerability management. Refer to section 5 – Findings, Minor non-conformities "Vulnerability Management".
5) We identified an opportunity for improvement relating to the CA publc key dissemination. Refer to section 5 – Findings, Minor non-conformities "CA public key dissemination".
6) We identified an opportunity for improvement relating to TSP systems hardening. Refer to section 5 – Findings, Opportunities for improvement "TSP systems hardening".

Conformity statement:

We verified the conformity of the trust service provider with this article through document review, record review, observation and interviews. Based on the presence of compensating controls for the identified non-conformities and the items under opportunity for improvement, we found the trust service provider to be in conformance with this article.

Activities performed:

- We reviewed TSP documentation for the requirement to use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them.
- We reviewed records of technical measures at the application and network level, cryptography-specific measures, physical access which was also reviewed by observation, incident management and IT operations including backup.

  We reviewed platform audit logs and confirmed appropriate logging of events and protection against record modification or deletion.
- We interviewed TSP personnel as per areas identified above.

Documents reviewed:

- Certificate Practice Statement & Policy
- Information Security Policy
- Network diagram
- Change Management procedure
- Logical Access procedure
- Backup procedure

Review of record(s):

- Firewall ruleset
- Routers configurations
- Vulnerability assessment
- Cryptographic units, algorithms, key sizes, validity periods
- Qualified Signature Creation devices
- X.509 Certificates (CA, subCAs, Subscribers) specifications including QCStatements
- CRLs specifications
- OCSP service
- Employee Access to PKI systems and applications
- Authentication scheme of PKI systems and applications
- Employee Access to PKI spaces and access logs

- Backup records
- Platform audit logs

Observation(s):

- Physical Access provisions

Interview(s):

- Eleftheria Theologou (Digital Certifications Services Manager)
- Vassilis Papastogiannidis (PKI Infrastructure - Systems Administrator)
- Georgios Vasiliou (PKI Infrastructure – Network Administrator)
- Spyridon Skoularikis (Backup Administrator)

vi) Article 24.2 f

Relevant controls within supporting standards:

- [ETSI EN 319 401] Clause 7.4 a, f (Access control)
- [ETSI EN 319 401] Clause 7.5 (Cryptographic controls)
- [ETSI EN 319 401] Clause 7.7 (Operation security)
- [ETSI EN 319 401] Clause 7.8 (Network security)
- [ETSI EN 319 401] Clause 7.9 (Incident Management)
- [ETSI EN 319 401] Clause 7.10 (Collection of evidence)
- [ETSI EN 319 411-1] Clause 6.4.3 (Procedural controls)

Finding(s):

We identified an opportunity for improvement relating to TSP systems monitoring. Refer to section 5 – Findings, Opportunities for improvement "TSP systems monitoring".

Conformity statement:

We verified the conformity of the trust service provider with this article through document review, record review, observation and interviews. Based on the presence of compensating controls for the identified item under opportunity for improvement, we found the trust service provider to be in conformance with this article.

Activities performed:

- We reviewed TSP documentation as to the trustworthiness of systems used to store data provided, in a verifiable form, and the trustworthiness of the related access path to the data.
- We reviewed access to data including personal data on TSP systems and applications as well as to the physical records. We reviewed technical provisions for the authenticity of data,

  Moreover, we reviewed physical access documentation and observed related implementations.

  Finally, we inspected onsite the Provisions for Storage of physical Subscriber Agreements (as of now no certificates have been issued to customers)
- We interviewed the Digital Certifications Services Manager on related provisions.

Documents reviewed:

- Certificate Practice Statement & Policy
- Information Security Policy
- Physical security policy
- Terms and Conditions
- Network diagram

- Athens Stock Exchange cryptography standards
- Subscriber Agreement (template)

Review of record(s):

- Employee access to PKI Certificate Management applications
- Employee access to PKI Certificate register
- Employee Access to PKI spaces and access logs
- Firewall ruleset
- Routers configurations
- Vulnerability assessment

Observation(s):

- Provisions for Storage of physical Subscriber Agreements (as of now no certificates have been issued to customers)
- Physical Access provisions

Interview(s):

- Eleftheria Theologou (Digital Certifications Services Manager)
- Stamatis Vamvakeris (PKI Software Administrator)
- Vassilis Papastogiannidis (PKI Infrastructure - Systems Administrator)
- Georgios Vasiliou (PKI Infrastructure – Network Administrator)

vii) Article 24.2 g

Relevant controls within supporting standards:

- [ETSI EN 319 401] Clause 7.6 (Physical and environmental security)
- [ETSI EN 319 401] Clause 7.7 (Operation security)

Conformity statement:

We verified the conformity of the trust service provider with this article through document review, record review, observation and interviews. We found the trust service provider to be in conformance with the article.

Activities performed:

- We reviewed TSP documentation as to the appropriateness of measures against forgery and theft of data and the trustworthiness of the related access path to the data.
- We reviewed access to data including personal data on TSP systems and applications as well as to the physical records. We reviewed technical provisions for the authenticity of data,

  Moreover, we reviewed physical access documentation and observed related implementations.

  Finally, we inspected onsite the Provisions for Storage of physical Subscriber Agreements (as of now no certificates have been issued to customers)
- We interviewed the Digital Certifications Services Manager on related provisions.

Documents reviewed:

- Certificate Practice Statement & Policy
- Information Security Policy
- Physical security policy
- Terms and Conditions
- Network diagram

- Athens Stock Exchange cryptography standards
- Subscriber Agreement (template)

Review of record(s):

- Employee access to PKI Certificate Management applications
- Employee access to PKI Certificate register
- Employee Access to PKI spaces and access logs
- Firewall ruleset
- Routers configurations
- Vulnerability assessment

Observation(s):

- Provisions for Storage of physical Subscriber Agreements (as of now no certificates have been issued to customers)
- Physical Access provisions

Interview(s):

- Eleftheria Theologou (Digital Certifications Services Manager)
- Stamatis Vamvakeris (PKI Software Administrator)
- Vassilis Papastogiannidis (PKI Infrastructure - Systems Administrator)
- Georgios Vasiliou (PKI Infrastructure – Network Administrator)

viii) Article 24.2 h

Relevant controls within supporting standards:

- [ETSI EN 319 401] Clause 7.10 (Collection of evidence)

Conformity statement:

We verified the conformity of the trust service provider with this article through document review, record review and interviews. We found the trust service provider to be in conformance with the article.

Activities performed:

- We reviewed TSP documentation for the requirement to record and maintain information concerning data issued and received by the qualified trust service provider, even after potentially ceasing of the service.
- We reviewed platform audit logs and confirmed appropriate logging of events and protection against record modification or deletion.

  Moreover, we reviewed the contract with the related party to transfer obligation for information maintenance in case of cessation of operations.
- We interviewed the Digital Certifications Services Manager on the above.

Documents reviewed:

- Certificate Practice Statement & Policy
- Contract to transfer obligations to a reliable party for maintaining all information necessary to provide evidence of the operation of the TSP

Review of record(s):

- Platform audit logs

Interview(s):

- Eleftheria Theologou (Digital Certifications Services Manager)

ix) Article 24.2 i

Relevant controls within supporting standards:

- [ETSI EN 319 401] Clause 7.12 (TSP termination and termination plans)

Finding(s):

1) We identified a minor non-conformity relating to the CA Termination procedure/plan. Refer to section 5 – Findings, Minor non-conformities "Incomplete CA termination procedure".

Conformity statement:

We verified the conformity of the trust service provider with this article through document review and interviews. Based on the presence of compensating controls for the identified minor non-conformity, we found the trust service provider to be in conformance with this article.

Activities performed:

- We reviewed TSP documentation relating to provisions for the Cessation of its Operations including the TSP termination plan.

  We reviewed the contracts with other parties for the secure handling & destruction of data and provisions to transfer obligation for information maintenance in case of cessation of operations.

- We interviewed the Digital Certifications Services Manager on the above.

Documents reviewed:

- Certificate Practice Statement & Policy
- Contract to transfer obligations to a reliable party for maintaining all information necessary to provide evidence of the operation of the TSP
- Procedure for the destruction of assets & related contract with reliable party

Interview(s):

- Eleftheria Theologou (Digital Certifications Services Manager)

x) Article 24.2 j

Relevant controls within supporting standards:

- [ETSI EN 319 401] Clause 7.13 a,c (Compliance)
- [ETSI EN 319 411-1] Clause 6.8.4 (Privacy of personal information)

Conformity statement:

We verified the conformity of the trust service provider with this article through document and record review, observation and interviews. We found the trust service provider to be in conformance with the article.

Activities performed:

- We reviewed TSP documentation related to
  - data privacy, processing and protection of personal data
  - Information ownership
  - Information classification

  The TSP has formal data privacy policy aligned to the relevant provisions of Greek Law (Law 2472/1997) on the protection of individuals and the protection of personal data as supplemented by the decisions of the Chairman of the Commission for Personal Data Protection, P.A. 207/1998 and 79/2000 and Article 8 of Law 2819/2000 and Law 2774/1999 and European law (Directives 95/46/EP and 97 /66/EP).

- We reviewed access to personal data on TSP systems and applications as well as to the physical records.

- We interviewed the Digital Certifications Services Manager on provisions on data privacy, processing and protection of personal data.

Documents reviewed:

- Certificate Practice Statement & Policy
- Data Privacy Policy
- Information Security Policy
- Data Classification Policy
- PKI Data Classification

Review of record(s):

- Employee access to PKI Certificate Management applications
- Employee access to PKI Certificate register

Observation(s):

- Provisions for Storage of physical Subscriber Agreements (as of now no certificates have been issued to customers)

Interview(s):

- Eleftheria Theologou (Digital Certifications Services Manager)

6.2 Requirements applicable to the provisioning of qualified certificates for website authentication

6.2.1 Requirements for qualified trust service providers

i) Article 24.1

Relevant controls within supporting standards:

- [ETSI EN 319 411-1] Clause 6.2.2 (Initial Identity Validation)
- [ETSI EN 319 411-2] Clause 6.2.2 (Initial Identity Validation)
- [ETSI EN 319 411-1] Clause 6.2.3 (Identification and authentication for Re-key requests)

Conformity statement:

We verified the conformity of the trust service provider with this article through document review, record review and interviews. We found the trust service provider to be in conformance with the article.

Activities performed:

- We reviewed TSP documentation on subscriber identity verification.
- We reviewed the subscriber application procedure and the subscriber agreement (template) and related actions that need be performed by the TSP (as of now no certificates have been issued to customers).
- We interviewed the Digital Certifications Services Manager and a Registration Officer on identity validation procedures.

Documents reviewed:

- Certificate Practice Statement & Policy

Review of record(s):

- Subscriber Agreement (template)

Interview(s):

- Eleftheria Theologou (Digital Certifications Services Manager)
- Eirini Manolopoulou (Registration Services)

ii) Article 24.2 e

Relevant controls within supporting standards:

- [ETSI EN 319 401] Clause 7.5 (Cryptographic controls)
- [ETSI EN 319 411-1] Clause 6.5 (Technical Security Controls)
- [ETSI EN 319 411-2] Clause 6.5 (Technical Security Controls)

Finding(s):

1) We identified a minor non-conformity relating to the CA Root private key being online. Refer to section 5 – Findings, Minor non-conformities "CA Root private key is online".
2) We identified a minor non-conformity relating to Malware detection. Refer to section 5 – Findings, Minor non-conformities "Malware detection".
3) We identified a minor non-conformity relating to patch management. Refer to section 5 – Findings, Minor non-conformities "Patch Management".
4) We identified a minor non-conformity relating to vulnerability management. Refer to section 5 – Findings, Minor non-conformities "Vulnerability Management".

5) We identified an opportunity for improvement relating to the CA publc key dissemination. Refer to section 5 – Findings, Minor non-conformities "CA public key dissemination".

6) We identified an opportunity for improvement relating to TSP systems hardening. Refer to section 5 – Findings, Opportunities for improvement "TSP systems hardening".

Conformity statement:

We verified the conformity of the trust service provider with this article through document review, record review and interviews. Based on the presence of compensating controls for the identified non-conformities and the items under opportunity for improvement, we found the trust service provider to be in conformance with this article.

Activities performed:

- We reviewed TSP documentation on the use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them.
- We reviewed cryptographic device certifications, the ceremonies of CA and subCAs, technical measures of the cryptographic functions, certificate and CRL profiling and the OCSP service.
- We interviewed the Digital Certifications Services Manager on the above.

Documents reviewed:

- Certificate Practice Statement & Policy
- Information Security Policy
- Athens Stock Exchange cryptography standards
- Ceremony of CA and subCAs

Review of record(s):

- Cryptographic units, algorithms, key sizes, validity periods
- Qualified Signature Creation devices
- X.509 Certificates (CA, subCAs, Subscribers) specifications including QCStatements
- CRLs specifications
- OCSP service

Interview(s):

- Eleftheria Theologou (Digital Certifications Services Manager)

iii) Article 24.2 h

Relevant controls within supporting standards:

- [ETSI EN 319 401] Clause 7.10 (Collection of evidence)
- [ETSI EN 319 411-2] Clause 6.4.5 (Audit logging procedures)
- [ETSI EN 319 411-1] Clause 6.4.5 (Audit logging procedures)
- [ETSI EN 319 411-2] Clause 6.4.6 (Records archival)
- [ETSI EN 319 411-1] Clause 6.4.6 (Records archival)

Conformity statement:

We verified the conformity of the trust service provider with this article through document review and interviews. We found the trust service provider to be in conformance with the article.

Activities performed:

- We reviewed TSP documentation for the requirement to record and maintain information concerning data issued and received by the qualified trust service provider, even after potentially ceasing of the service.
- We reviewed platform audit logs and confirmed appropriate logging of events and protection against record modification or deletion.

  We reviewed the contract with the related party to transfer obligation for information maintenance in case of cessation of operations.
- We interviewed the Digital Certifications Services Manager on the above.

Documents reviewed:

- Certificate Practice Statement & Policy
- Information Security Policy
- Contract to transfer obligations to a reliable party for maintaining all information necessary to provide evidence of the operation of the TSP

Review of record(s):

- Platform audit logs

Interview(s):

- Eleftheria Theologou (Digital Certifications Services Manager)

iv) Article 24.2 i

Relevant controls within supporting standards:

- [ETSI EN 319 401] Clause 7.12 (TSP termination and termination plans)
- [ETSI EN 319 411-1] Clause 6.4.9 (Certification Authority or Registration Authority termination)
- [ETSI EN 319 411-2] Clause 6.4.9 (Certification Authority or Registration Authority termination)

Finding(s):

1) We identified a minor non-conformity relating to the CA Termination procedure/plan. Refer to section 5 – Findings, Minor non-conformities "Incomplete CA termination procedure".

Conformity statement:

We verified the conformity of the trust service provider with this article through document review and interviews. Based on the presence of compensating controls for the identified minor non-conformity, we found the trust service provider to be in conformance with this article.

Activities performed:

- We reviewed TSP documentation relating to provisions for the Cessation of its Operations including the TSP termination plan.

  We reviewed the contracts with other parties for the secure handling & destruction of data and provisions to transfer obligation for information maintenance in case of cessation of operations.
- We interviewed the Digital Certifications Services Manager on the above.

Documents reviewed:

- Certificate Practice Statement & Policy
- Contract to transfer obligations to a reliable party for maintaining all information necessary to provide evidence of the operation of the TSP
- Procedure for the destruction of assets & related contract with reliable party

Interview(s):

- Eleftheria Theologou (Digital Certifications Services Manager)

v) Article 24.2 k

Relevant controls within supporting standards:

- [ETSI EN 319 411-1] Clause 6.1 (Publication and repository responsibilities)

Conformity statement:

We verified the conformity of the trust service provider with this article through a record review and interviews. We found the trust service provider to be in conformance with the article.

Activities performed:

We confirmed that the TSP maintains an updated certificate database.

We interviewed the Digital Certifications Services Manager on the above.

Review of record(s):

- Certificate Register (database)

Interview(s):

- Eleftheria Theologou (Digital Certifications Services Manager)

vi) Article 24.3

Relevant controls within supporting standards:

- [ETSI EN 319 411-1] Clause 6.2.4 (Identification and authentication for revocation requests)
- [ETSI EN 319 411-2] Clause 6.2.4 (Identification and authentication for revocation requests)
- [ETSI EN 319 411-1] Clause 6.3.9 (Certificate Revocation and Suspension)
- [ETSI EN 319 411-2] Clause 6.3.9 (Certificate Revocation and Suspension)

Conformity statement:

We verified the conformity of the trust service provider with this article through document review, record review and interviews. We found the trust service provider to be in conformance with the article.

Activities performed:

- We reviewed TSP documentation on suspension and revocation of certificates.
- We reviewed the timely execution after validation of the requesting entity and the registration in the certificate database of a suspension and a revocation (note that this refers to cases related to qualified certificates for eSignatures; as of now as of now no certificates have been issued to customers)
- We interviewed the Digital Certifications Services Manager on the above.

Documents reviewed:

- Certificate Practice Statement & Policy

Review of record(s):

- Suspension & Revocation requests
- Suspension & Revocation execution
- Platform audit
- Certificate Register (database)

Interview(s):

- Eleftheria Theologou (Digital Certifications Services Manager)

vii) Article 24.4

Relevant controls within supporting standards:

- [ETSI EN 319 411-1] Clause 6.3.10 (Certificate Status Services)
- [ETSI EN 319 411-1] Clause 6.6.2 (CRL profile)
- [ETSI EN 319 411-1] Clause 6.6.3 (OCSP profile)
- [ETSI EN 319 411-2] Clause 6.3.10 (Certificate Status Services)

Conformity statement:

We verified the conformity of the trust service provider with this article through document review and interviews. We found the trust service provider to be in conformance with the article.

Activities performed:

- We reviewed TSP documentation on the provision to provide to any relying party information on the validity or revocation status of qualified certificates issued by them. This information shall be made available at least on a per certificate basis at any time and beyond the validity period of the certificate in an automated manner that is reliable, free of charge and efficient.
- We reviewed CRL profiles and the OCSP mechanism and confirmed the above.
- We interviewed the Digital Certifications Services Manager on the above.

Documents reviewed:

- Certificate Practice Statement & Policy

Review of record(s):

- CRL profiles
- OCSP profiles

Interview(s):

- Eleftheria Theologou (Digital Certifications Services Manager)

6.2.2 Qualified certificates for website authentication

i) Article 28.1

Relevant controls within supporting standards:

- [ETSI EN 319 411-1] Clause 6.2.1 (Naming)
- [ETSI EN 319 411-2] Clause 6.6.1 (Certificate Profile)
- [ETSI EN 319 411-1] Clause 6.6.1 (Certificate Profile)
- [ETSI EN 319 412-1] Clause 4 (ETSI EN 319 412 certificate profiles)
- [ETSI EN 319 412-1] Clause 5 (Common data structures)
- [ETSI EN 319 412-2] Clause 4 (General certificate profile requirements)
- [ETSI EN 319 412-2] Clause 5 (EU Qualified Certificate requirements)
- [ETSI EN 319 412-3] Clause 4 (Profile requirements)
- [ETSI EN 319 412-5] Clause 4 (Qualified certificate statements)
- [ETSI EN 319 412-5] Clause 5 (Requirements on QCStatements in EU qualified certificates)

Conformity statement:

We verified the conformity of the trust service provider with this article through document review, record review and interviews. We found the trust service provider to be in conformance with the article.

Activities performed:

- We reviewed TSP documentation as to the requirements for qualified certificates for website authentication as per the regulation.
- We reviewed CA, subCA and subscriber certificates (this refers to a test certificate issued to test the profiling, extensions and QCStatements) as to the requirements.
- We interviewed the Digital Certifications Services Manager on the above.

Documents reviewed:

- Certificate Practice Statement & Policy

Review of record(s):

- Review of Certificate profiles (X.509)
- Review of CA, subCA and subscriber certificates (this refers to a test certificate issued to test the profiling, extensions)
- Review of Certificate QCStatements

Interview(s):

- Eleftheria Theologou (Digital Certifications Services Manager)

ii) Article 28.3

Relevant controls within supporting standards:

- [ETSI EN 319 411-1] Clause 6.2.1 (Naming)
- [ETSI EN 319 411-2] Clause 6.6.1 (Certificate Profile)

Conformity statement:

We verified the conformity of the trust service provider with this article through document review, and interviews. We found the trust service provider to be in conformance with the article.

Activities performed:

- We reviewed TSP documentation as to the requirements for Qualified certificates for electronic signatures as per the regulation.
- We reviewed CA, subCA and subscriber certificates (this refers to a test certificate issued to test the profiling, extensions and QCStatements) as to the requirements; No non-mandatory additional attributes are in place.
- We interviewed the Digital Certifications Services Manager on the above.

Documents reviewed:

- Certificate Practice Statement & Policy

Review of record(s):

- Review of Certificate profiles (X.509)
- Review of CA, subCA and subscriber certificates (this refers to a test certificate issued to test the profiling, extensions)
- Review of Certificate QCStatements

Interview(s):

- Eleftheria Theologou (Digital Certifications Services Manager)

iii) Article 28.4

Relevant controls within supporting standards:

- [ETSI EN 319 411-1] Clause 6.3.9 (Certificate Revocation and Suspension)
- [ETSI EN 319 411-2] Clause 6.3.9 (Certificate Revocation and Suspension)

Conformity statement:

We verified the conformity of the trust service provider with this article through document review, record review, observation and interviews. We found the trust service provider to be in conformance with the article.

Activities performed:

- We reviewed TSP documentation as to the permanence of the revoked status of certificates that have been revoked.
- We performed compliance testing via the certificate management application
- We interviewed the Digital Certifications Services Manager on the above.

Documents reviewed:

- Certificate Practice Statement & Policy

Review of record(s):

- Review and compliance testing via Certificate Management application

Observation(s):

- Review and compliance testing via Certificate Management application

Interview(s):

- Eleftheria Theologou (Digital Certifications Services Manager)

iv) Article 28.5 a,b

Relevant controls within supporting standards:

- [ETSI EN 319 411-1] Clause 6.2.4 (Identification and authentication for revocation requests)
- [ETSI EN 319 411-2] Clause 6.2.4 (Identification and authentication for revocation requests)
- [ETSI EN 319 411-1] Clause 6.3.9 (Certificate Revocation and Suspension)
- [ETSI EN 319 411-2] Clause 6.3.9 (Certificate Revocation and Suspension)

Conformity statement:

We verified the conformity of the trust service provider with this article through document review, observation and interviews. We found the trust service provider to be in conformance with the article.

Activities performed:

- We reviewed TSP documentation on suspension of certificates.
- We performed compliance testing on a suspended certificate validity and the OCSP response.

  Moreover, we reviewed the period of suspension for a subscriber certificate on the certificate database.
- We interviewed the Digital Certifications Services Manager on the above.

Documents reviewed:

- Certificate Practice Statement & Policy

Review of record(s):

- Review and compliance testing of suspended certificate

- Review of suspension period in certificate register (database)
- Platform audit

Documents reviewed:

- Certificate Practice Statement & Policy

Review of record(s):

- Review and compliance testing via Certificate Management application
- Review of Certificate Register

Observation(s):

- Review and compliance testing via Certificate Management application

Interview(s):

- Eleftheria Theologou (Digital Certifications Services Manager)

v) Article 45.1

Relevant controls within supporting standards:

- [ETSI EN 319 411-1] Clause 6.5 (Technical security controls)
- [ETSI EN 319 411-2] Clause 6.5 (Technical security controls)
- [ETSI EN 319 411-1] Clause 6.6 (Certificate, CRL, and OCSP Profiles)
- [ETSI EN 319 411-2] Clause 6.6 (Certificate, CRL, and OCSP Profiles)
- [ETSI EN 319 412-1] Clause 4 (ETSI EN 319 412 certificate profiles)
- [ETSI EN 319 412-1] Clause 5 (Common data structures)
- [ETSI EN 319 412-2] Clause 4 (General certificate profile requirements)
- [ETSI EN 319 412-2] Clause 5 (EU Qualified Certificate requirements)
- [ETSI EN 319 412-3] Clause 4 (Profile requirements)
- [ETSI EN 319 412-5] Clause 4 (Qualified certificate statements)
- [ETSI EN 319 412-5] Clause 5 (Requirements on QCStatements in EU qualified certificates)

Conformity statement:

We verified the conformity of the trust service provider with this article through document review, record review and interviews. We found the trust service provider to be in conformance with the article.

Activities performed:

- We reviewed TSP documentation as to the requirements for qualified certificates for website authentication as per the requirements on Annex IV of the regulation.
- We reviewed cryptographic device certifications, the ceremonies of CA and subCAs, technical measures of the cryptographic functions, certificate and CRL profiling and the OCSP service.

  We reviewed CA, subCA and subscriber certificates (this refers to a test certificate issued to test the profiling, extensions) as per the requirements of the regulation.
- We interviewed the Digital Certifications Services Manager on the above.

Documents reviewed:

- Certificate Practice Statement & Policy
- Information Security Policy
- Athens Stock Exchange cryptography standards
- Ceremony of CA and subCAs

Review of record(s):

- Cryptographic units, algorithms, key sizes, validity periods
- X.509 Certificates (CA, subCAs, Subscribers) specifications including QCStatements
- Review of Certificate profiles (X.509)
- Review of CA, subCA and subscriber certificates (this refers to a test certificate issued to test the profiling, extensions)
- Review of Certificate QCStatements
- CRLs specifications
- OCSP service

Interview(s):

- Eleftheria Theologou (Digital Certifications Services Manager)

7 Appendices

7.1 Appendix A – Trust service hierarchy

ATHEX Root CA G2

Name of "Service digital identifier" (as in "Service digital identifier" certificate)	**Certificate serial number (as in "Service digital identifier" certificate)**
ATHENS STOCK EXCHANGE	3e cf
Subject Key Identifier (as in "Service digital identifier" certificate)	
47 a3 a6 04 9d 2d 96 e5	
Base 64 PEM representation	
-----BEGIN CERTIFICATE----- MIIFPzCCAyegAwIBAgICPs8wDQYJKoZIhvcNAQEMBQAwSDELMAkGA1UEBhMCR1Ix HjAcBgNVBAoTFUFUSEVOUyBTVE9DSyBFWENIQU5HRTEZMBcGA1UEAxMQQVRIRVgg Um9vdCBDQSBHMjAeFw0xNjAzMTUxMTE0MzJaFw0zNjAzMTQyMjAwMDBaMEgxCzAJ BgNVBAYTAkdSMR4wHAYDVQQKExVBVEhFTlMgU1RPQ0sgRVhDSEFOR0UxGTAXBgNV BAMTEEFUSEVYIFJvb3QgQ0EgRzIwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIK AoICAQCv8F+SyvwcsJAt1CaLvyqZeTbHdIwB76G9cvg0hMwtTdfrk5HLCYO2+tRl M12cmBtew+bgQENIZ2OlcKvlqxZgtqsUezqjbvUZbyrEdKBZdJT2ntf8Mn8M+a8U UbiPWrjVdg6n/XEKPgv8EFJL78LEH1Kh8eXpsRAyrKluW68rt4DJUStKA+w//fBT LO++WqbEAfCcBO3g+n1GvxE36w+BrDoZhwed+F5YqP9jvHB1puCrMdGzgoY2aaOx atU2RdWf8IWKCkUOC0GxEZqx7MAmbUuIN1/sFlOF570+ZZ1K0geHbYaDWLplGcww ldusUvq2zH5uHbmwgFV5U1wNCFZTUrfkl4NjarnSH7xqlREiVhzoPRmEzlmGKtEG JxLbRyukp7DD+B68/qw/sp7csCLFT3Bh0/4o4RUZLHg8P8N9mWA2eW5byThmoaXp LYHGUqyezxteyybZ7dQF7VcmdqQC4zbkTkV+NGcY//wUKPX2vANOvIjLegkorQHj cOi5O1WNEMiUJAduG5pyxAsY+21rZXlv6L2MFaDkoBUU6TvJXfph4nnDCzNKBQ9B UQm8YoB3V+C0uxiSBe2OVCHd9YcYHGqosgJqQoxD1R4fZ+HV3QBjj+ALf0GUYQaW fACPoN9TGUe8VDLZGwu+jp89TNygUzyV2FHZp7idkbyDyPHkgQIDAQABozMwMTAP BgNVHRMBAf8EBTADAQH/MBEGA1UdDgQKBAhHo6YEnS2W5TALBgNVHQ8EBAMCAQYw DQYJKoZIhvcNAQEMBQADggIBAIbX9Rko9qewUKpuPSM+Bu/nNHusyYUusKmiwn0k RT+tyNaTJ7XKjyygBDiD2ZrP7Ics7LEJE7LOfCQbZ+BEgszipWRLSzVsZ0Jvc7w4 uX7ARMh1/AVxp/udBcLlJdkssXVntDH3uiUMjp3JfGxK/HUFYKTNz7ufjl+dsiBA S2tuHacQHu+/YA/LN/1Ml/pi431dgM2ubMfmp6STGHcfU9Z9qf914yTgT8uiYedm PtS0Ch0MFY46hQbG72xy/dRD0/2MqEOBWTjBhnwgh46oJlpGxAWtbaDVWBBTmZTy rlosVqZSSkw3OVW8wviueay5NoVuYVI+/TTqYWhlgYFM2xT5YI0EdQ8Q30PTJcdA X5vk0DB92gZB9O1m/jgRcyBZ2YB7FeFC1zqebGVfMXahE2XaJzuwEuisSLaZEQd+ LspikapRYfRnyit50o8hWl8WcI5UmJ/281kBba61pBJzn4KfF5/a7YOPl/1izjbe A8HRMKbTou+rXXV699ccLPfZ6WY6l5QpUNv8AgNf8jDXUTKcxC+dStkx8TUPfoOq HeK1xlFBa1ctIhmPO6cjuwN1nrv8+SCHzHBfjiBwLzo+Yg1f0uE2nUbWVbKYCi6c wFXS+x56a0p2KSYS9q+kp7ztMqFw0/mNiweBpX0GwI3xNb62YLJvHiOikcr5YI3m 6JPv -----END CERTIFICATE-----	

Athex SSL Certificates CA G2

Name of "Service digital identifier" (as in "Service digital identifier" certificate)	Certificate serial number (as in "Service digital identifier" certificate)
ATHEX SSL Certificates CA G2	3e f8
Subject Key Identifier (as in "Service digital identifier" certificate)	
4c cd 5b ec 9a 03 92 2f	
Base 64 PEM representation	
-----BEGIN CERTIFICATE----- MIIFljCCA36gAwIBAgICPvgwDQYJKoZIhvcNAQELBQAwSDELMAkGA1UEBhMCR1Ix HjAcBgNVBAoTFUFUSEVOUyBTVE9DSyBFWENIQU5HRTEZMBcGA1UEAxMQQVRIRVgg Um9vdCBDQSBHMjAeFw0xNjAzMzAwODQ1MTdaFw0yNjAzMjkyMTAwMDBaMFQxCzAJ BgNVBAYTAkdSMR4wHAYDVQQKExVBVEhFTlMgU1RPQ0sgRVhDSEFOR0UxJTAjBgNV BAMTHEFUSEVYIFNTTCBDZXJ0aWZpY2F0ZXMgQ0EgRzIwggEiMA0GCSqGSIb3DQEB AQUAA4IBDwAwggEKAoIBAQDBGs9Qo9jgWXyrpGjMQm5BrxrD9oJ6agfukVZCD27q 3MkEJNrvnWJWmT1F0Y+JQ8Zhyda6vARjiV5OKtRK3Q9ufw1XT6VPWujqgujgrEKt HblZnwWfgbPlD6pfcw4YC8rsRqYR3fBhYVuzOSlsBCvchQgml3o7iOqdiZjDLjtv 2kSGE9V5FazVjfe9b6BPnUM6fC790ClRZKBfcKrgAt6fE4VmK9N85Zelm24Sjk5n vjA/SCm58rtSKAsEnFzRfUyz5DNm3UFFEPmQsQMOl/Kn6b3YAQIMGvG/HGfyrQ3Z lDkrPPt9eV7EzlzskhLKB+o4sLZRSu0Fueq4MjuJOMZ/AgMBAAGjggF8MIIBeDAP BgNVHRMBAf8EBTADAQH/MBEGA1UdDgQKBAhMzVvsmgOSLzBmBgNVHSAEXzBdMFsG BFUdIAAwUzBRBggrBgEFBQcCARZFaHR0cDovL3d3dy5oZWxleC5nci9lbC93ZWIv Z3Vlc3QvZGlnaXRhbC1jZXJ0aWZpY2F0ZXMtcGtpLXJlZ3VsYXRpb25zMBMGA1Ud IwQMMAqACEejpgSdLZblMIGBBggrBgEFBQcBAQR1MHMwMwYIKwYBBQUHMAGGJ2h0 dHA6Ly9vY3NwLmF0aGV4Z3JvdXAuZ3IvQXRoZXhSb290Q0FHMjA8BggrBgEFBQcw AoYwaHR0cDovL3d3dy5oZWxleC5nci9wa2kvLS9maWxlL0F0aGV4Um9vdENBRzIu Y3J0MA4GA1UdDwEB/wQEAwIBhjBBBgNVHR8EOjA4MDagNKAyhjBodHRwOi8vd3d3 LmhlbGV4LmdyL3BraS8tL2ZpbGUvQXRoZXhSb290Q0FHMi5jcmwwDQYJKoZIhvcN AQELBQADggIBAKztJlxHHFT1lhWmdB1CfPystG/3UqtKecHF4WZYX/NuHcGCJtgU enTIIT9/p9VTRej7JwKFu6F372SQExXrva3JZr5Pp3qAkiLGt+Z7YisaQDG/DoWj PEF+45y8+nMT1V7d9BOLtohE8KYyBTgOT3yua6w2rDYExb+48kpAX13zBisNjN0F 5IDZAyTgGnB8Tt19ZEnEWssoPo41CYTxqpB1rWFTMQCsLnPHzVdibxm33tyWxlOr djvWTFNi4o6ga4zrejJqTFtC82i8BcGozO+z2x1bbm2rR5JheVUVzH1W4Y4OyUXj z+Qzy0b62rmnjFOtHhI9yKEAqToqVYDF/VyMlBI8dqdJBOl7MXzicdXsxKbtko8A WleaoaUSgbkbunhPeGji2AMxohch82dA9VuxA0wxv7Gz/n12lYhZOjhnQlBK5+9Z R3q5DMcioYSvMw/V8t/PJF7POoxtjsb0uN7vQ9xTAg/5cVDoRFCOT3c5YlvMta5j bfq4v425RxIuo/mZ6AmAh95M/lkTZba+if/gQtJQMY4DmuHTu0jn0r90qN0uAgVs YxO4vt6L220PrRW0f9h1D7BhQ1lmWdtjpuBNrux/w5V8FbR+EawsYJvr7b++NGMz yKRz7uhl031qDGOidXoELs3Yqj7laf4MeR4nUjT5XfUSZvAQTZYNiORe -----END CERTIFICATE-----	

7.2 Appendix B – Classification of identified findings

Guidance for the classification of findings is as follows:

1. Major non conformity - an absence of, or the repeated failure to implement and maintain one or more required mandatory standard element, or a situation which would, on the basis of objective evidence, raise significant doubt as to the capability of the trust service provider to achieve its objectives.

2. Minor non conformity - a single identified gap or a concern in meeting a requirement of the regulation, which would not in itself raise significant doubt as to the capability of the trust service provider to achieve its objectives.

3. Opportunity for improvement - information on situations that management is well advised to consider, whereas although formal compliance to the requirements of the regulation is adequately met, based on conformity assessment experience and knowledge and illustrative controls provided in the regulation-supporting standards, additional effectiveness or robustness might be possible with a modified approach to prevent a potential non-conformity in the future.