

CIS 3

EDITION 1 | NOVEMBER 2002

UKAS Guidance for bodies operating certification of Trust Service Providers seeking approval under *tScheme*

CONTENTS

SECTION	PAGE
1 General	2
1.1 Scope	2
1.2 Background	2
2 Requirements for Certification Bodies	2
2.1 Certification Body	2
2.2 Certification Body Personnel	3
3 Requirements for Certification	4
3.1 Application for certification	4
3.2 Audit methodology	4
3.3 Assessment report	5
3.4 Decisions on certification	5
3.5 Surveillance and reassessment procedures	5
3.6 Use of the <i>tScheme</i> Mark	5
4 References	6

THE UNITED KINGDOM ACCREDITATION SERVICE (UKAS) IS RECOGNISED BY THE UK GOVERNMENT AS THE UK NATIONAL ACCREDITATION BODY RESPONSIBLE FOR ASSESSING AND ACCREDITING THE COMPETENCE OF ORGANISATIONS IN THE FIELDS OF INSPECTION, CALIBRATION, TESTING AND THE CERTIFICATION OF SYSTEMS, PRODUCTS AND PERSONNEL.

United Kingdom Accreditation Service, 21–47 High Street, Feltham, Middlesex, TW13 4UN
Web site: www.ukas.com Email: av@ukas.com Tel: 020 8917 8421 (9 am – 1 pm) Fax: 020 8917 8500

1 GENERAL

1.1 Scope

This document has been produced to supplement the guidance in EA-7/03⁽¹⁾ “*EA Guidelines for the Accreditation of bodies operating certification / registration of Information Security Management Systems*” when applied to bodies operating certification of Information Security Management Systems (ISMS's) and supporting technical infrastructures for electronic trust service providers offering services under the approval of *tScheme*.

Where EA-7/03 refers to ISMS this should be read to include the supporting technical infrastructure. The acceptance criteria that are to be met with respect to this supporting technical infrastructure are set out in the *tScheme* Approval Profiles.

1.2 Background

Accreditation for certification of trust service providers (TSP's) has been developed by UKAS under ISO/IEC Guide 62 / EN 45012⁽²⁾. It is integral

to the operation of *tScheme*, a non-statutory self-regulatory BS 7799 sector scheme for approving cryptographic based trust services, which supports the UK legislation for the enactment of the ‘Electronic Signatures’ Directive (1999/93/EC – hereafter referred to as ‘Dir.99/93’⁽³⁾). The term ‘trust service provider’ (TSP) used by *tScheme* is analogous to the term ‘certification-service-provider’ (CSP) used by Dir.99/93. However, *tScheme* goes further than Dir.99/93, in that ‘TSP’ covers a wider range of service provision activities than the ‘CSP’ activity defined in Dir.99/93.

tScheme requires trust service providers to operate effective quality management and information security management systems. Certification bodies are required to assess this to ensure that the QMS is fit for its intended use and compatible with ISO 9001:2000⁽⁴⁾, and that the ISMS meets the requirements of BS 7799 Part 2⁽⁵⁾ or other recognised standard that includes all of the requirements of BS 7799 Part 2.

2 REQUIREMENTS FOR CERTIFICATION BODIES

2.1 Certification Body

2.1.1 *tScheme* Agreement

It is a requirement of *tScheme* that ‘recognised-assessors’ shall hold accreditation from a national accreditation body for certification against the *tScheme* Approval Profiles. Within the UK the United Kingdom Accreditation Service fulfils this function, and has developed the accreditation service as a Sector Scheme of BS 7799.

Prior to applying to UKAS for accreditation, the certification body shall enter into an agreement with the administrators of *tScheme* (*tScheme* Ltd) in order to be recognised as a ‘*tScheme*-recognised assessor’.

2.1.2 Quality System

In addition to the requirements specifying the minimum content of the Quality Manual and associated quality procedures (EA-7/03, clause 2.1.4.3), the policy and procedure for implementing the certification process shall be amplified to include:

- checks of the use and application of *tScheme* documentation, e.g. *tScheme* Approval Profiles.
- the procedures for assessing and certifying an organisation’s technical infrastructure under *tScheme*. The technical infrastructure includes the technology (hardware and software), the technical standards and specifications used to implement and provide trusted services, communications and other services used to support the delivery and any other technical items that are specified in the *tScheme* Approval Profiles.

2 REQUIREMENTS FOR CERTIFICATION BODIES (CONT'D)

2.1.3 Confidentiality

Except as required in EA-7/03, information about a particular organisation shall not be disclosed to a third party without the written consent of the organisation (clause 2.1.9.2). With respect to *tScheme* this means that the certification body and trust service provider shall have a written agreement that will allow the certification body to disclose confidential information to tScheme Ltd where this could have a direct impact on the TSP's approval by tScheme. This agreement should be produced and agreed by both parties when the certification body is first contracted, and should be signed by representatives of both parties.

2.2 Certification Body Personnel

2.2.1 General

When a certification body is conducting an assessment under *tScheme* it will need to ensure that its competence analysis and contract review covers all relevant areas (Clause IS.3.2 of EA-7/03). In particular it shall have systems that ensure knowledge of the technological and legal developments relevant to *tScheme*, as well as the quality and information security management systems of the organisations that it assesses. It shall also have an effective system for the analysis of the competencies in electronic trust services as well as information security management with respect to all the technical areas in which it operates.

In addition to the five points listed in EA-7/03 Clause IS 3.2, the certification body shall be able to demonstrate that it has the capability to define the competencies needed to certify the supporting technical infrastructure of the ISMS under *tScheme*.

The certification body's criteria for the training and selection of audit teams shall be amplified to include an appropriate level of understanding of *tScheme* and electronic trust services. (Clause IS 3.3 of EA-7/03)

2.2.2 Qualification criteria for auditors and technical experts

2.2.2.1 Auditor competence

Persons employed by certification bodies for performing '*tScheme*' audits by themselves should have at least four years full time practical workplace experience in information technology. At least two years of this should have been in a role or function relating to the full scope of electronic trust services subject to assessment as well as information security management. They shall also have an appropriate understanding of the concepts of management systems in general, and of the up-to-date issues related to relevant areas of public key infrastructure (PKI), information security management, and organisational reliability. The candidate shall gain experience in the entire process of assessing under tScheme prior to assuming responsibility for performing as an auditor. Furthermore they shall have participated in at least three complete tScheme audits prior to being authorised to act as a lead auditor. (Clause IS 4 of EA-7/03)

Note: Initially, certification bodies may be unable to identify individuals who fulfil the requirements relating to previous experience of tScheme audits. In this instance the certification body should be able to provide recorded evidence that justifies the use of its chosen assessors and lead assessors based on other, relevant, experience.

The range of knowledge required by the audit team, whether by an individual or collectively as a team, shall encompass the external standards and guidelines that the trust service provider has included within its specification(s) for assessment, e.g. a knowledge of the government guidelines relating to the Government Gateway (UK).

If the scope of the intended audit includes the assessment of qualified certificates, as covered by Dir.99/93, then the certification body must ensure that the assessment team includes personnel with an appropriate understanding of the requirements for certification authorities issuing qualified certificates, e.g. an understanding of ETSI TS 101 456 (QCP)(6).

2 REQUIREMENTS FOR CERTIFICATION BODIES (CONT'D)

2.2.3 Selection Procedures

Further to the audit team competence listed in clause IS.5 of EA-7/03 the certification body shall ensure that all members of the audit team are able to demonstrate appropriate experience and understanding of *tScheme* and its requirements. In addition the audit team as a whole shall possess an up-to-date knowledge of technical infrastructure solutions, standards and specifications in the fields of:

- a) Electronic trust services
- b) Electronic signatures and digital certificates
- c) Public-key infrastructure
- d) Management of cryptographic technologies
- e) Identification and authentication technologies
- f) Access control technologies
- g) Network security
- h) Directory systems

The audit team shall also include competence in technical compliance checking of:

- i) Inter-organisational communication security
- j) Third party dependencies
- k) Security testing techniques (both manual and software assisted)
- l) Hardware and software risk assessment

3 REQUIREMENTS FOR CERTIFICATION

3.1 Application for certification

3.1.1 The application

The official application form required by the certification body (clause 3.1.2.1 of EA-7/03) shall be submitted together with a *tScheme* Registered Applicant Agreement and one or more outline Specification of Service Subject to Assessment (S3A). The S3A is a *tScheme*-defined document specifying the scope of assessment that the applicant wishes to have undertaken. In some instances the application may include, or solely comprise, an electronic trust service component as opposed to a full electronic trust service (such components, once approved, are referred to as '*tScheme*-Ready'). Applications submitted for *tScheme*-Ready assessments shall include one or more outline Specification of Service Component Subject to Assessment (C3A) instead of a S3A.

NB: Although the certification body may be involved in early dialogue with a trust service provider, it should not proceed with a formal assessment until it has received all of the above documents (as applicable).

3.2 Audit Methodology

3.2.1 Audit (Stage 1)

During audit (stage 1) the certification body shall review each S3A and obtain documentation on the details and design of the trust service(s) put forward for assessment, and of the quality and information security management systems in place (EA-7/03 Clause IS 9.1). The audit (stage 1) includes, but should not be restricted to, the document review. In every case the document review should be completed prior to the commencement of audit (stage 2).

3.2.2 Audit (Stage 2)

The overall objective of audit (stage 2) is for the TSP to demonstrate to the auditors that it has appropriate controls in place to be able to deliver trust services. The auditor needs to have sufficient confidence and assurance that the TSP is managing its security risks appropriately to be able to deliver such services. This shall include confirmation that the supporting technical infrastructure complies with the acceptance criteria as documented in the *tScheme* Approval Profiles for each trusted service offered (EA-7/03 Clause IS 9.2). To do this, part of the audit shall focus on the organisation's technical security controls for the trusted service specified in each submitted S3A.

3 REQUIREMENTS FOR CERTIFICATION (CONT'D)

In addition the auditors shall assess the delivery of the service included in each S3A to ensure that its implementation complies with the documentation presented to the auditors during audit (stage 1). This shall include an assessment of the TSP's service documents to ensure that its claims are not overstated (and therefore misleading), not over-simplified or ambiguous (and therefore non-descriptive), and that non-beneficial service conditions, exclusions, disclaimers, and other limitations are clearly presented.

Where the TSP contracts with an external provider to supply one or more trust service components, the certification body shall ensure that the overall quality and security of the trust service being audited is not prejudiced by any insecurities in these external trust service components. This may include an assessment of the external provider if the certification body deems it necessary.

3.2.3 Security Products and Systems

A *tScheme* audit is not a security product or system evaluation in the sense of an ITSEC (IT Security Evaluation Criteria) or CC (Common Criteria) assessment, and the audit team is not required to have technically competent staff to this end. However, the audit team should be able to verify that the evidence submitted in support of such products/systems is acceptable. Hence, if components of the technical infrastructure deployed by the trust service provider use products and technologies that have been evaluated under ITSEC or CC then proof of such evaluation shall be considered as evidence of acceptability.

3.3 Assessment Report

The certification body may adopt reporting procedures that suit its needs but as a minimum these procedures shall ensure that the requirements of clause 3.4.1 of EA-7/03 are met. In addition to the minimum information that must be included in the report on the outcome of the assessment (clause 3.4.1 (e)) the report shall also contain comments on the conformity of the TSP's technical infrastructure with respect to *tScheme* Approval Profile criteria and on the delivery of the audited service(s).

In order for the certification body to make an informed decision on granting, maintaining, extending, reducing, suspending or withdrawing certification the reports from the audit team to the certification body must include an account of the assessment of both the technical

infrastructure covered by the applicable *tScheme* Approval Profile and the TSP's information security risk analysis.

3.4 Decisions on certification

The decision whether or not to certify a TSP's management system related to one or more specified trust service shall be taken by the certification body on the basis of information gathered during the certification process and any other relevant information. Those who make the certification decision shall have competence in the area of electronic trust services and shall not have participated in the audit.

The certification documentation provided by the certification body to a trust service provider shall consist of a report that includes, in addition to the information covered in clause 3.5.3 of EA-7/03, the content required by *tScheme* based upon its published model assessment reports for services and components, references tSd 0238⁽⁷⁾ and tSd 0239⁽⁸⁾.

Note: It is a tScheme requirement that certification bodies only issue reports and not certificates with respect to tScheme assessments.

3.5 Surveillance and Reassessment Procedures

The certification body shall carry out periodic surveillance and reassessment at sufficiently close intervals to verify that its organisations whose management systems are certified continue to comply with the certification requirements. In most cases it is unlikely that a period of greater than one year for periodic surveillance and greater than three years for periodic reassessment would satisfy requirements (clause 3.6 of EA-7/03).

3.6 Use of the tScheme Mark

Certification bodies should be aware that trust service providers can only use the *tScheme* Mark with respect to their trust services, or refer to those services as '*tScheme* approved', once their management system relating to those services has been certified by a '*tScheme*-recognised assessor' (i.e. accredited certification body) and has been formally granted approval by *tScheme*. This formal approval shall take the form of a contractual arrangement between the TSP and *tScheme* as detailed in the *tScheme* guidance document tSd 0254 "*tScheme* Model Agreement Permitting Use of the *tScheme* Mark".

4 REFERENCES

1. **EA-7/03** *EA Guidelines for the Accreditation of bodies operating certification/registration of Information Security Management Systems*
2. **EN 45012** *General Requirements for Bodies Operating Assessment and Certification/Registration of Quality Systems*
3. **Dir.99/93** *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures*
4. **ISO 9001:2000** *Quality Management Systems – Requirements*
5. **BS 7799 Part 2** *Information Security Management Systems - Specification with guidance for use*
6. **ETSI 101 456 (QCP)** *Policy Requirements for Certification Authorities Issuing Qualified Certificates*
7. **tSd 0238** *Model Assessment Report - Service*
8. **tSd 0239** *Model Assessment Report - Component*
9. **tSd 0254** *tScheme Model Agreement Permitting Use of the tScheme Mark*