Independent Assurance Report on PKI CA Key Generation Ceremony

Athens Exchange S.A.

ERNST & YOUNG

Athens Exchange S.A.

Executive Summary

PKI Certification Authority (CA)
Key Generation Ceremony for the ATHEX Root CA

ATHEX Root CA Thumbprint
DB2B 7B43 4DFB 7FC1 CB59 26EC 5D95 21FE 350F F279

We have reviewed Athens Exchange S.A. management's assertions accompanying this report regarding generating and protecting its Certification Authority ('CA') keys, ATHEX Root CA, ATHEX General Certificates CA and ATHEX Qualified Certificates CA on October 18, October 19, 2010.

Based on our work described in this report, nothing has come to our attention that causes us to believe that the management's assertions on Root Key Ceremony Process controls are not fairly stated in all material respects based on the criteria mentioned in the following report. Furthermore, nothing has come to our attention that causes us to believe that the procedures we observed during the CA key generation process for the ATHEX Root CA, ATHEX General Certificates CA and ATHEX Qualified Certificates CA on October 18, October 19, 2010, have not complied, in all material respects, with the ATHEX Root Key Generation Ceremony Script, version 1.0, dated October 18, 2010, AICPA/CICA WebTrustSM/TM Program for Certification Authorities (http://www.aicpa.org or http://www.cica.ca), relevant aspects of the Internet Engineering Task Force (IETF) PKIX framework - RFC 2527 (http://www.ietf.org) and relevant aspects of the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework - RFC 3647, which obsoletes RFC 2527

This report is intended solely for the information and use of ATHEX's management, regarding the procedures performed by ATHEX on October 18 and October 19 2010 to generate the CA keys for the indicated CAs with the thumbprints above, and is not intended to be and should not be used by anyone other than these specified parties

October 20, 2010

Athens, Greece

ERNST & YOUNG

Quality In Everything We Do

ERNST & YOUNG
Business Advisory Solutions S.A.
11th Km National Road Athens-Lamia
144 51 Athens, Greece

Tel: +30 210.2886.000
Fax: +30 210.2886.901
www.ey.com

20th October, 2010

Athens Exchange S.A.
108, Athinon Ave.
10442, Athens
Greece

To The Management of Athens Exchange S.A.:

We have reviewed Athens Exchange S.A. (hereinafter ATHEX S.A. or just ATHEX) management's assertions accompanying this report that, in generating and protecting its Certification Authority ('CA') keys, ATHEX Root CA, ATHEX General Certificates CA and ATHEX Qualified Certificates CA on October 18, October 19, 2010, ATHEX:

- documented its CA key generation and protection procedures in its Certificate Policy and Certification Practice Statement (CP/CPS) for the indicated CAs, respectively, final version 1.0, dated October 18, 2010;
- included appropriate detailed procedures and controls in its Root Key Generation Ceremony Script for the indicated CAs, final version 1.0, dated October 18 2010;
- maintained effective controls to provide reasonable assurance that the indicated CA keys were generated and protected in conformity with the procedures described in its above-mentioned CP and CPS and with its Root Key Generation Ceremony Script; and
- performed, during the Root Key Generation Process, all the procedures required by its Root Key Generation Ceremony Script

based on relevant aspects of the AICPA/CICA WebTrust$^{SM/TM}$ Program for Certification Authorities (http://www.aicpa.org or http://www.cica.ca), relevant aspects of the Internet Engineering Task Force (IETF) PKIX framework - RFC 2527 (http://www.ietf.org) and relevant aspects of the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework - RFC 3647, which obsoletes RFC 2527.

ATHEX's management is responsible for its assertions. Our responsibility is to express a conclusion on management's assertions based on our review.

Our work was performed in accordance with standards for assurance engagements other than Audits or Reviews of Historical Financial Information established by the International Federation of Accountants (ISAE3000). Those standards require that we plan and perform our work to obtain limited assurance that nothing has come to our attention regarding ATHEX's management's assertion that Root Key Generation Process controls are not effective, in all material aspects, based on the aforementioned criteria. Our work included:

- obtaining an understanding of ATHEX's documented plan of procedures to be performed for the generation of the certification authority key pairs for the indicated CAs,
- examining the CA key generation script for design effectiveness,
- testing and evaluating, during the CA key generation process, the effectiveness of controls over the integrity, confidentiality and availability of all private keys (including back-up copies), and access keys (physical keys, tokens, passwords and PINs) used in the Root Key Ceremony Procedure, and

ERNST & YOUNG
Business Advisory Solutions S.A.
11th Km National Road Athens-Lamia
144 51 Athens, Greece

Tel: +30 210.2886.000
Fax: +30 210.2886.908
www.ey.com

- physical observation of all procedures performed during the CA key generation process to ensure that the procedures actually performed on October 18 and October 19, 2010 were in accordance with the Root Key Generation Ceremony Script for the indicated CAs.

Based on our work described in this report, nothing has come to our attention that causes us to believe that the management's assertions on Root Key Ceremony Process controls are not fairly stated in all material respects based on the aforementioned criteria. Furthermore, nothing has come to our attention that causes us to believe that the procedures we observed during the CA key generation process for the ATHEX Root CA, ATHEX General Certificates CA and ATHEX Qualified Certificates CA on October 18, October 19, 2010, have not complied, in all material respects, with the ATHEX Root Key Generation Ceremony Script, final version 1.0, dated October 18, 2010, AICPA/CICA WebTrustSM/TM Program for Certification Authorities (http://www.aicpa.org or http://www.cica.ca), relevant aspects of the Internet Engineering Task Force (IETF) PKIX framework - RFC 2527 (http://www.ietf.org) and relevant aspects of the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework - RFC 3647, which obsoletes RFC 2527.

Because of inherent limitations in controls, error or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that the validity of such conclusions may be altered because of:

- changes made to the systems or controls,
- changes in processing requirements,
- changes required because of the passage of time,
- deterioration in the degree of compliance with the policies or procedures.

The following Distinguished Names (DN) and fingerprints of the CA public keys were generated under our direct observation:

CN=ATHEX Root CA, OU=Root CA O=Athens Exchange S.A. C=GR Thumbprint (SHA-1)= DB2B 7B43 4DFB 7FC1 CB59 26EC 5D95 21FE 350F F279

CN=ATHEX General Certificates CA, OU=General Certificates CA O=Athens Exchange S.A. C=GR Thumbprint (SHA-1)= 9C72 BB4D 9C02 D71E 2E98 F43F E290 C277 4A87 531B

CN=ATHEX Qualified Certificates CA, OU=Qualified Certificates CA O=Athens Exchange S.A. C=GR Thumbprint (SHA-1)= 04A2 838B 617A 3178 FFA4 4ADA 7CA2 7343 34F7 3F31

This report is intended solely for the information and use of ATHEX's management, regarding the procedures performed by ATHEX on October 18 and October 19 2010 to generate the CA keys for the indicated CAs with the thumbprints above, and is not intended to be and should not be used by anyone other than these specified parties.

ERNST KAI ΓΙΑΝΓΚ Ανώνυμη Εταιρεία
Παροχής Συμβουλευτικών Υπηρεσιών
Επίσημη Μετάφραση

GEORGIOS PAPADIMITRIOU

ERNST & YOUNG
Quality In Everything We Do

ERNST & YOUNG
Business Advisory Solutions S.A.
11th Km National Road Athens-Lamia
144 51 Athens, Greece

Tel: +30 210.2886.000
Fax: +30 210.2886.901
www.ey.com

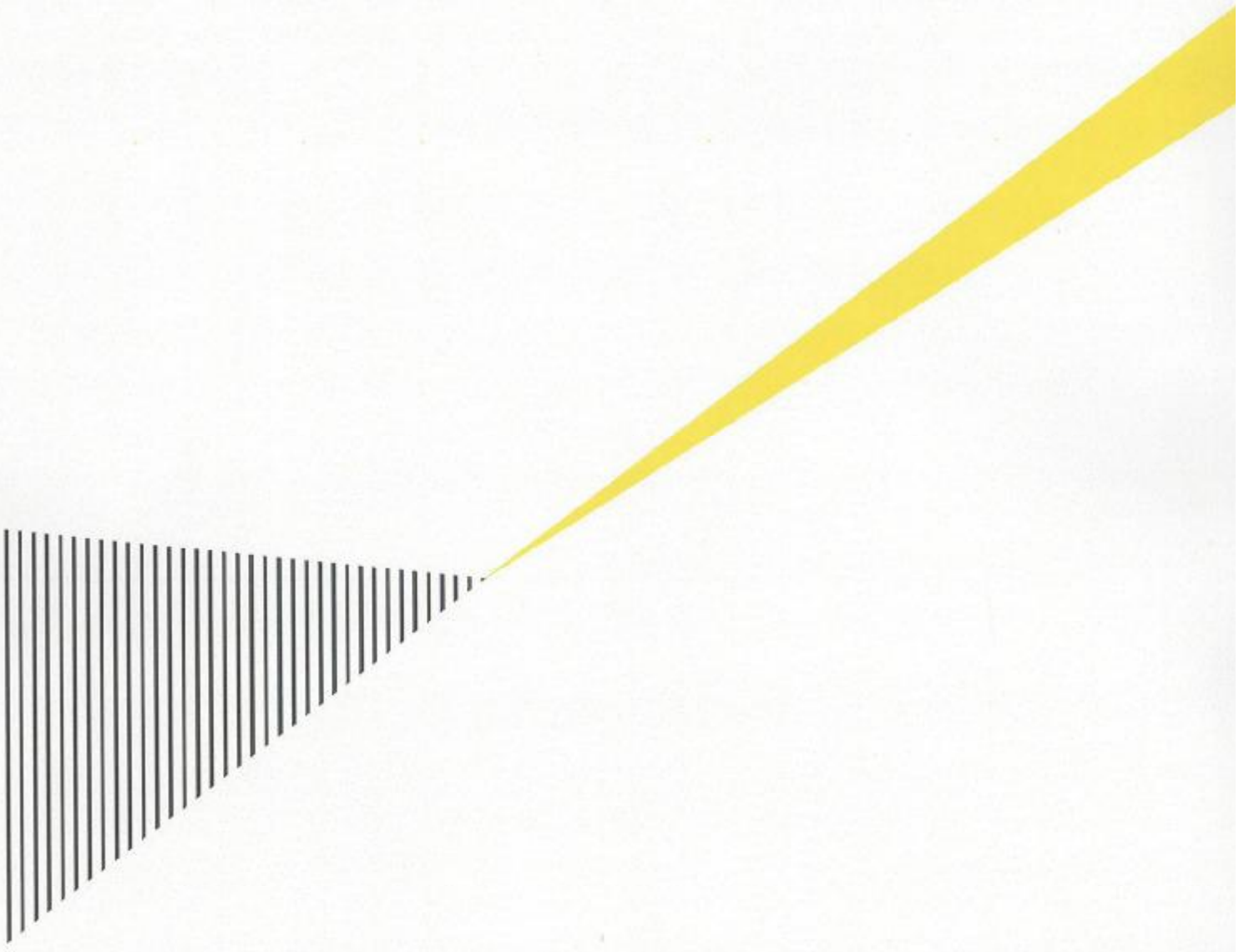
Management Assertions on Root Key Ceremony Process controls

Root Key Generation Environment

- The computer hardware platform was built under audit observation starting from sealed clean equipment or auditable equivalent.
- All software components were loaded from shrink-wrap or certified equivalent.
- Commercially available CA software, which has been independently verified for FIPS/RSA compliance or equivalent, was used.
- Configuration network was detached during the duration of key generation process.
- The environment under audit included all software components (e.g., operating system, databases, CA software, and directory software).
- The environment built process was totally scripted to the key-stroke level of detail.
- The environment was built (loaded) under audit presence or auditable equivalent.
- Detailed records of the process, participants and access were maintained (e.g., detailed access logs to the room, process videotaped, etc.).
- The process occurred in an appropriately secured physical facility.
- All participants prior to entering the room delivered all electronic devices under their procession.

Root Key Generation Procedures

- The CP/CPS components relating to root key matters were complete.
- The detailed script of procedures was prepared to the key-stroke level of detail.
- The network was detached during the duration of key generation process.
- The entire process was performed under audit presence or auditable equivalent.
- Detailed records of the process, participants and access were maintained (e.g., script steps signed off, process videotaped, etc.).
- The process occurred in an appropriately secured physical facility.
- All crypto material and key components was placed under appropriate pre-defined and audit-reviewed split custody.
- The duplication of private keys (cloning) for disaster recovery procedures as stated in the CPS was performed as part of the ceremony.
- The ceremony included production of a self-signed certificate containing the CA public root key.
- The ceremony incorporated secure storage under split-custody safekeeping of all private keys generated.
- All cryptographic material was secured in appropriate split-custody safekeeping.



ERNST & YOUNG