Issued

Current Interpretation Responses

Ref. tSi 0271

Issue 1.00

2004-10-21

Executive summary

This document serves as the "Interpretation Library" referred to in Guidance for Assessments (tSi 0250). It contains a list of all questions that have been put to *tScheme* for clarification on the intention or interpretation regarding its criteria for Assessment.

DOCUMENT HISTORY

Status	Issue	Date	Comment	Authorised
tSi	1.00	2004-10-21	First version, tracked under Document Management procedures.	*tScheme* Secretariat

CONTENTS

1. INTRODUCTION

1.1 Purpose

This document is intended to serve as a compendium of responses to questions that have been put to *tScheme* for clarification on the intention or interpretation regarding its criteria for Assessment

It lists the questions in order of the date of the first Profiles & Processes committee meeting at which the questions were tabled.

Within each section there are a number of sub-sections, one for each question, under the title of the primary *tScheme* document to which the question applies. For each question there are sub-sections giving: the question, the answer and a list of *tScheme* documents with markers that have been raised as a result.

1.2 Readership

This document is intended for any participants in the *tScheme* process.

2. 26TH AUGUST 2004

The following three questions were posed in order to seek clarification with regard to the Assessment of a CA issuing Qualified Certificates to the public.

2.1 Approval Profile for a Certification Authority (tSd 0102)

2.1.1 Question

CR-020/QC within tSd 0102 (Approval Profile for a Certificate Authority) requires the TSP to provide evidence of compliance with the European Directive 99/93 [Dir 99/93]. Annexes I to III set out the requirements for QCs, CSP issuing QCs and SSCD respectively. There is however also an Annex IV, which sets out recommendations (not requirements) for secure signature verification and we would welcome clarification on whether this is also a need to demonstrate compliance with these recommendations.

2.1.2 Answer

HMG when enacting the Directive, through [ESR 2002], did not make any reference to the Annex IV Recommendations for secure signature verification. Therefore, we would defer to the wording of the Directive. This means that, unless sound reasons are given in support of an equivalent approach, we would expect the recommendations to be followed. For the avoidance of future doubt, a marker will be added to tSd0102 to modify CR-020/QC to say:

"... and, if secure signature verification is being provided, including the recommendations of Annex IV or equivalent approach";

and to tSi 0250 section 4.3 to say:

“Compliance with Annex IV of [Dir 99/93] can be demonstrated by conformance to the following or equivalent standards:

1. CEN Workshop Agreement 14171; Procedures for Electronic Signature Verification”.

2.1.3 Documents Modified

The following documents were released, which were modified as above, after review at the PPC meeting of 21st October 2004:

1. Approval Profile for a Certification Authority (tSd 0102 Issue 3.01);

2. Guidance for Assessments (tSi 0250 Issue 2.03).

2.2 Approval Profile for Signing Key Pair Management (tSd 0103)

2.2.1 Question

SGQC-090/QC & SGQC-100/QC within tSd 0103 (Approval Signing Key Pair Management) requires that subscriber enter into a written agreement with the CSP that contains certain stated obligations. These appear to go beyond the requirements of TS 101456, which requires that the CSP record the signed agreement with the subscriber. Can you therefore clarify what is meant by written and whether these criteria can be satisfied by an on-line agreement.

2.2.2 Answer

The criteria requiring written agreement should be interpreted in the sense that written implies humanly readable. Thus the criteria can be satisfied by an on-line agreement. This is in accordance with Note 10 to paragraph 7.3.1 h) of TS 101456, which states that "This agreement may be in electronic form".

2.2.3 Documents Modified

None.

2.3 Approval Profile for Certificate Generation (tSd 0104)

2.3.1 Question

CC-110/QC within tSd 0104 (Approval Profile for Certificate Generation) requires that QCs meet the criteria setout in sections 7.2.1 & 7.2.2 of TS 101456. These require that CA key generation be performed using an algorithm that is recognised as being fit purpose of QCs and that the selected key length and algorithm of the CA Signing key be recognised as bit fit for purposes of QCs as issued by the CA. TS 101456 also indicates that the guidance on algorithms and associated key lengths would be provided by a cryptographic advisory panel set under the EC Electronic Signature Committee. To the best of my knowledge, no such guidance has yet been published and we would therefore welcome your guidance on what criteria should be used to determine whether the algorithms and key lengths are fit for purpose.

2.3.2 Answer

In fact, an advisory panel did meet within EESSI and produced a guidance paper, ESI Special Report SR 002 176 “Algorithms and Parameters for Secure Electronic Signatures”, [ALGO paper]. In line with current *tScheme* practice, reference to such external documents is via “Guidance for Assessments” (tSi 0250) as an example of how evidence may be provided to satisfy particular criteria.

Criterion SI-060 in section 3.1.1 Information for Users already requires the service provider to state what algorithms and key lengths are being used and a marker will be added so that a new criterion is added to section 3.1.2 Information for Assessors requiring the service provider to supply a justification for the choice of algorithm and key length. A marker will also be added to tSi 0250, section 4.5 to say:

“Justification of choice of cryptographic algorithms, together with the requirements on their parameters, can be made by reference to the following or equivalent documents:

1. [ALGO paper].”

2.3.3 Documents Modified

The following documents were released, which were modified as above, after review at the PPC meeting of 21st October 2004:

1. Approval Profile for Certificate Generation (tSd 0104 Issue 3.01);

2. Guidance for Assessments (tSi 0250 Issue 2.03).

3. REFERENCES

[ALGO paper] ESI Special Report SR 002 176 "Algorithms and Parameters for Secure Electronic Signatures", published March 2003.

[CWA14171] CEN Workshop Agreement 14171; Procedures for Electronic Signature Verification.

[Dir 99/93] EC Directive 1999/93/EC on a Community framework for electronic signatures.

[ESR 2002] The Electronic Signatures Regulations 2002.

[TS 101456] "Policy requirements for certification authorities issuing qualified certificates", ETSI TS 101 456.

