Consultation procedure on Electronic Signatures regarding issues relevant to the Provision of Certification Services and Voluntary Accreditation.

NOTE

The present document was constructed by the National Telecommunications and Post Commission concerning the regulatory framework as regards the provision of certificate services and voluntary accreditation.

EETT invites all interested parties to express their opinions by answering the questions of the present text, notifying distinctly the number of the question to which each answer is referred. Answers have to be comprehensive, explicit and all opinions must be adequately substantiated. The interested parties are not obliged to respond to the entire questioner.

The outcome of the present proceeding on subject opinions is not binding to EETT as regards the regulations that will be adopted.

Any anonymous answer shall not be considered. Submitted answers shall be under indication: «Subject Opinions on issues relevant to the provision of certification service and voluntary accreditation.»

All answers have to be submitted undersigned, written in Greek, in printed and in electronic form until Friday, November 30, 2001, to the following address:

Post address:

Ref: «Consultation procedure on Electronic Signatures regarding issues relevant to the Provision of Certification Services and Voluntary Accreditation.»
National Telecommunications and Post Commission
60, Kifissias Avenue
GR-151 25 Maroussi

E-mail:

esign@eett.gr

Consultation procedure on Electronic Signatures regarding issues relevant to the Provision of Certification Services and Voluntary Accreditation.

INTRODUCTION

With the Presidential Decree 150/2001 «Implementation of Directive 99/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures» (Official Government Gazette125/A/2001) the provisions of the Directive 99/93/EC of the European Parliament and of the Community 13th December 1999 «on a Community framework for electronic signatures » (EEL 13/19.1.2000) was implemented to the Greek legislation.

EETT, within the framework of its responsibilities, deriving from the Presidential Decree150/2001 intends to issue Regulation on:

- The procedure, the terms and the conditions on voluntary accreditation for certification-service providers.
- Conformity Assessment of secure signature-creation-devices with the requirements laid down in Annex III to the Presidential Decree 150/2001.
- The supervision and inspection of certification-service providers established in Greece and the bodies designated by EETT as responsible for the conformity assessment of secure signature-creation-device with the requirements laid down in Annex III to the Presidential Decree 150/2001.

On the occasion of issuing the Regulation and in order to meet in the most effective way the demands created in Greece from the development of certification-service market, EETT raises public consultation on specific issues for which the opinion and expertise of the market is considered to be particularly constructive.

I. PROVISION OF CERTIFICATION SERVICES-QUALIFIED CERTIFICATES

REVOCATION – WITHDRAWAL OF CERTIFICATES

In order to ensure the safety of business transaction, EETT considers that there must be specific cases of revocation or withdrawal of qualified certifications. In particular:

The certification-service provider is obliged to proceed to direct withdrawal / revocation of a qualified certificate, in the following cases:

a. upon a request of the owner of the signature-creation data or other person legally authorized by him,
b. in case it has been proven by EETT that the qualified certificates contain false and inaccurate information with regard to Annex I to the Presidential Decree 150/2001,
c. in case that the certification-service provider ceases his operation

Question 1: Word your comments.
Do you consider that the Regulation that EETT intends to issue should include other cases for which the withdrawal – revocation of a certificate is necessary?

Cessation of provision of Certification-Services

EETT considers that, in case the certification-service provider ceases his operations; specific procedures should be provided for, ensuring that the qualified certificates will be taken over by another certification-service provider. In particular:

Before the cessation of the operations, for whatever reason, or if this is not objectively possible soon after its cessation, the certification-service provider is under the obligation to:

(a) report to EETT the cessation of his operations without delay,

(b) inform directly and in writing the owners of the certificates that he ceases his operation and that they may choose either their certificates that he had created and are still valid to be taken over by another certification-service provider of owner's choice, or if there is no such choice, by another certification-service provider of provider's choice. In case the voluntary accredited certification-service provider ceases his operation then the certificates are taken over by another voluntary accredited certification-service provider. In case of cessation of operations of the certification-service provider who issues qualified certificates, then the qualified certificates shall be taken over by another certification-service provider

also issuing qualified certificates, or by a voluntary accredited certification-service provider.

(c) to hand over all relevant document and evidences of his record to certification-service provider, which shall take over the certificates, according to the aforementioned under (b).

(d) to proceed in case that the aforementioned under (b) shall not apply, to the direct revocation of the certificates in question, and submit all the documents and evidences of his record to be kept by EETT informing the contracting parties.

Question 2: Do you agree with the above approach in case of cessation of operations by the certification-service provider?
Do you believe that there are technical or other difficulties for the implementation of the above procedure?
Do you believe that there is another alternative procedure and if yes, which?

II. Voluntary Accreditation of Certification-service Providers

Requirements for the Voluntary Accreditation

With the voluntary accreditation it is accredited that the certification-service provider fulfils the requirements laid down in the Presidential Decree 150/2001 and in particular:

(a) he fulfils the requirements for issuing qualified certificates and the certificates that he issues are qualified, and
(b) he uses only secure-signature-creation device,

The above laid down a) and b) are the requirements for assignment of the voluntary accreditation, however the certification-service provider is allowed to issue non-qualified certificates. In such case the user shall be informed whether the certificate issued on his account is qualified or not.

Question 3: Do you agree with the above requirements?
What is in your opinion the procedure that should be followed in order to put the above distinction between the non-qualified certificate and the qualified certificate into practice?

EETT as the Root of Certification Authority of the Voluntary Accredited Certification-Service Providers

Voluntary Accreditation scheme aims at securing and an enhanced level of certification-service provision of service.

For the certification of authenticity of the signature-verification data, it is necessary to locate a full certification path so as the forwarder who wishes to send a secure message to an individual who is certificated by another certification-service provider, is able to verify the identity of all the certifications-service providers that intervene before the receiver. This necessitates the development of confidence relationship through the establishment of confidence model.

EETT believes that a possible organization structure of the certification-services providers is also the implementation of a Root Certification Authority model, where the voluntary accreditation providers shall be under a recognized authority, which is the Root Certification Authority. The confidence among the members of the Root Certification Authority shall be gained through the procedure of the voluntary accreditation. In such a case, EETT, apart from the awarding of voluntary accreditation, may undertake to operate us the Root Certification Authority certifying the public keys of the voluntary accredited providers and issuing their certifications. The voluntary accredited providers, in their turn, will certify the keys of their subscribers. The issue of qualified certificates by EETT shall be a significant factor in the process of ensuring the security of the certification system.

Question 4: Do you agree with the function of EETT, as the Root Certification Authority of the voluntary accredited?
In case that EETT proceeds to the implementation of the above-mentioned function, do you believe that EETT should create the signature-creation data and signature-verification device of the voluntary accredited?

Evaluation of Applications for Voluntary Accreditation by Bodies other than EETT – Designation of Bodies

During the evaluation of the file submitted by the provider requesting voluntary accreditation, EETT shall evaluate the providers' conformity to the conditions of the voluntary accreditation. According to the Presidential Decree 150/2001, EETT may designate public or/and private bodies, for the project in question. In this case, EETT shall designate bodies that fulfil the requirements with which it shall be ensured that they provide the sufficient technical competence and adequate experience for the performance of the above evaluation.

EETT shall draw up a catalogue with all the aforementioned designated bodies. The provider may choose from the catalogue the designated which he wishes to evaluate his file.

The person who applies for the voluntary accreditation shall submit the application file to EETT. Following that and after the implementation of the application evaluation is concluded, the designated body shall submit to EETT a report regarding the provider's conformity to the conditions of voluntary accreditation based on which EETT shall issue the relevant decision.

Question 5: do you agree with the implementation of such a scheme for the evaluation of the application for the voluntary accreditation?
What do you believe that should be the criteria with which EETT shall choose the competent authorities and how do you believe the relevant procedure should be organized?
Would you be interested in undertaking such an activity? And if yes, on what conditions?
Who do you believe that must be charged with the cost of the evaluation of the applications for voluntary accreditation?
Would you give a differed answer if the evaluation performed by EETT or by a third body? If yes, how?

Issue of Qualified Certificates only in conditions of secure signature-creation device

EETT is intended to impose on the voluntary accredited the obligation of issue qualified certificates to natural or legal persons only when they use secure signature-creation device for storing of signature-creation data and for the creation of their digital signature

Question 6: Express your opinions. Do you agree that the voluntary accredited certification-service provider should issue qualified certificates for natural or legal person only when they use secure signature-creation device for storing signature-creation data and for the creation of their digital signature?
Do you believe that the imposition of such obligation might cause problems? If yes, what are they?

Specification of Conditions for Voluntary Accreditation

Annex II of the Presidential Decree 150/2001, includes a number of conditions (technical, economical etc.) which must be fulfilled by the provider who issues qualified certification. Within the framework of the assignment of voluntary accreditation, EETT or the bodies designated by it –should that happened- shall assess the conformity of the applicant for the voluntary accreditation to

the Annex II. In many cases the conditions included to Annex II are of general nature and the way with which the provider requesting voluntary accreditation will prove its conformity to them is not clear.

Question 7: In your point of view what are the evidences that the provider has to submit in order to prove his conformity to the criteria of Annex II to Presidential Decree 150/2001?
Do you consider that the conformity to other evidences must be required? And if yes, with what;

III. PRODUCTS FOR ELECTRONIC SIGNATURE

Appointment of Authority for the Conformity Assessment of Secure-Signature-creation Device

According to the Presidential Decree 150/2001, the conformity assessment of secure-signature-creation device shall be determined by appropriate public or private bodies designated by EETT, are proved to dispose the required professional reliability, impartiality (including the necessary technical and equipment infrastructure) for the implementation of the project.

EETT intends to form a catalogue with the public or private designated bodies. As regards the conformity assessment of secure-signature-creation device to Annex III to the Presidential Decree 150/2001, each interested party shall submit an application to EETT, choosing from the catalogue the designated body, which will be responsible for the performance of his conformity assessment. The designated body shall report to EETT the conformity or not of secure-signature-creation device to Annex III to the Presidential Decree 150/2001 and EETT shall issue the relevant decision (Accreditation Act).

Question 8: Do you believe that there are in Greece bodies that would be appropriate for this role, and if yes, who could be?
Which would be in your opinion the procedure for the conformity assessment to Annex III to the Presidential Decree150/2001?

Suggested Standards for the Secure-Signature-creation Device

Provided that numbers of generally recognized standards for electronic signature products are published in the Official Journal of the European Communities, according to article 3 paragraph 5 and article 9 of Directive 99/33/EC (EE L 013, 19/01/2000, p. 12-20), the conformity of an electronic

signature product to the above standards is a presumption of conformity to the requirements determined in point (f) to Annex II and Annex III to the Presidential Decree 150/2001.

Regarding the secure-signature-creation device, in case of non-publication of reference numbers of generally recognized standards, it is suggested that the conformity to the following standards should presume the conformity to the conditions to Annex III to the Presidential Decree 150/2001.

a) *CEN/ISSS WS/E-Sign "Security Requirements for Signature Creation Systems".*

b) *Common Criteria for Information Technology security evaluation ISO/IEC 15408: Information Technology – Security Techniques- Evaluation Criteria for IT security at least EAL 4.*

c) *Information Technology Security Evaluation Criteria- ITSEC Evaluation at least E 3*

In case that the products are used within specially secured area then the evaluation will cover at least evaluation level EAL3 or E2.

d) *FIPS PUB 140-1 level 2 "Security Requirements For Cryptographic Modules".*

Question 9: Do you agree with standards suggested by EETT for secure-signature-creation device? Do you have any suggestion on other supplementary standards?

Suggested Standards for the Use of Reliable Systems and Products

Regarding the use of reliable systems and products it is suggested that the conformity to the following standards should presume conformity to point f to Annex II to the Presidential Decree150/2001

a) *Common Criteria for Information Technology security evaluation ISO/IEC 15408: Information Technology – Security Techniques- Evaluation Criteria for IT security at least EAL 4 or,*
b) *Information Technology Security Evaluation Criteria- ITSEC Evaluation at least E 3*
In case that the products are used within specially secured area then the evaluation will cover at least evaluation level EAL3 or E2.
or
c) *FIPS PUB 140-1 level 2 "Security Requirements For Cryptographic Modules" or,*
d) *CEN/ISSS WS/E-Sign "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures"*

Hash algorithms

a) SHA-1 FIPS PUB 180-1: Secure Hash Standard or,
b) RIPEMD ISO/IEC10118-3: IT – Security techniques Hash-Functions Part 3: Dedicated Hash -Functions

Signature Algorithms

a) PKCS#1 RSA Encryption Standard or,
b) DSA FIPS PUB 186-1: Digital Signature Standard, or
c) DSA variants, based on elliptic curves:
ISO/IEC 148883-3 :IT –Security Techniques- Digital signatures with appendix – Part3. or
IEEE – Standard P1363 Section 5.3.3. or
IEEE – Standard P1363 Section 5.3.4.

The above hash and signature algorithms are considered to be secure until 2006. This date may be modified due to technology development.

Question 10: Do you agree with standards suggested by EETT for the reliable systems and products? Would you like to suggest any other supplementary standard?

IV. SUPERVISION AND CONTROL OF CERTIFICATION-SERVICE PROVIDERS ESTABLISHED IN GREECE AND OF BODIES DESIGNATED BY EETT

Object and Content of Supervision and Control

The provision of certification-service is free and it is not subject to previous approval. According to the Presidential Decree 150/2001, EETT supervises and inspects the certification-service providers established in Greece. Within this framework, it is suggested that all certification-service provider are obliged to notify their operation and their services to EETT. In cases that ex-officio or upon a complaint there is a proven violation of the provisions of the legislation in force EETT as supervision authority shall act repressively.

Question 11: Do you agree with that supervision and control scheme? Do you believe that it should be stricter?

Furthermore, EETT supervises and inspects bodies designated for accreditation and conformity assessment to Annex III to the Presidential Decree150/2001.

Question 12: what in your opinion should be the form of supervision and control of these designated bodies?

V. RECOMMENDATIONS FOR SECURE-SIGNATURE VERIFICATION

Presidential Decree 150/2001 to Annex IV includes recommendations for secure-signature verification.

Question 13: Do you believe that the performance of this Annex should be required? What is in your opinion the proper way to assure its implementation?