CIS 3

Edition 3 February 2020 – Draft for consultation

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

United Kingdom Accreditation Service 2 Pine Trees, Chertsey Lane, Staines-upon-Thames, TW18 3HR
Website: www.ukas.com Publications requests email: UKASPublications@ukas.com

Contents

Changes since last edition

Updated to reference the eIDAS Regulation for Trust Service Providers and to reflect current standards and scheme reference documents.

1. Introduction

1.1 Scope

This document has been produced as guidance to bodies operating certification of Information Security Management Systems (ISMSs) and supporting technical infrastructures for electronic trust service providers offering services under the approval of *tScheme*.

References to ISMS 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 (TSPs) is integral to the operation of *tScheme*, which was established as a non-statutory, self-regulatory ISMS sector scheme for approving cryptographic based trust services to support 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 is a sector scheme of ISMS, for which the accreditation criteria are ISO/IEC 17021-1:2015 and ISO/IEC 27006:2015.

tScheme can now be used to provide evidence in support of a Conformity Assessment of a TSP's compliance with the eIDAS Regulation[3a] (hereafter referred to as eIDAS) to allow the TSP to gain and maintain Qualified status in accordance with Articles 21.1 and 20.1 respectively.

tScheme requires trust service providers to operate effective quality management and information security management systems. Certification bodies are required to audit this to ensure that the QMS is fit for its intended use and compatible with ISO 9001:2015[4], and that the ISMS meets the requirements of ISO/IEC 27001:2013 or other recognised standard that includes all of the requirements of ISO/IEC 27001:2013.

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 'recognised assessors' are in the form of third-party certification bodies. The national accreditation body for the UK is the United Kingdom Accreditation Service (UKAS), which has recognised tScheme as a Sector Scheme of ISMS.

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 regarding the quality manual (ISO/IEC 17021-1:2015 clause 10.2.2 and ISO/IEC 27006:2015, clause 10), 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 auditing 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.

2.1.3 Confidentiality

Except as required in ISO/IEC 17021-1:2015 and ISO/IEC 27006:2015, information about a particular organisation shall not be disclosed to a third party without the written consent of the organisation (ISO 17021-1:2015, Clause 8.4.3 and ISO/IEC 27006:2015, Clause 8.4). 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 under *tScheme*. This agreement shall be produced and agreed by both parties when the certification body is first contracted and shall be signed by representatives of both parties.

2.2 Certification Body Personnel

2.2.1 General

When a certification body is conducting an audit under *tScheme* it will need to ensure that its competence analysis and contract review covers all relevant areas (ISO/IEC 17021-1:2015, Clause 7.1 and ISO/IEC 27006:2015, Clause 7.1.1.1). 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 audits. 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.

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* (ISO/IEC 17021-1:2015, Clause 7.1 and ISO/IEC 27006:2015, Clause 7.1.1.1).

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 (ISO/IEC 17021-1:2015, Clause 7.2.4 and ISO/IEC 27006:2015, Clause 7.2.1.1).

2.2.2 Qualification Criteria for Auditors

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 security. 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 audit 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), identity management, information security management, and organisational reliability. The candidate shall gain experience in the entire process of auditing 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 (ISO/IEC 17021-1:2015, Clauses 7.1.1 and 9.1.3 and ISO/IEC 27006:2015, Clause 7.2.1.1)

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 auditors and lead auditors based on other, relevant experience

The *tScheme* Approval Profiles cover two different classes of technology relating to the provision of credentials for Identity Management. These are separated into services relating to public key infrastructure (PKI), which are audited against the criteria given in the CA Profile[10] and related sub-service Profiles identified therein, and services that do not use PKI technology, which are audited against the criteria given in the IdP Profile[11] and related sub-service Profiles identified therein. 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 audit.

If the scope of the intended audit includes the assessment of Qualified Certificates, for electronic signatures or seals as covered by eIDAS, then the certification body must ensure that the audit team includes personnel with an appropriate understanding of the requirements for certification authorities issuing Qualified Certificates, e.g. an understanding of ETSI EN 319 401[6], ETSI EN 319 411-1[6a] and ETSI EN 319 411-2[6b].

If the scope of the intended audit includes the assessment of Qualified Certificates, for website authentication as covered by eIDAS and the CA Browser Forum, then the certification body must ensure that the audit team includes personnel with an appropriate understanding of the requirements for certification authorities issuing Qualified Certificates, e.g. an understanding of ETSI EN 319 401[6], ETSI EN 319 411-1[6a], ETSI EN 319 411-2[6b] and the CA Browser Forum requirements[6c].

2.2.3 Selection Procedures

Further to the audit team competence 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 (ISO/IEC 17021-1:2015, Clause 7.2.4 and ISO/IEC 27006:2015, Clause 7.2.1.1). 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) Identity lifecycle management
c) Credential lifecycle management
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

2.2.3.1 Additional Selection Procedures for Audits of Services using PKI Technology

a) Electronic signatures and digital certificates
b) Public-key infrastructure

3. Requirements for Certification

3.1 Application for Certification

3.1.1 The Application

The official application form required by the certification body (ISO/IEC 17021-1:2015, Clause 9.1.1 and ISO/IEC 27006:2015, Clause 9.1) shall be submitted together with a *tScheme* Registered Applicant Agreement[8] and one or more outline Specification of Service Subject to Audit (S3A)[12]. The S3A is a *tScheme*-defined document specifying the scope of assessment that the applicant wishes to have undertaken.

If the scope of the intended audit includes the assessment of Qualified Certificates, as covered by eIDAS, then the service provider must demonstrate that they are aware of the process for the initiation of a new Qualified Trust Service by the relevant Supervisory Body.

NB: Although the certification body may be involved in early dialogue with a trust service provider, it should not proceed with a formal audit 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 (ISO/IEC 17021-1:2015, Clause 9.3.1.1 and ISO/IEC 27006:2015, Clause 9.3.1.1). The audit (Stage 1) includes, but shall 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 (ISO/IEC 17021-1:2015, Clause 9.3.1.2 and ISO/IEC 27006:2015, Clause 9.3.1.2). 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.

In addition, the auditors shall audit 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 audit 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 audit 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, CC or similar scheme, then proof of such evaluation shall be considered as evidence of acceptability.

If the scope of the intended audit includes the assessment of Qualified Certificates using Qualified Electronic Signature Creation Devices or Qualified Electronic Seal Devices, as covered by eIDAS, then the service provider must use products and technologies that have been certified in accordance with Article 30 or Article 38.2 (respectively).

3.3 Audit Report

The certification body may adopt reporting procedures that suit its needs but as a minimum these procedures shall ensure that the objectives of ISO/IEC 17021-1:2015, Clauses 9.3.1.1 & 9.3.1.2 and ISO/IEC 27006:2015, Clauses 9.3.1.1 & 9.3.1.2) are met. In addition to the minimum information that must be included in the report on the outcome of the audit (ISO/IEC 17021-1:2015, Clause 9.4.8

and ISO/IEC 27006:2015, Clause 9.4.3), 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).

If the scope of the intended audit includes the assessment of Qualified Certificates as covered by eIDAS, then the report should also include statements on the conformity of the TSP's technical infrastructure with the relevant requirements of the eIDAS Regulation.

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 ISO/IEC 27006:2015, Clause 8.2.1, the content required by *tScheme* based upon its published model assessment report for services (tSd 0238[7]).

If the scope of the intended audit includes the assessment of Qualified Certificates as covered by eIDAS, then the certification body should also produce a conformity assessment report in the format and containing the information required by the relevant Supervisory Body.

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 recertification 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 recertification would satisfy requirements (ISO/IEC 17021-1:2015, Clause 9.1.3 and ISO/IEC 27006:2015, Clause 9.1.3).

If the scope of the intended audit includes the assessment of Qualified Certificates as covered by eIDAS, then the certification body should also produce a conformity assessment report in the format and containing the information required by the relevant Supervisory Body.

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. an 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"[9].

4. References

1 ISO/IEC 17021-1:2015 Conformity assessment - Requirements for bodies providing audit and certification of management systems

2 ISO/IEC 27006:2015 Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management 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

3a eIDAS Regulation - Regulation 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

4 ISO 9001:2015 Quality Management Systems - Requirements

5 ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements

6 ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers supporting Electronic Signatures"

6a ETSI EN 319 411-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements for Trust Service Providers issuing certificates"

6b ETSI EN 319 411-2: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for Trust Service Providers issuing qualified certificates"

6c CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates

7 tSd 0238 - Model Assessment Report - Service

8 tSd 0253 - *tScheme* Model Registered Applicant Agreement

9 tSd 0254 - *tScheme* Model Agreement Permitting Use of the *tScheme* Mark

10 tSd 0102 - Approval Profile for a Certification Authority

11 tSd 0112 - Approval Profile for an Identity Provider

12 tSd 0230 - *tScheme* Model Specification of Service Subject to Assessment (S3A)