Department for Science, Innovation & Technology

Office for Digital Identities & Attributes

Certification scheme requirements for Conformity Assessment Bodies

UK digital verification services trust framework certification scheme

Version 1.15

Table of contents

1 Version history

Version	Date	Pages	Changes	Author
0.1	November 2023	All	From previous version of Document previously title 0 – Certification Scheme as issued by DSIT	DSIT
1.1	November 2023	All	Updates as per review document and actions requested by UKAS. Additional extended content added by DSIT.	DSIT
1.2	March 2024	All	Updates to reflect actions issued by UKAS in the February review.	DSIT
1.3	April 2024	All	Updates to reflect outstanding actions from UKAS post March review.	DSIT
1.4	April 2024	All	Updates from the workshop with UKAS	DSIT
1.5	June 2024	All	Grammatical corrections, clarification in Annex C and update to the table in Annex C	DSIT

1.6	September 2024		Change file name and version number	DSIT
		p. 27	Updated rules on the use of existing certification as proof of conformity to the UK DIATF certification scheme	
		pp. 20, 43-44, 50 p. 52	Updated the application flow diagram and process to become certified and join the GOV.UK register of digital identity and attributes services	
			Updated information about rolling over certificates that are close to expiry	
		pp. 57-59	Removed Annex A as it was duplicate content from the “CAB Principles and Code of Ethics – v1.3” document	
		pp. 57-59	Renamed Annex B to Annex A to account for removal of Annex A	
			Updated Annex B (now renamed Annex A) subsets for the Home Office Right to Work and Right to Rent, and Disclosure and Barring Service DBS supplementary schemes	
		p. 60	Annex C is renamed Annex B to account for renaming of other annexes	
			Removed Annex D and put into new document on requirements for certificate production	

1.7	October 2024	All	Significant changes to reflect new Trust Framework version 0.4. Format updated across the document. Changes to terminology throughout, for added clarity (e.g. move away from 'audit' to 'evaluation', remove language that could be confused with ISO 17021). Procedural changes throughout including: • move to a 3 yearly certification cycle • inclusion of section on due diligence checks to be carried out prior to certification • white labelling section added • new roles included as per the TF 0.4 • further information provided on surveillance activities. • clarifications, including CABs being required to submit certificates and certification feedback reports.	DSIT
1.8	January/February 2025	All	Added additional requirements in relation to white-labelling and co-branding	DSIT
1.9	April 2025		Information on Scheme Owner expanded. Further information on maintenance, development and uplift of the scheme included. Requirements and process of CAB approval, including a letter of approval template included. The approval process and letter of approval are replacing the contract from the previous version of the scheme.	DSIT

1.9.1	May 2025	p.27 p.38 p.58 Annex C	Small amendments to the letter of approval and section 7.1.2 on approval, including sections 9.3.3 and 10.5.1 to clarify decision stage	DSIT
1.10	June 2025	p.13 p.58 p.74 p.80 p.84	Updated 2.13 10.6.2, section 2 updated Section 5 updated 11.5, section 2 updated Section 1 updated	DSIT

1.11	February - March 2026	All p..9-11, 5 Terms and Definitions p.29, 9.6.4 p.68	Stylistic changes made to the document, using active voice (You, us vs CAB and the scheme owner). Making the document accessible and removing capitalisation of defined terms along with the green colour and replacing it with bold letters for defined terms Changes if ‘will’ to ‘shall’ across the document Reduced number of defined terms only to those that are specific to the scheme. New definitions added Para added on spot audits New diagram added under Annex C	DSIT

1.12	April 2026	p.9, 3.3.5 p.15 p.16, 6.4 Trust Mark p45, 10.6.2.c (iii) p.27	Added line to the trust framework - main document setting out requirements for digital verification services, products or processes that want to be certified against the trust framework certification scheme Added a line under 6.3.7 b on CAB being accredited against ISO17065 and compying with all the requirements stated in the standard (6.3.7.b (i) You shall be accredited against ISO17065 and will be checked by UKAS that you comply with all the requirements of ISO17065.). Added a new section on Trust Mark and additional section under certification decision. Added a line under 9.3.2 d 9.3.2 d (You shall complete a legally enforceable contract, inter alia, that covers all relevant requirements of ISO17065). This is also covered in the CAB Principles and code of Ethics, under section 2.	
1.13	May		Updates based on UKAS actions	DSIT
1.14	June		New section that includes information on the uplift to 1.0 and timelines	DSIT
1.15	June	P27-28, 9.3.2d P18, 6.4.3 and 6.4.4	Addition of line in 9.3.2d on GDPR Addition of line on usage guidelines	DSIT

2 Scope

2.1 This document is produced by the Office for Digital Identities and Attributes (OfDIA). **We** are part of the Department for Science, Innovation and Technology (DSIT). **We** are the team responsible for day-to-day operation of this certification scheme for **the UK digital verification service trust framework (trust framework)**.

2.2 These certification scheme requirements are for Conformity Assessment Bodies (CABs). They contain the requirements you need to meet when certifying against this scheme.

2.3 ISO/IEC 17065:2012 is the international standard, which sets out criteria for bodies operating certification of services and will be used to assess and accredit CABs operating the trust framework certification scheme (the scheme) for DSIT. This document will be used to supplement and interpret the general criteria contained in ISO/IEC 17065:2012, and additional requirements will be highlighted where applicable.

3 Normative references

3.1 The following documents contain provisions that, through reference in this text, become part of the scheme.

3.2 This document, **shall** be referred to as the Certification scheme requirements for conformity assessment bodies (the scheme).

3.3 The following referenced documents are also applicable to this scheme:

3.3.1 ISO/IEC 17000, Conformity assessment — Vocabulary and general principles

3.3.2 ISO/IEC 17020, Conformity assessment — Requirements for the operation of various types of bodies performing inspection

3.3.3 ISO/IEC 17065:2012, Conformity assessment — Requirements for bodies certifying products, processes and services

3.3.4 ISO/IEC 17066:2012, Conformity assessment — Fundamentals of product certification and guidelines for product certification schemes

3.3.5 UK digital verification services trust framework 1.0 – main document setting out requirements for digital verification services, products or processes that want to be certified against the trust framework certification scheme.

3.3.6 Conformity assessment body personnel skills and competencies

3.4 For documents that specify a date or version number, later amendments or revisions of that document do not apply as a normative requirement.

3.5 We encourage you to review the most recent editions and any guidance documents available, to gain further insight into how they have changed and consider whether to implement the latest changes.

3.6 For documents without dates or version numbers, the latest published edition of the document referred to applies.

4 Informative references

4.1 This document should be read alongside the following, from the International Organization for Standardization:

4.2 ISO/IEC Directives, Part 2, 2018, 33.2, Conformity schemes and systems (opens in a new window)

4.3 ISO/IEC 17007, Conformity Assessment guidance for drafting normative documents suitable for use for conformity assessment (opens in a new window)

4.4 ISO/IEC 17067 Conformity assessment — Fundamentals of product certification and guidelines for product certification schemes (opens in a new window)

4.5 ISO and UNIDO, Building trust – The conformity assessment toolbox (opens in a new window)

5 Terms and definitions

5.1 Within this document, we use the following terms which have specific meanings:

5.1.1 '**We**' or '**us**' refers to The Office for Digital Identities and Attributes (OfDIA)

5.1.2 '**You**' refers to any CAB that is, or wishes to become, approved by us to certify services under the scheme

5.1.3 '**Shal**l' indicates a requirement

5.1.4 '**Shall not**' indicates a prohibition

5.1.5 '**Should**' indicates a recommendation

5.1.6 '**May**' indicates a permission

5.1.7 '**Can**' indicates a possibility or a capability

5.2 For the purposes of this document, the terms and definitions given in ISO/IEC 17000, ISO/IEC 17065 and the following shall apply:

5.2.1 '**Accredited**' - having been recognised by The United Kingdom Accreditation Service (UKAS), (opens in a new window) under an accreditation process based on ISO 17065 and the scheme.

5.2.2 '**Approved**' – means we have issued the relevant CAB with a letter of approval.

5.2.3 '**Attestation**' – means issue of a statement of conformity with the scheme in accordance with section 11.9 of this document.

5.2.4 '**Auditor'** – refers to an individual that undertakes evaluation of a process, service, or product under the scheme . This can take the form of inspection, audit or testing, depending on the nature of the process, service or product.

5.2.5 '**Certified'** - means a service has been assessed as compliant with the relevant requirements of the scheme appropriate to its scope by an approved CAB and has been issued with a certificate.

5.2.6 '**Letter of approval'** – a letter we issued to you as a formal ratification that you meet the requirements as defined by us in the scheme documentation.

5.2.7 '**Registered'** – indicates that the provider of a certified service has been added to the register of digital verification services (the register).

5.2.8 '**Trust mark'** – the symbol or logo we issue to a service provider operating products, services and processes that appear on the register, as defined in the Data (Use and Access) Act 2025 for use on the registered product, service or process.

5.2.9 '**Trust marked'** – indicates that we have authorised a product, service or process to display a trust mark. A trust mark may only be displayed if the product, service or process is also registered.

5.3 In the context of white labelling and co-branding, the following terms shall apply:

5.3.1 '**Underpinning service'** – a service that complies with the appropriate requirements of the trust framework, plus has additional controls in place as described below in section 10.3.2.

5.3.2 '**Underpinning certificate'** – a certificate from a CAB confirming that an underpinning service has been evaluated successfully against all relevant requirements of the scheme.

5.3.3 '**White labelling'**– the practice of producing, reproducing or rebranding white label services.

5.3.4 '**White label services'** – products, services or processes that are produced by a first-party for a second-party and then rebranded, giving

users of the service the appearance that the second-party created them. The white label service relies upon an underpinning service operated by the first-party, in whole or in part, with the relationship between both parties being controlled by means of a contract or another legally-binding mechanism

5.3.5 '**First-party'** (for example, first-party organisations, first-party services) – any organisation offering its certified underpinning service for redistribution or re-branding to a second-party.

5.3.6 '**Second-party'** (for example, second-party organisations, second-party services) – any organisation redistributing the product, service or process provided by a first-party or that allows its brand to be applied to a white label service by a first-party.

5.3.7 '**Co-branding'** - where both the first-party and second-party providers' brands are displayed together

5.4 The above defined terms, including the name of **the scheme** and the **trust framework, shall not** be used to name services **certified** under this **scheme**.

6 Certification scheme

6.1 Introduction

6.1.1 A certification scheme is a structured and standardised approach to providing third party attestation that required regulations, standards and criteria are met.

6.1.2 This certification scheme **shall** be referred to as the UK digital verification services trust framework certification scheme (**the scheme**).

6.2 Scheme owner

6.2.1 The Department of Science, Innovation and Technology (DSIT) is the scheme owner. The Office for Digital Identities and Attributes (OfDIA), is part of DSIT. We (OfDIA) are the team responsible for day-to-day operation of **the scheme**.

6.2.2 As part of our day-to-day activities, we:

6.2.2 a develop, maintain and publish the trust framework (opens in a new window), supplementary codes, and the associated scheme documentation;

6.2.2 b manage the approved status of CABs (opens in a new window),

6.2.2 c work with stakeholders on the development and maintenance of standards and evaluation methods relevant to the certification scheme,

6.2.2 d collaborate with the international community focusing on interoperability between different national digital identity frameworks.

6.3 Development and maintenance of the certification scheme

6.3.1 As the **scheme owner**, **we shall** manage the scheme. This involves reviewing it and providing approval for its use during certification activities. **We shall** maintain the scheme to reflect relevant updates to the external requirements on which it is built.

6.3.2 **We shall** develop and maintain **the scheme** in line with the requirements set out in this document.

6.3.3 Periodic review of the certification scheme

6.3.3 a **We** shall carry out a periodic review of the content and performance of:

6.3.3.a (i) **the trust framework**

6.3.3.a (ii) **supplementary codes**

6.3.3.a (iii) the associated scheme documentation

6.3.3 b The periodic review:

6.3.3.b (i) **shall** take place at least annually

6.3.3.b (ii) **may** take place more frequently if required

6.3.3 c **We shall**, as part of the review, consider whether changes need to be made and whether consultation is required. This will depend on the complexity and potential implications of the changes on the ecosystem.

6.3.4 Management of external dependencies

6.3.4 a **We shall** maintain a list of externally referenced documents and standards that underpin the **scheme**. **We shall** monitor for changes and **shall** determine whether iterations of those standards and documents are compatible with **the scheme**.

6.3.4 b **We shall** update **the scheme** and reissue it, where a change to an externally referenced document or standard is considered significant.

For example, if a document uplifts a control because of a known security vulnerability. **We shall** do this as soon as is practical.

6.3.4 c If **we** consider a change to an externally facing document or standard to be routine, **we shall** update **the scheme** to reference the new version or standard as part of the annual review cycle.

6.3.4 d If an external document or standard is updated, the pre-existing document referenced in **the scheme** still applies until we have revised and issued the updated version.

6.3.5 **Consultation and iteration**

6.3.5 a **We shall** consult with stakeholders that **we** consider appropriate on proposed changes or updates to the **scheme** and relevant documentation. **We shall** iterate the **scheme** based on the feedback, where appropriate.

6.3.6 **Pre-release**

6.3.6 a **We may** publish on GOV.UK pre-release versions of:

6.3.6.a (i) **the trust framework**

6.3.6.a (ii) **supplementary codes**

6.3.6 b **We shall** also share draft scheme documentation with approved CABs.

6.3.6 c **You shall not** use pre-release versions of documentation as a basis for conformity assessment. These versions are shared with **you** to provide advance notice of potential scheme changes and **may** be pending UKAS recognition.

6.3.6 d As soon as it has been amended, **we shall** email all applicable and supporting documentation to CABs. **We shall** email this to the named person you have nominated to receive it. **You shall** be required to confirm receipt of updated documentation via email.

6.3.7 **Certification scheme uplift**

6.3.7 a **UKAS recognition**

6.3.7.a (i) **We shall** share final drafts of the scheme documentation, including **the trust framework** and **supplementary codes**, with UKAS for recognition.

6.3.7.a (ii) **We shall** inform **you** once UKAS has recognised the latest version of **the scheme**.

6.3.7.a (iii) **We shall** also provide **you** with rules, guidance and timelines for implementing the changes and assessing against the new published documents. The timelines will take into consideration the size and complexity of changes as well as possible urgency of implementing them to prevent any major disruptions in the digital identity ecosystem.

6.3.7.a (iv) For the latest information on scheme uplift please see section 11 of this document.

6.3.7 b **Accreditation**

6.3.7.b (i) You shall be accredited against ISO17065 and will be checked by UKAS to ensure that you comply with all the requirements of ISO17065.

6.3.7.b (ii) Before seeking uplift of accreditation, **you shall** apply to us for approval, using the process set out in Section 7 of **the scheme**.

6.3.7.b (iii) Once **we** have given **you** approval, **you shall** apply to UKAS for uplift of accreditation against the latest version of:

- the trust framework

- any applicable **supplementary codes**

- the certification scheme underpinning those activities

6.3.7.b (iv) If **you** do not wish to apply for approval or to apply to uplift accreditation, **you shall** withdraw from **the scheme**.

6.3.7 c **Certification scheme release**

6.3.7.c (i) To enable accreditation, when **the scheme** is recognised by UKAS, **we shall** bring into effect, for the purposes of certification, versions of:

- the trust framework

- supplementary codes

- the certification scheme underpinning those activities

6.3.7.c (ii) **We shall** publish **the trust framework** and **supplementary codes** on GOV.UK, when ready.

6.3.7.c (iii) **We shall** release all other documents to **approved** CABs via email.

6.3.7.c (iv) As soon as **we** have amended all applicable and supporting documentation, **we shall** email it to the named person in **your** CAB that **you** have nominated to receive it.

6.3.7.c (v) **You shall** confirm receipt of the updated documentation, to **us**, by email.

6.3.7.c (vi) Where documentation is not published in the public domain, **we shall** make relevant scheme documentation available on request. **We shall** publish information about how interested third parties can request the documentation on GOV.UK.

6.3.7 d **Expiry of old versions**

6.3.7.d (i) **We shall** include timelines for expiry of old versions of documentation in the latest published version of **the trust framework** and **supplementary codes**.

6.3.7.d (ii) If the provider of a service that **you** certify fails to implement the changes in accordance with requirements published before expiry, there **can** be consequences (for that service) up to and including the loss of certification and removal from the register.

6.3.7.d (iii) If **you** fail to implement the changes before expiry, there **may** be consequences (for your conformity assessment body) up to and including removal of your approved status to operate under **the scheme**.

6.4 **Trust mark**

6.4.1 **We** own and license use of a trust mark that **can** be used by providers that have certified and registered digital verification services. Detailed requirements that providers **shall** comply with and **you shall** check are included in the trust framework.

6.4.2 **We shall** issue terms of use to **you** and **you shall** share these with the provider during their certification process for them to sign. **You shall** collect the signed terms of use before **you** issue positive certification decision and **you shall** send the signed terms of use to us together with

the certification feedback report and the certification as detailed in section 10.6.2.c of this document.

6.4.3 During the certification process **you shall** check that the provider's service and its marketing material and any other relevant material aligns with the usage guidelines published on GOV.UK.

6.4.4 **You shall** check compliance with the usage guidelines on a regular basis, as per the certification cycle. Provider's non-compliance or misuse **shall** be treated as a non-conformity.

6.5 **Scheme type**

6.5.1 Type 6 certification scheme focuses on evaluating that a product, process, or service meets specific requirements through ongoing, continuous surveillance. This **scheme** is type 6 and mainly applicable to certification of services and processes.

6.5.2 Although services are considered as being generally intangible, the determination activities are not limited to the evaluation of intangible elements (for example, effectiveness of an organisation's procedures, delays and responsiveness of the management).

6.5.3 In some situations, the tangible elements of a service **can** support the evidence of conformity indicated by the assessment of processes, resources and controls involved. For example, the ease of use of a biometric provision for persons with a physical disability. As far as processes are concerned, the situation is very similar. For example, the determination activities for threat intelligence or incident reporting **can** include testing and inspection of samples of the resultant incident log and analysis, if applicable. For both services and processes, the surveillance part of this **scheme should** include periodic audits of the management system and periodic assessment of the service or process (ISO/IEC 17067:2013 clause 5.3.8).

6.5.4 Certification will be for products, systems, services and processes used by organisations that want to provide digital verification products and services and based on ISO 17065 and the additional requirements required by **us** as **the scheme owner**.

6.5.5 **Providers**

6.5.5 a Based on the definition of the roles in **the trust framework**, the following specific services are in the scope of **the scheme**:

6.5.5.a (i) an identity service provider (IDSP)

6.5.5.a (ii) an attribute service provider (ASP)

6.5.5.a (iii) an orchestration service provider (OSP)

6.5.5.a (iv) a holder service provider (HSP)

6.5.5.a (v) a component service provider (CSP)

6.6 Supplementary codes

6.6.1 In addition to certification against **the trust framework**, service providers **can** also get certified against **supplementary codes**.

6.6.2 The **supplementary codes** against which **you can** provide certification are detailed in **List of supplementary codes**.

6.6.3 **You** shall **not** associate certification against these **supplementary codes** or **the trust framework** with certification against any other external requirements.

6.7 Liability

6.7.1 **We** do not accept liability for outcomes against this **scheme**. **You**, and any organisation **you** certify, **should** have appropriate contractual arrangements in place to manage issues relating to liability.

6.8 Principles

6.8.1 CABs, **auditors**, and any other entities that operate **the scheme shall** follow the principles below based on ISO/IEC 17065. Further explanation and expansion of these principles can be found in **the Conformity assessment body principles and code of ethics**:

6.8.1 a Impartiality: The operation and implementation of this **scheme** will be impartial, so that it can provide confidence in its outcomes. Any conflicts of interest are mitigated throughout the operation of the scheme.

6.8.1 b Openness: This **scheme** will apply openness by disclosing and giving access to appropriate information, while respecting confidentiality. This includes access to the scheme requirements.

6.8.1 c Transparency: This **scheme** will be operated and administered in a transparent manner. Transparency means that this scheme has been developed to be accessible, in a non-discriminatory manner, to all interested parties.

6.8.1 d Improvement: **We** will measure the **scheme**'s impact and demonstrate progress towards its intended outcomes, and regularly integrate learning to improve and to increase the benefits for end-users.

6.8.1 e Relevance: This **scheme** has been developed in response to market needs. It is designed to be fit-for-purpose and to meet those market needs.

6.8.1 f Engagement: A balanced and representative group of interested parties is engaged in the development and management of **the scheme**.

6.8.1 g Truthfulness: This **scheme** is developed with the aim that the outcomes achieve the intended results and any communication, including claims, is a true and fair reflection of outcomes.

6.8.1 h Efficiency: All the components of this **scheme** are structured to deliver measurable, quality outcomes. This **scheme** contains the necessary requirements to achieve the intended outcomes and does not overburden participants.

7 Requirements for the conformity assessment bodies

7.1 A CAB carrying out conformity assessment and certification against the present document **shall** be accredited under:

7.2 ISO/IEC 17065

7.3 the UK digital verification services trust framework certification scheme

7.4 **You shall** conduct conformity assessments and certification against the present document in accordance with the ISO/IEC 17065 standard and **the scheme**.

7.5 **Certification scheme owner approval for conformity assessment bodies**

7.5.1 **You shall** get **our** approval, prior to accreditation, so that **you may** undertake conformity assessment activities against this **scheme** with explicit intention of getting **accredited** by UKAS against this **scheme**.

7.5.2 **You shall** maintain your **approved** status at all times when certifying under **the scheme**.

7.5.3 **You shall** be approved if:

7.5.3 a **you apply** to **us** to become an **approved** CAB. The CAB application **shall** include information as defined in the application section of this document; and

7.5.3 b **we** are satisfied that **you** meet the requirements for approval as defined in section 7.7; both at the point of application and on an ongoing basis.

7.5.4 Any conformity assessment **you** conduct when **you** haven't been **approved** or were not **approved** at the time **you** carry out the conformity assessment **shall not** be valid under **the scheme**.

7.5.5 Certificates **shall** only be valid under **the scheme** if they are issued by an **approved** CAB.

7.6 Application for approval

7.6.1 **You shall** apply to us for a **letter of approval**.

7.6.2 **You shall** do so by providing:

7.6.2 a a description of conformity assessment activities **you** intend to carry out

7.6.2 b a confirmation that **you** meet all the necessary requirements as defined by **us**

7.6.2 c a confirmation you are applying for a **letter of approval** with the intention of getting **accredited** by UKAS against **the scheme**

7.6.3 **We shall** maintain an application form on GOV.UK. **You shall** use this form to apply for approval.

7.6.4 **We shall** publish a list of **approved** CABs on GOV.UK.

7.7 Conditions of approval

7.7.1 To obtain and maintain approval, **you shall**:

7.7.1 a operate in line with the requirements of **the scheme** as set out in the documentation we provide.

7.7.1 b operate in line with the additional requirements set out in the **letter of approval**, a template for which is included in Annex D.

7.7.1 c operate in line with ISO 17065 and associated normative references as specified by us.

7.7.1 d provide reasonable data to **us** about **your** performance as a CAB to assist with policy development, as requested by **us**, unless otherwise prohibited in law.

7.7.1 e implement other such operational requirements as determined by **us** on an ongoing basis, with **us** providing reasonable notice.

7.7.1 f positively promote **the scheme** as part of your ongoing business.

7.8 **Letter of approval**

7.8.1 If **your** application is successful **we shall** issue you with a letter of approval.

7.8.2 The **letter of approval shall** confirm that **you** meet the key requirements for CABs, as set out by **us**, to obtain and maintain **approved** status. **You shall** share the **letter of approval** with UKAS before starting the accreditation process against this **scheme**.

7.8.3 If **you** are approved by **us**, **you shall** apply for, or hold, accreditation to certify services against **the trust framework**.

7.8.4 **You shall** inform UKAS of any changes to **your approved** status. **You shall** do that within the period of 30 calendar days.

7.8.5 A proforma for the **letter of approval** is contained in Annex D.

7.9 **Withdrawal of approved status**

7.9.1 **We may** withdraw **approved** status from **you** if **you** no longer conform to the conditions of approval or lose **your** UKAS accreditation against this **scheme**.

7.9.2 Before withdrawing **your approved** status, **we shall**, by written notice, inform **you** of our intention to do so. The written notice shall:

7.9.2 a state the reason(s) why **we** intend to withdraw **your approved** status

7.9.2 b explain that **you may** make written or oral representations to **us** about our intention to withdraw your approved status

7.9.2 c state the period within which **you may** make those representations

7.9.3 The period within which **you may** make representations to **us** about our intention to withdraw your **approved** status **shall not** be less than 21 calendar days, beginning on the day on which the notice is given.

7.9.4 **We shall not** decide to withdraw your **approved** status unless or until **we** have considered all representations made by **you**.

7.9.5 If **we** decide finally to withdraw your **approved** status **we shall**, by written notice, inform **you** and UKAS. **We shall** remove **you** from the list of **approved** CABs.

8 Certification process

8.1.1 The present **scheme** describes the requirements for certification of service providers against the trust framework requirements. This includes provider criteria, and the related controls, which should be sufficient to demonstrate a service's conformity with all the relevant rules in **the trust framework** in such a way that the requirements:

8.1.1 a are organised per type of service (such as identity service provider, orchestration service provider and so on)

8.1.1 b are organised per trust framework requirement as applicable to a specific type of service

8.1.1 c include a sufficient set of criteria to confirm that the assessed **service** meets the applicable trust framework requirements

8.1.1 d ensure that all relevant aspects of the **service** activities are fully covered

8.1.1 e follow the outcome-based approach to the trust framework's requirements. Do not impose specific ways to implement the applicable requirements (in particular, no specific standard for the assessed **service provider** to implement the applicable requirements)

8.1.2 **You shall:**

8.1.2 a demonstrate that criteria are suitable for confirming that a **service** meets the applicable requirements needed to support the evaluation. This is particularly important where the evaluation criteria are based on standards and publicly available specifications

8.1.2 b allow separate certification of services against specific standards, where applicable under sector specific scheme processes

8.2 Product or product group to be certified

8.2.1 Based on the definition of the roles in **the trust framework**, the following specific services are in the scope of **the certification scheme**:

8.2.1 a an identity service provider (IDSP)

8.2.1 b an attribute service provider (ASP)

8.2.1 c an orchestration service provider (OSP)

8.2.1 d a holder service provider (HSP)

8.2.1 e a component service provider (CSP)

8.3 **Name of the scheme**

8.3.1 **UK digital verification services trust framework certification scheme**

8.4 **Methods of conformity assessment**

8.4.1 ISO/IEC 17067 scheme type 6:

8.4.1 a initial review of provider and service design

8.4.1 b initial assessment of provider and service implementation

8.4.1 c initial assessment of provider and service operations

8.5 **Surveillance**

8.5.1 Assessment of the:

8.5.1 a provider and service design changes

8.5.1 b provider and service supporting processes

8.5.1 c provider and service operations

8.5.1 d management system

8.5.1 e provider and service's publicly available information regarding ongoing adherence to requirements in relation to its certification & registration status and its use of trust mark (as applicable).

8.6 **Standards, guidance and normative documents**

8.6.1 **Required**

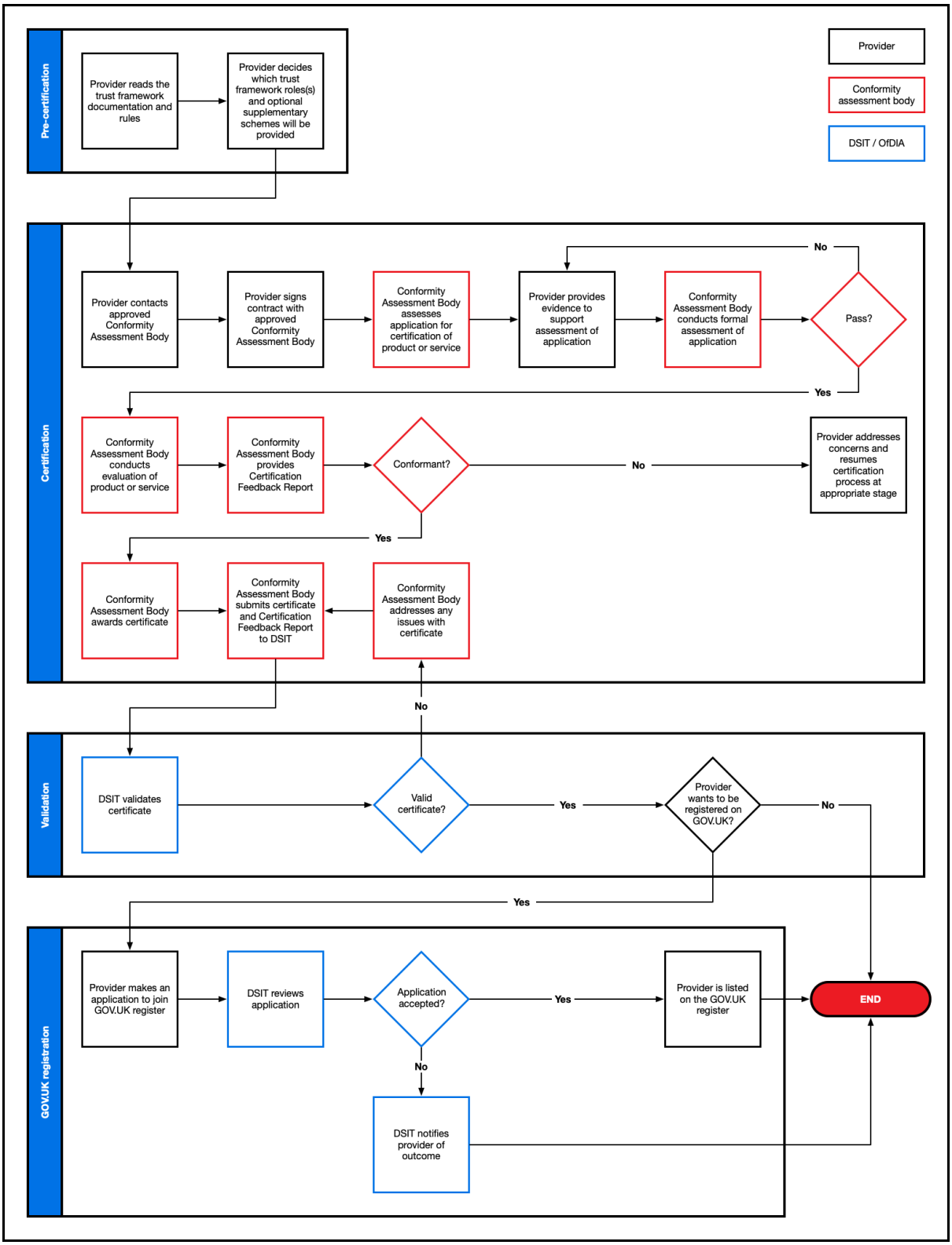
8.6.1 a **UK digital verification services trust framework v1.0**

8.6.2 **Supporting standards and guidance**

8.6.2 a As found in **the trust framework**, table of standards, guidance and legislation

8.7 **Process flow**

8.7.1 An overview of the certification process is described in the diagram below.



9 Application

9.1 Process overview and activities

9.1.1 In this process, you shall perform a set of preparation activities aiming to define and agree on the plan and scope of the conformity assessment. This initial stage will also help set:

9.1.1 a the timing of the evaluations

9.1.1 b the exact locations where the stages will take place

9.1.1 c an assessment and certification proposal regarding the desired area of certification

9.1.1 d the assessment and certification agreement terms and conditions

9.1.2 **You shall** ensure that the information you request from the service provider meets the minimum information included in the service provider application guidance provided by us.

9.2 Application review

9.2.1 The purpose of performing an application review is to determine if sufficient information has been received from the applying organisation to prepare for the certification evaluation.

9.2.2 Determining applicant eligibility

9.2.2 a **You shall** be responsible for determining whether a product, process or service making up the digital verification service presented by a potential client meets the scope for a trust framework certification, and which role the service covers.

9.2.2 b **You may** request our guidance in this matter. If the service provider does not agree with **you**, **you may** refer the complaint to **us** for our consideration.

9.2.2 c From this information **you can** determine the evaluation size for each location in scope in order to prepare a suitable proposal for the certification evaluation.

9.3 Process overview and activities

9.3.1 The process of performing an application review consists of several subprocesses.

9.3.2 **Review the application**

9.3.2 a **You shall** review the application from the service provider to determine if sufficient information is provided to scope the evaluation requirements. As part of the review, the following items **shall** be assessed:

9.3.2.a (i) the information as provided about the service provider and the service is sufficient for the conduct of the certification process

9.3.2 b All associated business risks, areas of activity and types of sites in scope are outlined by the service provider so they can be understood by **auditors**:

9.3.2.b (i) any known difference in understanding between **you** and the service provider which can be resolved, including agreement regarding standards or other normative documents

9.3.2.b (ii) the scope of certification sought is defined (that is, the service and, if applicable, specific components in scope including any **white labelling** activities)

9.3.2.b (iii) the means are available to perform all evaluation activities

9.3.2.b (iv) assessing contractors, subcontractors, franchisees, and so on where all or part of the service delivery is contracted or outsourced

9.3.2.b (v) **you** have the competence and capability to perform the certification activity, and

9.3.2.b (vi) the availability of the required competencies can be confirmed.

9.3.2.b (vii) the intention of the service provider to get their service(s) published on the register.

9.3.2 c All details **shall** be documented in the Application Review and used to determine if the appropriate competencies are available within your CAB. The decision to undertake certification **shall** be justified in the Application Review.

9.3.2 d You **shall** complete a legally enforceable contract, inter alia, that covers all relevant requirements of ISO17065.This contract **shall** either include the terms of a GDPR Data Processing/Sharing Agreement relating to both parties or those terms **shall** be included

in a separate contract.

9.3.3 **Conduct checks on the applicant in line with our requirements**

9.3.3 a **You shall** carry out checks on the provider wishing to certify their product, process or service, before starting certification. Checks will be in line with requirements **we** set out in the trust framework. The checks will include:

9.3.3.a (i) that the service provider is a legitimate entity and is registered with the Companies House or equivalent (for other jurisdictions) and has relevant number (Charities Commission registration number, Data Universal Numbering System (DUNs) number, Legal Entity Identifier (LEI) or other information that identifies the provider as a registered entity in the UK or in another jurisdiction), as specified in section 11.1.d of **the UK digital verification services trust framework 1.0.**

9.3.3.a (ii) that the directors of the service provider do not have any restrictions or constraints to carry out their duties. This would include, but is not limited to, checks for bankruptcy proceedings against or court summons for the directors.

9.3.3.a (iii) the service provider (and parent company where applicable), ultimate beneficial owners, company directors and people with significant control do not appear on UK sanctions list (which can be downloaded from GOV.UK website).

9.3.3.a (iv) the service provider is not involved in any outstanding proceedings which could affect the provision of the digital verification service. This could include, but is not limited to, proceedings in relation to patent disputes, court orders, criminal or small claims court proceedings.

9.3.3.a (v) the service provider does not have any convictions or pending sanctions cases relating to corruption, bribery, money laundering, terrorism financing or fraud as defined in law such as the Money Laundering Regulations, and the Fraud Act (2006).

9.3.3.a (vi) The service provider has adequate financial resources for the provision of the product, service or process they wish to certify, including potential liabilities.

9.3.3 b **You shall** do the above checks via appropriate means so that **you can** satisfy yourself that the service provider meets those requirements.

9.3.4 **Determine evaluation time**

9.3.4 a The time you allocate to evaluation activities **shall** be based on following factors:

9.3.4.a (i) size of the service scope

9.3.4.a (ii) complexity of the service

9.3.4.a (iii) type of business performed within scope of the service

9.3.4.a (iv) extent and diversity of technology utilised in the implementation of the various components of the service

9.3.4.a (v) number of sites and location of sites

9.3.4.a (vi) extent of testing or sampling of the services or processes

9.3.4.a (vii) previously demonstrated performance of the service

9.3.4.a (viii) extent of outsourcing and third-party arrangements used within the scope of the service

9.3.4.a (ix) standards, publicly available specifications and regulatory requirements that apply to the certification, and

9.3.4.a (x) existing certifications, including whether the service provider has been assessed against the trust framework before.

9.3.4 b This **certification scheme** expects that the usual evaluation activities include:

9.3.4.b (i) conducting the opening meeting

9.3.4.b (ii) performing document review while conducting the evaluation

9.3.4.b (iii) testing/sampling of the services/processes

9.3.4.b (iv) communicating during the evaluation

9.3.4.b (v) assigning roles and responsibilities of guides and observers

9.3.4.b (vi) collecting and verifying information

9.3.4.b (vii) generating findings

9.3.4.b (viii) documenting results of all evaluation activities prior to review

9.3.4.b (ix) preparing conclusions in a certification feedback report

9.3.4.b (x) conducting the closing meeting

Note: The template for the certification feedback report that **you** produce **shall** be provided as an external document

9.3.4 c The time **you** allocate for the evaluation **should** be calculated using all of the above sets of factors and will be documented in a justification document or equivalent document for any evaluations carried out on the service.

9.4 Preparing the proposal

9.4.1 Based on the positive evaluation of a potential service provider's certification application, **you shall** prepare a proposal. This internal process is described in Section 4 of the "General Procedures and Processes" - ISO/IEC 17065.

9.5 Certification efforts

9.5.1 **You shall** allow **auditors** sufficient time to undertake all activities relating to an initial certification, surveillance or recertification.

9.5.2 Certification evaluations **may** include:

9.5.2 a remote evaluation techniques such as interactive web-based collaboration

9.5.2 b teleconferences or other remote means of verification of the organisation's processes

9.5.2 c on-site assessments

9.5.3 Data protection and privacy requirements must still be met in the use of the above.

9.5.4 All activities **shall** be identified in the evaluation plan, and the time spent on these activities may be considered as contributing to the total duration of evaluation. In instances where **you** plan an evaluation for which the remote evaluation activities represent more than 30% of the planned on-site duration, **you shall** justify the evaluation plan and maintain the records of this justification. **You shall** make this record available to us or UKAS for review.

9.5.5 **We** will not set the number of days required for certification. **You shall** set the time needed to carry out conformity assessments, certification and any related activities, when applicable. The number of days expected for certification must be transparent and justified based on the factors listed under Determine evaluation time.

9.6 Surveillance

9.6.1 Certificates, once issued, are valid for three years, subject to satisfactory ongoing surveillance, as described below.

9.6.2 The focus of surveillance is to ensure a certified service continues to comply with the certification requirements between certification and recertification evaluations. These **should** take place every 12 months and **shall** take place plus or minus 30 days of the anniversary of the initial certification.

9.6.3 Surveillance activities **may** take place outside of this window if there is any change to the service being offered, or if requested by **us**, or **you** as the CAB, so long as the period between evaluations is not greater than 15 months. **You shall** seek approval from **us** for this extension in advance of the original surveillance timeline expiring. **You shall** maintain records justifying extension period as well as our decision in relation to that request.

9.6.4 If there is evidence that an out of schedule spot audit is needed to maintain certification of a service, this **can** be requested by **you** (as the CAB conducting the audit) or by **us**. **You shall** seek approval from **us** for any such requests. **You may** charge the service provider for these surveillance activities as they are part of the standard certification requirements.

9.6.5 Surveillance activities **should** be scoped to include the conformity assessment preparation and reporting. The effort will depend on the size and complexity of the service provider organisation and implementation of the service it provides, which **could** require visiting less or more locations with associated travel and extra reporting time.

9.6.6 The surveillance activity **shall** be based on defined upgrade paths.

9.6.7 **You shall** document the reasons for the number of person-days in your proposals to service providers and **should** be able to present such information to **us** and UKAS, on request, if required.

9.6.8 **You shall** document results of surveillance evaluations in the certification feedback report. This report **shall** always be provided to the service provider. If, following surveillance activities, **you** have issued a revised

certificate then **you shall** submit the new certificate and the updated report to **us** within 48 hours.

9.7 Certification costs

9.7.1 The costs for carrying out evaluations, certification and any related activities, when applicable, **shall** be indicated in **your** applicable terms and conditions. **You shall** ensure these costs visible, transparent and justified.

10 Selection

10.1 Evaluation criteria

10.1.1 The scope of the evaluation criteria for the certification, re-certification and surveillance is defined by a selection or combination of:

10.1.1 a requirements for all trust framework participants

10.1.1 b identity service provider criteria

10.1.1 c attribute service provider criteria

10.1.1 d holder service provider

10.1.1 e orchestration service provider criteria

10.1.1 f component service provider

10.1.1 g assessing compliance with one or more supplementary codes

10.1.1 h assessing compliance with **white labelling** requirements

10.1.1 i assessing compliance with all relevant parts of UK GDPR

10.1.2 Standards and reference material

10.1.2 a **The trust framework** does not mandate compliance with a specific standard. However, standards can provide controls that allow for specific elements of the normative requirements to be verified or tested, thereby assisting the conformity assessment team in assessing the conformity with a requirement. Where a specific standard is given as an example that would satisfy a particular requirement, **you** must evaluate any alternative approach to ensure this is the case. The standards or reference material are subject to changes, for example, if a new version of the standard is published.

10.1.2 b **The trust framework** requires service providers to operate effective quality management and information security management systems. CABs are required to audit this to ensure that:

10.1.2.b (i) the QMS is fit for its intended use and compatible with ISO 9001,

10.1.2.b (ii) the ISMS meets the requirements of ISO/IEC 27001 or other recognised standard that includes all of the requirements of ISO/IEC 27001

10.1.2 c **You should** avoid re-evaluating service providers for standards for which they can provide evidence of existing certification. Such existing certification must be by a CAB:

10.1.2.c (i) accredited as competent to provide such certifications

10.1.2.c (ii) that has **auditor** competency requirements for the accreditation of CABS against such standards that meet or exceed the relevant competencies for this **scheme**.

10.1.2 d Existing certificates **should** be provided, by service providers, as part of the application process. **You should** ensure that there is at least six months until expiry.

10.2 Preparing the conformity assessment process

10.2.1 Once there is a certification contractual agreement in place between **you** and the service provider, **you shall** request that the service provider make all necessary arrangements for the conduct of the evaluation. This includes the provision for examining documentation and access to all areas, including those of subcontractors and records. This **should** also include internal audits and reports of independent reviews of information security and personnel for the purposes of evaluations and resolution of complaints.

10.2.2 Team selection

10.2.2 a The **auditors** that perform the evaluations **shall** have the proper technical skill set, qualifications and experience to successfully perform certification evaluations. It is essential that **you** are able to guarantee the quality of existing **auditors**, new **auditors** and local resources such as required for management oversight. For each evaluation, **auditors** and technical professionals will be:

10.2.2.a (i) selected based on their competence, training, qualifications and experience

10.2.2.a (ii) monitored for the performance during evaluations

10.2.2 b Requirements toward competencies and experience **shall** have been defined in forms for personnel involved in the certification process, based on the requirements of ISO/IEC 17065. Every member involved in the certification process will fill in the applicable competence and qualification forms, describing competencies and experiences.

10.2.3 **Preparing and sending the evaluation plan**

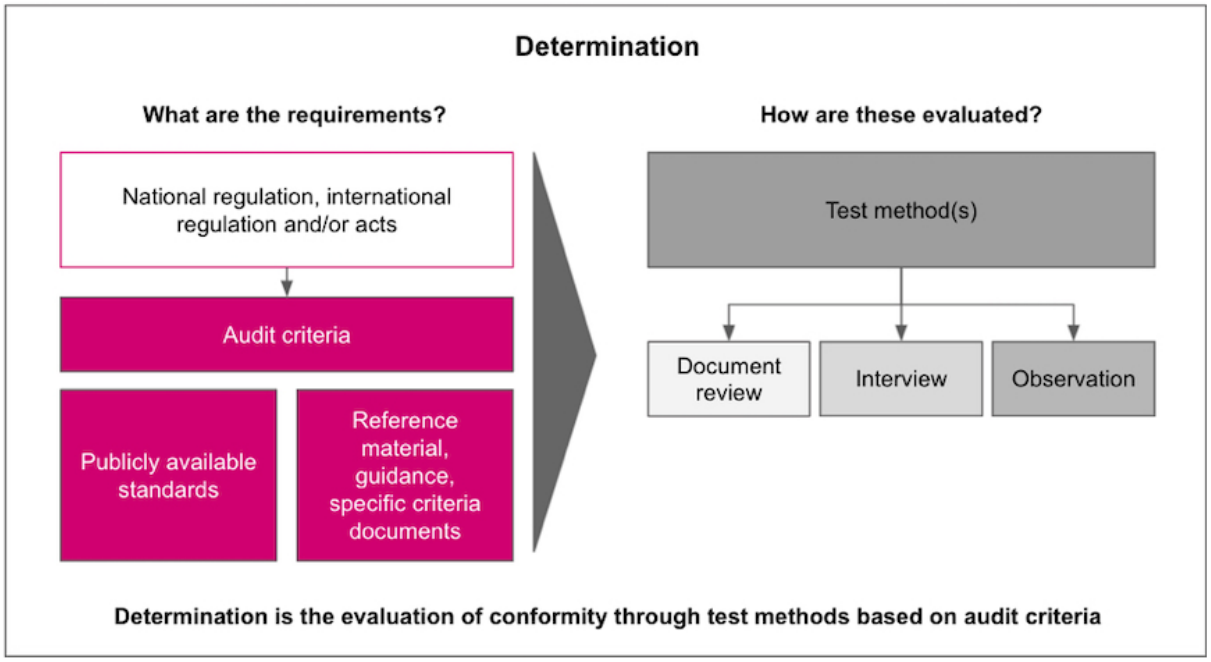
10.2.3 a To ensure both the **auditors** and the service provider are at the correct level of preparedness, **you shall** send an evaluation plan to the organisation prior to the evaluation.

10.3 **Determination**

10.3.1 Upon the conclusion of the certification contractual agreement, **you shall** assign a certification process number and inform the contracting service provider of the name of the responsible certifier and the responsible team leader. The responsible certifier and the **auditors** inform the service provider of the time schedule of the certification process.

10.3.2 **Overview**

10.3.2 a The following visualisation provides an overview of the determination activities.



10.3.3 **Performing the evaluation**

10.3.3 a **You shall** nominate a team leader for the certification activity. The evaluation is then performed by **your** team under the responsibility of the team leader according to **your** requirements and specifications. The responsible certifier, together with the service provider and the team, plans the time schedule of the evaluation and, if necessary, finally clears any questions regarding the evaluation in preliminary meetings.

10.3.3 b The evaluation comprises all activities that are necessary to obtain complete information about the fulfilment of the specified requirements by the certification object. That includes planning and preparation activities, as well as document review, observation and interviews. **You** will also sample the processes and evaluate these against the criteria.

10.3.3 c The **auditors** evaluate the service provider regarding their compliance with the relevant trust framework requirements. During such an evaluation, compliance of the organisational and technical measures of the service provider is evaluated against the applicable requirements.

10.3.3 d The evaluation **shall** include both a design and documentation review and an onsite evaluation to confirm that the implemented service conforms to the applicable normative requirements of the **scheme**.

10.3.3 e Upon completion of the evaluation, the **auditors shall** prepare a certification feedback report forming the basis of the certification decision. **You shall** perform a review of the evaluation using the prepared certification feedback report and monitor compliance with the procedural requirements based on ISO/IEC 17065. The certification decision is recorded. **You shall** inform the service provider of the decision.

10.3.3 f The evaluations **shall** be performed by **auditors** who are either **your** employees or are persons approved by **you**.

10.3.3 g When **you** make a positive certification decision, the certificate **you** issue **shall** reflect the scope of the certification and a validity period of three (3) years. For circumstances where **you** make a negative decision, **you shall** give the service provider the reasons for that

decision along with the findings that need to be addressed before **you** can make a positive certification decision.

10.3.3 h **You** perform your activities predominantly on your own premises. In addition, document reviews, observations and interviews are also performed on the service provider's premises or on any premises used by the service provider to provide its service, in accordance with ETSI EN 319 403, in particular for multi-site sampling.

10.4 Determination activities

10.4.1 Determination activity type

10.4.1 a The evaluation activities or tasks to be performed during the conformity assessment are of the determination activity type audit.

10.4.1 b **We** consider the following evaluation activities or tasks as part of the audit activity type, as defined by ISO 17065 clause 7.4.3 which refers to activities 'such as design and documentation review, sampling, testing, inspection and audit.':

10.4.1.b (i) Interviews

10.4.1.b (ii) Review of documentation and records

10.4.1.b (iii) Observation of processes and activities

10.4.2 Documentation request

10.4.2 a Throughout the conformity assessment, the following documents will typically be required to be provided by the organisation for assessment:

10.4.2.a (i) general information concerning and describing the service and the activities it covers

10.4.2.a (ii) description of the organisational structure of the service provider, including the use made and organisational structure of other parties (subcontractors) that provide parts of the service being audited

10.4.2.a (iii) description of the locations, sizes and functions (tasks and responsibilities) of roles and people involved in the service operational life cycle processes, facility, management, technical security control processes (including other parties used, for example, subcontractors), as well as evidence of their competence or any analysis done for the same

10.4.2.a (iv) service policy and service practices statement and, where required, the associated documentation like IT network infrastructure plans with all relevant systems, manuals and instructions for the operation of the service

10.4.2.a (v) risk assessment related documentation aimed to support demonstration of the requirement of trust framework (as per the list below.)

10.4.2 b Risk assessment related documentation aimed to support demonstration of the requirement of trust framework, including:

10.4.2.b (i) information security risk analysis with risks and opportunities and the actions taken to address them related to all of the interested parties

10.4.2.b (ii) description of the risk assessment and treatment methodology

10.4.2.b (iii) management (in particular, policy management authority, or PMA) review and meeting minutes

10.4.2.b (iv) internal and external audit reports or certifications

10.4.2.b (v) independent reviews of information security

10.4.2.b (vi) a security and personal data breach notification plan aimed to support demonstration of the requirements in data protection legislation

10.4.2.b (vii) evidence of the detection of and reaction to security incidents; nonconformities identified during external or internal audits, including the corrective action taken for each

10.4.2.b (viii) network overview diagrams supporting segmentation and security measures, including controls and risk assessments related to external components

10.4.2.b (ix) detailed verification steps and guidelines documentation training materials for vetting staff

10.4.2.b (x) arrangements to cover liability (certificate and evidence of payment)

10.4.2.b (xi) information security policies and procedures, including, but not limited to those in the list below.

10.4.2 c Information security policies and procedures, including, but not limited to:

10.4.2.c (i) key management

10.4.2.c (ii) logical security

10.4.2.c (iii) personnel security

10.4.2.c (iv) physical security

10.4.2.c (v) backup and recovery

10.4.2.c (vi) incident management

10.4.2.c (vii) business continuity and disaster recovery

10.4.2.c (viii) data protection and asset classification

10.4.2.c (ix) change management

10.4.2.c (x) procedures and controls in support of:

- publication and repository responsibilities
- identification and authentication, when applicable
- service life cycle operational requirements
- facility, management and operation controls
- technical security controls

10.4.2.c (xi) the termination plan of service

10.4.2.c (xii) subscriber agreement and related terms and conditions

10.4.2.c (xiii) risk analysis and business continuity plans relating to the certification status of an **underpinning service**, if the service provider is seeking certification is operating a **white label service**.

10.4.3 **Documentation review**

10.4.3 a In preparation for the evaluation, **auditors shall** obtain and review the documentation on the service provider and the service that is the subject of the evaluation. **Auditors shall** make the provider aware of any further types of information and records that may be additionally required for verification during the document review. In this stage of the evaluation, **you shall** also obtain documentation of the design of the service.

10.4.3 b The objectives of the documentation review are:

10.4.3.b (i) to evaluate and review the service provider's documentation

10.4.3.b (ii) to evaluate service provider locations and site-specific conditions

10.4.3.b (iii) to provide a focus for planning the on-site evaluation by gaining an understanding of the structure and extent of the service

10.4.3.b (iv) to review service provider's status and understanding regarding the normative requirements and specifically those of regulation, policy and standards, in particular with respect to the identification of key performance or significant aspects, processes, objectives and operation of the service

10.4.3.b (v) to collect necessary information regarding the scope of the service, processes and locations of the service provider; levels of controls established and related statutory and regulatory aspects and compliance (for example quality, environmental, legal aspects of operation, associated risks)

10.4.3.b (vi) to perform verification of records regarding legal entity, arrangements to cover liability, contractual relationships between service provider and potential contractors operating or providing sub-component services, and further investigations with regard to the preliminary evaluation of the self-declared partial compliance or noncompliance

10.4.3.b (vii) to evaluate the effectiveness of the service management to make certain the service provider is continually meeting its specified objectives

10.4.3.b (viii) to evaluate if the internal audits and management review are being planned and performed and that the level of implementation of service management substantiates that the service provider is ready for the on-site evaluation.

10.4.3 c During the first stage of the evaluation of the service, the **auditors** analyse and examine the conformity of the documentation required by the normative requirements. If the assessment reveals that the service as described does not meet the requirements, no on-site evaluation is performed. The service provider is given the opportunity then to adjust the documentation to the requirements and have it examined by the **auditors** again.

10.4.3 d If, after the examination of the service provider's documentation, the **auditors** arrive at the conclusion that the service with its documentation meets the requirements of the applicable normative requirements, the on-site evaluation is performed as the second stage of the conformity assessment process.

10.4.4 **On-site evaluation**

10.4.4 a The aim of the on-site evaluation is to determine whether the service is implemented as described in the documentation and complies with the normative requirements. The on-site evaluation is performed on the service providers premises on a date agreed with the organisation in advance.

10.4.4 b The objectives of the on-site evaluation are:

10.4.4.b (i) to confirm that the service provider adheres to its own policies, objectives and procedures

10.4.4.b (ii) to confirm that the implemented service conforms to the applicable normative requirements of the scheme supported by applicable evaluation criteria and abide by the applicable service provider's policies, objectives and procedures

10.4.4.b (iii) to do this, the evaluation will focus on collecting evidence of the service with respect to the following:

10.4.4.b (iv) implementation of service requirements

10.4.4.b (v) service-related organisational processes and procedures

10.4.4.b (vi) service-related technical processes and procedures

10.4.4.b (vii) implemented information security measures for the service, including IT network protection

10.4.4.b (viii) service-related products (trustworthy systems), such as cryptographic modules

10.4.4.b (ix) physical security of the relevant service provider sites

10.4.4 c The on-site evaluation includes the evaluation of the organisational, structural and technical implementation of the measures described in the documentation for fulfilling the applicable normative requirements.

10.4.4 d To this end, **auditors** gather evidence by document review, observation and interview. If the service provider provides declarations or test results, but they are unable to prove that these have been performed according to the requirements of the scheme, they **shall** not be used as evidence.

10.4.4 e To the extent available, evaluations of other appropriate independent bodies regarding individual components of the service to be evaluated **may** be used. For instance, it is not necessary that **auditors** perform their own evaluations of technical components.

They may use test reports and certificates of other independent bodies for their own evaluation. The responsible certifier and the **auditors shall** agree upon the reuse extent, ensuring that reused results are applicable for the certification of the compliance of the provider against the normative requirements.

10.4.4 f Where all or part of the service delivery is contracted or outsourced, **you shall** ensure that the overall quality and security of the service being evaluated is not prejudiced by any insecurities in these external service elements. This **may** include an evaluation of the external provider if **you** deem it necessary.

10.4.5 **Evaluation criteria**

10.4.5 a The evaluation of the service provider and the service it provides **shall** take the form of an evaluation carried out against defined criteria that:

10.4.5.a (i) take into account specificities of the type of service to be assessed

10.4.5.a (ii) ensure that all aspects of the service provider activity are fully covered

10.4.5.a (iii) are based on standards, publicly available specifications or regulatory requirements comply with the requirements specified by the **scheme**.

10.4.5 b **You shall** specify detailed controls and processes in work plans. These also indicate the recommended determination activity for each of the controls/processes.

10.4.6 **Evaluation**

10.4.6 a For each of the determination activity types, **we** define rules to allow the **auditor** to determine whether a control can be considered effective or ineffective (for example, a finding).

10.4.7 **Interview**

10.4.7 a A control that is covered through an interview **should** be considered effective if the interview provides sufficient evidence that the control is in place and performed according to the definition of the control requirements through a detailed description, such as (if applicable):

10.4.7.a (i) a walk-through of how the control is performed

10.4.7.a (ii) who performed the control

10.4.7.a (iii) a description of the process in which the control is present.

10.4.7 b **You should** consider a control that is covered through an interview ineffective if the interview is not able to provide evidence that the control is in place or that it is performed according to the definition of the control or its requirements.

10.4.8 **Review of documentation and records**

10.4.8 a **You should** consider a control that is covered through a review of documentation or records effective if the review provides sufficient evidence that the control is in place and performed according to the definition of the control requirements through a detailed description, such as (if applicable): a detailed explanation of the control or the process in which the control is present or evidence that a control was performed (for example, based on logs or audit records).

10.4.8 b **You should** consider a control that is covered through a review of documentation ineffective if the review is not able to provide evidence that the control is in place or that it is performed according to the definition of the control or its requirements.

10.4.9 **Observation of processes and activities**

10.4.9 a **You should** consider a control that is covered through observation of processes and activities effective if the observation (of the **auditor**) provides sufficient evidence that the control is in place and performed according to the definition of the control requirements through a detailed description, such as (if applicable): an observation that a control is performed (for example through on-site observation) within a process.

10.4.9 b **You should** consider a control that is covered through observation of processes and activities should be considered ineffective if, during observation, there is insufficient evidence that the control is in place or that it is performed according to the definition of the control or its requirements.

10.4.10 **Sampling methodology**

10.4.10 a Where it is appropriate for the evaluation to include sampling, the sampling methodology should:

10.4.10.a (i) be representative of the requirements that are to be fulfilled

10.4.10.a (ii) use the intended service delivery process

10.4.10.a (iii) consider all relevant functions, processes and sites (physical or virtual) of the service provider that impact on fulfilment of requirements

10.4.10.a (iv) consider all outsourced activities that have an impact on the service delivery.

10.4.11 **Multi-site sampling**

10.4.11 a Where the organisation has a number of sites where the service is delivered to customers in-person, the team will consider using a sample-based approach to a multiple-site evaluation based on the following requirements:

10.4.11.a (i) security for all applicable site is administered under control of the service provider's security policy administrations

10.4.11.a (ii) all applicable sites are subject to the service provider's security management review program.

10.4.11 b **You shall** consider the following during sampling of sites:

10.4.11.b (i) type of different sites as per application review form and in the Service Description

10.4.11.b (ii) a representative number of sites to be sampled, taking into account the following:

10.4.11.b (iii) the results of internal audits of the central site and the other sites

10.4.11.b (iv) the results of management review

10.4.11.b (v) variations in the size of the sites

10.4.11.b (vi) variations in the business purpose of the sites (including number of roles undertaken at the site)

10.4.11.b (vii) complexity of the service (including level of confidence of resulting digital identity profile)

10.4.11.b (viii) complexity of the information systems at the different sites

10.4.11.b (ix) variations in working practices

10.4.11.b (x) variations in activities undertaken

10.4.11.b (xi) potential interaction with critical information systems or information systems processing sensitive information

10.4.11.b (xii) whether the site is operated by a subcontractor or other external organisation (including where this is as a result of all or part of the service delivery being contracted or outsourced)

10.4.11.b (xiii) any differing regulatory requirements

10.4.11 c The sample **should** be partly selective based on the above points and partly nonselective and result in a range of different sites being selected without excluding the random element of site selection.

10.4.11 d Every site of the organisation subject to significant threats to assets, vulnerabilities or impacts should be included in the sampling program.

10.4.11 e The final sample size for **your** initial evaluation is based on the number of sites the service operates over. The sample size is the square root of this number of sites, plus one.

10.4.11 f For example, if a service operates across 27 sites, the square root will be 5 (rounded down to the nearest whole number of sites). You need to add one more site to this, so the sample size would be 6 sites.

10.4.11 g The service provider **shall** tell **you** the percentage of in-person service delivery instances conducted at each site. **You shall** include the busiest 25% in your sample of 6, and select the remaining 75% of sites at random.

10.4.11 h **You shall** design surveillance programs in the light of the above requirements and **shall**, within a reasonable time, cover all site operations, unless it can be demonstrated this does not impact the results of the evaluation.

10.4.11 i If you observe nonconformity, either at the main operational site or at a single site, **you shall** ensure the corrective action procedure apply to the main operational site and to all sites of the operations that may be impacted by the same nonconformity.

10.4.11 j The evaluation **shall** address the service provider’s main site activities to make certain that central security administration is applied to all sites at the operational level.

10.4.11 k A justification memo or equivalent document **shall** be used to justify the number of sites being sampled in the evaluation.

10.4.12 **Evaluation time**

10.4.12 a **You shall** allow auditors sufficient time to undertake all activities relating to an initial certification, surveillance and re-certification. The time allocated **shall** consider the following factors:

10.4.12.a (i) the size of the service provider's operation used to deliver the service (for example, the number of information systems used, number of employees, number of activities performed)

10.4.12.a (ii) complexity of the service in terms of roles and levels of confidence (if applicable)

10.4.12.a (iii) extent and diversity of technology utilized in the implementation of the various components of the service

10.4.12.a (iv) number of sites (see above)

10.4.12.a (v) previously demonstrated performance of the service

10.4.12.a (vi) extent of outsourcing and third-party arrangements used within the scope of the service

10.4.12.a (vii) the use of/providing of underpinning service for white labelling purposes.

10.4.12.a (viii) number of profiles and impact of effort

10.4.12.a (ix) risk and impact of effort

10.4.12 b **You shall** document the justification of the amount of time used in any initial certification, surveillance and re-certification.

10.4.12 c Having reviewed the factors given above, the guidance provided in Annex A for the calculation of Evaluation Time **should** then be applied.

10.5 **Review**

10.5.1 **Review process**

10.5.1 a **You shall** assign at least one person to review all information and results related to the evaluation (including the certification feedback report). The review **shall** be carried out by person(s) who have not been involved in the evaluation process.

10.5.1 b **You shall** document recommendations for a certification decision based on the review, unless the same person completes the review and certification decision concurrently.

10.6 Decision

10.6.1 Certification decision

10.6.1 a **You shall** ensure that the persons or committees that make the certification decisions for granting or refusing certification, expanding or reducing the scope of certification, suspending or restoring certification, withdrawing certification or renewing certification are different from those who carried out the evaluations. The individual(s) appointed to conduct the certification decision **shall** have appropriate competence.

10.6.1 b The certification decision can be one of the following two categories:

10.6.1.b (i) **certified**: the evaluated service fulfils the criteria and is certified as conforming

10.6.1.b (ii) **not certified**: the evaluated service is not certified as conforming.

10.6.2 Certification documentation

10.6.2 a At the end of the process, you shall issue a conformity assessment report called the “certification feedback report” containing all of the results of the evaluation to the service provider.

10.6.2 b If **you** make a positive certification decision, **you shall** issue a certificate to reflect the scope of certification, with a validity period of a maximum of three years. The contents of the certificate **shall** be in accordance with the requirements specified in certificate requirements. There will be one certificate per service, but the certificate can cover multiple roles and supplementary codes, as defined in the **scheme** and **trust framework,** including possible restrictions on combination of roles and/or supplementary codes.

10.6.2 c When **you** reach a positive certification decision you shall submit the following documents to us:

10.6.2.c (i) Certificate

10.6.2.c (ii) Certification feedback report

10.6.2.c (iii) Signed terms of use for the trust mark

10.6.2 d **You shall** also provide the above documentation to us when there is a change in scope (extension or reduction of), in addition to positive certification decision.

10.6.3 **Findings**

10.6.3 a **You** rate the findings based upon the risk they pose to the service provider's organisation.

10.6.3 b Guidance for the classification of the findings is as follows:

10.6.3.b (i) minor nonconformity – a single identified gap or a concern in meeting a requirement of the standard or criteria documents in scope, which would not in itself raise significant doubt as to the capability of the service provider to achieve its objectives. Certification can be awarded with open non-conformities as long as you (the CAB) set a reasonable timeframe for closure. We consider within a range of up to six weeks acceptable.

10.6.3.b (ii) major nonconformity – an absence of, or the repeated failure to implement and maintain, one or more required mandatory standard elements or criteria documents in scope, or a situation that would, based on objective evidence, raise significant doubt as to the capability of the service provider to achieve its objectives.

10.6.3 c **You shall** not award certification while there are open major nonconformities. **You shall** set a timeframe of up to one month for closure. After this time, the client **shall** provide evidence of closure and **you shall** check for compliance.

10.6.3 d When **you** note findings during a conformity assessment, **you shall** follow up to make sure that the service provider takes the necessary measures to remediate these findings. **You may** do this through a surveillance evaluation.

10.6.4 **Register of digital verification services**

10.6.4 a **We shall** maintain a Register of digital verification services (the register) that have been certified by accredited CABs and have successfully applied to be on the register. **We shall** make the register publicly accessible with up-to-date information about the service provider and the certified service(s) they provide.

10.6.4 b To be on the register the service provider **shall**:

10.6.4.b (i) have a valid certificate

10.6.4.b (ii) apply to join

10.6.4.b (iii) pay any applicable fees

10.6.4 c **You shall** provide us with the certificate and associated certification feedback report to enable the service provider to apply to join the register. **We shall** use these documents to assess whether the certificate is valid for the purposes of registration.

10.6.4 d If **we** accept the certificate as valid, **we shall** invite the service provider to submit an application to join the register.

10.6.4 e After the service provider submits their application, **we shall** undertake due diligence checks to ensure the service provider complies with the trust framework requirements.

10.6.4 f If **we** are satisfied, as a result of the due diligence check, that the service provider has satisfied the registration requirements, **we shall** add the service provider and its certified service(s) to the register.

10.6.5 **Removal from the register**

10.6.5 a be listed on the register, all of the following requirements are required to be fulfilled:

10.6.5.a (i) A service provider holds a valid certificate for the service(s) it wants to register

10.6.5.a (ii) the CAB that evaluated the service has provided us with the certificate and certification feedback report for that service

10.6.5.a (iii) **We** have validated that the certificate conforms to the requirements of the **scheme**

10.6.5.a (iv) **We** have completed a ‘due diligence’ check on the service provider

10.6.5.a (v) the service provider has paid any applicable fees

10.6.5 b If any of the above requirements have not been fulfilled, we will not list service provider and its service on the register.

10.6.5 c If a service is already listed on the register, and the expiry date on its original certificate has passed, **we shall** temporarily remove a service provider and its service from the list until all of the above requirements have been fulfilled. **We shall** do this even if the service has recently been re-certified.

10.6.5 d In order to ensure it maintains a continuous certification and presence on the list, a service provider **should** engage its CAB well in advance of its certificate expiry date.

10.6.5 e In the event of recertification, **you should** provide **us** with a new certificate and certification feedback report for the certified service. **You should** do this at least 30 days in advance of the previous certificate's expiry date to enable continuous registration.

10.6.5 f Up to 60 days of remaining time on the previous certificate **may** be rolled over to a new certificate, following a full evaluation of a service, to support continuous certification and registration. This ensures a service provider does not 'lose' time on their expiring certificate unnecessarily.

10.6.5 g A service provider that is not listed on the register **shall not** claim to be registered, and a service provider that does not have a valid certificate must not claim to be certified against **the trust framework.**

10.6.6 **Issued, suspended and withdrawn certifications**

10.6.6 a **We** require **you** to provide information of issued, suspended and withdrawn certifications to us.

10.6.6 b For issued certifications, **you shall** provide this information to **us** within 48 hours of granting certification.

10.6.6 c For suspended and withdrawn certificates, **you shall** provide this information to **us**, along with reasoning for suspension or withdrawal, within 24 hours. This is so that we can amend our records, and update the list of certified services as well as other relevant sources in order to avoid any confusion in the market.

10.7 **Changes affecting certification**

10.7.1 There are instances in which certain changes **can** impact the certification of the service, such as when **the scheme** introduces new or revised requirements that affect the service provider. **You shall** make certain these changes are communicated to all service providers. **You shall** verify the implementation of the changes by the service provider and **shall** take action required by **the scheme**.

10.7.2 When the changes affecting certification are initiated by the service provider, due to changes in for example documentation (policies, objectives, and so on) or security-relevant changes, it is the

responsibility of the service provider to provide notification of the change, as agreed to within the certification agreement. The service provider **shall** notify their CAB within 48 hours of those changes happening as noted in **the trust framework**. Based on the nature of the changes, **you shall** agree with the service provider whether a surveillance activity or recertification is necessary and on timelines for either.

10.7.3 The service provider **shall** also notify their CAB if there are any changes in connection with **white labelling**, if relevant. For example, where the service provider is operating a **white-label** service and is informed that there has been a certification-related change to the **underpinning service**.

10.7.4 **You shall** perform an evaluation activity of the service under the following circumstances:

10.7.4 a whenever there are major changes to the scope

10.7.4 b whenever there are major changes to the service provided under the scope

10.7.4 c when there are major changes of IT systems or business processes used by the service provider

10.7.4 d when a major part of the service moves to another location

10.7.5 Appropriate actions will be taken to implement changes affecting the certification in accordance with the defined processes.

10.8 Conditions on expiration, suspending, withdrawing or reducing scope of certification

10.8.1 **You shall** suspend certification in cases when, for example:

10.8.1 a the certified service has persistently or seriously failed to meet certification requirements, including requirements for the effectiveness of the management system, which is indicated in the report following a surveillance evaluation or recertification evaluation

10.8.1 b the service provider does not allow surveillance or recertification evaluations to be conducted at the required frequencies

10.8.1 c the service provider has voluntarily requested a suspension

10.9 Transfer of certifications

10.9.1 a The following is based on IAF MD2[1] which is for Management System certificates but pertinent elements have been used here. Attribution is given.

10.9.1 b This section provides normative criteria on the transfer of service certification between **approved** CABs. The criteria **may** also be applicable in the case of acquisitions of CABs **approved** by **us**. The objective of the transfer guidance is to assure the maintenance of the integrity of service certification issued by one **approved** CAB if subsequently transferred to another.

10.9.1 c This section provides minimum criteria for the transfer of certification. CABs may implement procedures or actions which are more stringent than those contained herein provided that a client service provider's freedom to choose a CAB is not unduly or unfairly constrained.

10.9.2 **Transfer of certification definition**

10.9.2 a The transfer of certification (as defined in the IAF MD2 document) is the recognition of an existing and valid service certification, granted by one **approved** CAB, (hereinafter referred to as the 'issuing CAB'"), by another **approved** CAB, (hereinafter referred to as the 'accepting CAB') for the purpose of issuing its own certification. Multiple certification (concurrent certification by more than one CAB) does not fall under the definition above.

10.9.3 **Eligibility of a certification for transfer**

10.9.3 a **The scheme** will allow for transfer of certificates with the following conditions:

10.9.3.a (i) Minimum disruption to the service provider for whom the transfer needs to be made

10.9.3.a (ii) If you are approached by a service provider who asks to transfer certification of a service to your CAB, you should ensure that the transfer request is not being made:

- to avoid payment to the original CAB

- because the service provider is attempting to avoid closing non-conformities or any other behaviour that could be considered underhand.

1.1.1

[1] GACI equivalent of IAF MD2 will be recognised by this scheme, when published.

10.9.3.a (iii) In the case where **you** are ceasing to trade, or no longer wish to partake in **the scheme**, **you** will inform each client of **your** intention and the need for them to transfer to another CAB. **You shall** share the list of **approved** CABs that can be approached with **your** clients, but **you shall not** do this in such a way that promotes one CAB over another.

10.9.3.a (iv) **You shall** make clear that there is a window of time in which the transfer can take place.

10.9.3.a (v) In the case where **you** are ceasing to trade, or no longer wish to take part in **the scheme**, **you shall** no longer accept new certifications and **shall** communicate this clearly to prospective clients.

10.9.3 b Only certification issued by a CAB we have **approved shall** be eligible for transfer. **You shall** treat organisations holding certification that is not issued by an **approved** CAB as new clients.

10.9.3 c Only valid certification **shall** be transferred. **You shall not** accept transfer requests for any certificates which are known to be suspended.

10.9.3 d In cases where certification has been granted by a CAB which has ceased trading or which has been removed from the list of **approved** CABs, the transfer **shall** be completed within 180 days, or on expiration of the certification (whichever is sooner). If you are the accepting CAB in such a case, **you shall** inform **us** and UKAS prior to the transfer taking place.

10.9.4 **Pre-transfer review – requirements for accepting conformity assessment bodies**

10.9.4 a **You shall** have a process for obtaining sufficient information to allow you to make a decision on certification, and inform the transferring service provider of this process. This information shall, as a minimum, include arrangements regarding the certification cycle.

10.9.4 b **You shall** carry out a review of the certification of the transferring service provider. **You shall** conduct this review by means of a documentation review. If you identify the need to do so during this review, for example because of outstanding major conformities, **you shall** include a pre-transfer visit to the transferring service provider to confirm the validity of the certification.

Note: The pre-transfer visit is not an evaluation.

10.9.4 c **You shall** determine the competence criteria for personnel involved in pre-transfer review. One or more persons may conduct the review. The individual or group conducting the pre-transfer visit **shall** have the same competence that is required for an audit team appropriate for the scope of certification being reviewed.

10.9.4 d The review **shall** cover the following aspects as a minimum and the review and its findings **shall** be fully documented:

10.9.4.d (i) confirmation that the service's certification falls within the approved scope of the issuing and accepting CABs

10.9.4.d (ii) the reasons for seeking a transfer

10.9.4.d (iii) that the site or sites wishing to transfer certification hold a valid certification

10.9.4.d (iv) the initial certification or most recent recertification evaluation reports, and the latest surveillance report; the status of all outstanding nonconformities that may arise from them and any other available, relevant documentation regarding the certification process. If these evaluation reports are not made available or if the surveillance evaluation or recertification evaluation has not been completed as required by the issuing CAB's evaluation programme, then the organisation **shall** be treated as a new client;

10.9.4.d (v) complaints received and action taken;

10.9.4.d (vi) considerations relevant to establishing an evaluation plan and an evaluation programme. The evaluation programme established by the issuing CAB **should** be reviewed if available; and

10.9.4.d (vii) any current engagement by the transferring service provider with regulatory bodies relevant to the scope of the certification in respect of legal compliance.

10.9.5 *Transfer of certification – requirements for accepting conformity assessment bodies*

10.9.5 a **You shall not** issue certification to the transferring service provider until:

10.9.5.a (i) you have verified the implementation of corrections and corrective actions in respect of all outstanding major nonconformities

10.9.5.a (ii) you have accepted the transferring service provider's plans for correction and corrective action for all outstanding minor nonconformities

10.9.5 b Where the pre-transfer review (document review and/or pre-transfer visit) identifies issues that prevent the completion of transfer, **you shall** treat the transferring service provider as a new client.

10.9.5 c **You shall** explain the justification for this action to the transferring service provider. You shall document the decision and maintain the records.

10.9.5 d If **you** do not identify any problems during the pre-transfer review, **you shall** base the certification cycle on the previous certification cycle. **You shall** establish the evaluation programme for the remainder of the certification cycle.

10.9.5 e The certification cycle for certification is three (3) years, with your surveillance evaluations performed annually.

NOTE: Some certificates issued under **the trust framework 0.4** currently have a two (2) year validity. **You shall** only change these to three (3) year certificates following recertification.

NOTE: **You can** quote the service's initial certification date on the certification documents with the indication that the service was certified by a different CAB before a certain date. Where **you** have had to treat the service provider as a new client as a result of the pre-transfer review, **you shall** begin the certification cycle with the certification decision.

10.9.5 f **You shall** take the decision on certification before **you** initiate any surveillance or recertification evaluations.

10.9.6 Cooperation between the issuing and accepting conformity assessment bodies

10.9.6 a Cooperation between the issuing and accepting CABs is essential for the effective process for transfer and the integrity of certification. When requested, the issuing CAB **shall** provide to the accepting CAB all the documents and information required by this process. Where it has not been possible to communicate with the issuing

CAB, the accepting CAB **shall** record the reasons and make every effort to obtain necessary information from other sources.

10.9.6 b The transferring service provider **shall** authorise that the issuing CAB provides the information sought by the accepting CAB. The issuing CAB **shall not** suspend or withdraw the service's certification following the notification that the service provider is transferring to the accepting CAB if the service provider continues to satisfy the requirements of certification.

10.9.6 c The accepting CAB and/or the transferring service provider **shall** contact us, and UKAS, when:

10.9.6.c (i) the requested information they have requested has not been provided

10.9.6.c (ii) the issuing CAB suspends or withdraws the transferring service provider's certification without cause

10.9.6 d Where the issuing CAB does not cooperate with the accepting CAB, or suspends or withdraws the transferring service provider's certification without cause, the accepting CAB shall follow UKAS process for addressing the situation, including the suspension or withdrawal of the accreditation.

10.9.6 e If **you** are the accepting CAB, **you shall** email the issuing CAB to inform them once you have issued the certification. **You shall** also inform the service provider and us.

10.9.6 f If **you** are the accepting CAB, **you shall** produce the certificate in line with the certificate requirements as specified by us.

10.10 Attestation

10.10.1 Publication of certificates

10.10.1 a **You** should maintain an accessible public register of services you have certified.

10.10.1 b Service providers are entitled to use the certificate in connection with the certified service in publications, catalogues, and so on, in compliance with the certification conditions. In case of an incorrect reference or misleading use by the service provider, then **we** and/or the relevant CAB are entitled to withdraw the certificate.

10.10.1 c CABs perform regularly monitoring the compliance of the service provider's use of the certificates with the applicable terms and

conditions.

10.11 **Complaints and appeals**

10.11.1 CABs **shall** make their complaints and appeals procedures for certification decisions publicly available on their website.

10.11.2 If a complaint relates to the activities of a UKAS accredited CAB or a service provider, in the first instance the complaint should be addressed to them, (that is the UKAS accredited CAB or the service provider). UKAS will only consider complaints where the complainant have given the CAB or service provider the opportunity to investigate and respond in accordance with their respective complaint processes. In situations where the complainant can find no resolution with the CAB or service provider, they can then make a written complaint to UKAS who will go through a structured process.

10.12 **Surveillance**

10.12.1 **You should** perform surveillance activities annually and **shall** perform a minimum of two surveillance evaluations between certification and recertification. **Your** surveillance activities **shall** take place plus or minus 30 days of the anniversary of the initial certification.

10.12.2 Surveillance activities **may** take place outside of this window if there is change to the service being offered or if requested by **us**, or a CAB, so long as the period between evaluations is not greater than 15 months. **You shall** seek approval from **us** for this exception to the ordinary process in advance of the activities taking place. CABs **shall** maintain records justifying extension period as well as **our** decision in relation to that request.

10.12.3 CABs **shall** perform surveillance evaluations in accordance with the surveillance activities defined by ISO/IEC 17067 scheme type 6, through document review, observation and interviews. **You shall** design the sample such that all changes and modifications that have been implemented since the time of the last evaluation are covered.

10.12.4 **You shall** detail, in the applicable evaluation plans, the activities to be performed during the different types of evaluations and assessments.

10.13 **Recertification**

10.13.1 **We** recommend that **you** plan and conduct a recertification evaluation in due time before the certificate expiry date. This is so that such that if

any major nonconformity is found, there is time for the necessary correction and corrective actions to be implemented and verified prior to the certification expiring. In accordance with the requirement given under the relevant part of the 10.6.3. findings of this document, at most **you should** allow one month for the correction.

10.13.2 When recertification activities are successfully completed prior to the expiry date of the existing certification, **you can** base the expiry date of the new certification on the expiry date of the existing certification. The issue date on a new certificate **shall** be on or after the recertification decision.

10.13.3 **You may** roll over a maximum of 60 days of remaining time on an existing certificate to a new certificate.

10.13.4 If **you** have not completed the recertification or are unable to verify the implementation of corrections and corrective actions for any major nonconformity prior to the expiry date of the certification, **you shall not** recommend recertification and **shall not** extend the validity of the certification. **You shall** inform the service provider and explain the consequences to the service provider.

10.13.5 Following expiration of certification, **you can** restore certification within 6 months provided that the outstanding recertification activities are completed, otherwise **you shall** conduct at least on-site evaluations. The effective date on the certificate **shall** be on or after the recertification decision and the expiry date **shall** be based on the prior certification cycle.

11 Uplift routes and timelines to 1.0 trust framework

11.1 The trust framework 1.0 does not specify date when 0.4 trust framework expires. Instead the following will apply:

11.1.1 If a service has an existing certification against 0.4 trust framework the provider will have two options of when to uplift

11.1.1 a They can either ask you to uplift their service's certificate to 1.0 at their next evaluation activity (surveillance audit or recertification), or remain on 0.4 certification

11.1.1 b They can ask you to uplift their service's certification at second evaluation activity if they haven't done so at the first one. If they do not uplift their certification at this point you **shall** forcefully expire their certificate and ask for them to be removed from the register.

11.2 Routes to uplift:

11.2.1 You shall uplift services with existing certificates via any of the below routes:

11.2.1 a Surveillance audit

11.2.1 b Recertification

11.2.1 c Delta assessment – delta assessment being an out of cycle activity that enables you to check only new requirements set out in trust framework 1.0. You **shall** perform delta assessment for services with existing certificates that are already on a three-yearly cycle. This route is not available to anyone else.

11.2.2 For services without existing certification against 0.4 standard process of certification applies.

12 White labelling

12.1.1 **White label** services are certified products, services or processes that are produced by a **first-party** service provider for a **second-party** who intentionally rebrands them to giving users of the service the appearance that the **second-party** created them. The **white label** service is operated by the **first-party** service provider, in whole or in part, with the relationship between both parties being controlled by means of a contract or another legally-binding mechanism.

12.1.2 If a user, when interacting with a service, is visibly and obviously passed to a different organisation's service as part of a wider journey (such that the user is initially interacting with Company A and they are aware that they are temporarily interacting with Company B) then this is not an example of **white labelling** under this scheme. **White labelling** is done intentionally to make Company B invisible to the end user.

12.1.3 As the focus of **white labelling** is related to user experience it does not apply to the orchestration service provider role. **White labelling** does not apply to the role of component service provider as this role is part of normal supply chain processes.

12.1.4 If a service provider wants one of its certified services to become an **underpinning service**, **you shall** evaluate them to ensure they have appropriate controls in place to manage the relationship with any **second-party** that relies upon that **underpinning service** through a **white label** service.

12.1.5 Digital verification services rely on complex supply chains to operate. **You shall** consider the evaluation of supply chains, in addition to consideration of **white labelling**.

12.2 Types of white labelling

12.2.1 There are two approaches to **white labelling** that **may** be certified under this **scheme**:

12.2.1 a First-party **white labelling**

12.2.1 b Second-party **white labelling**

12.2.2 A service provider **shall** apply to **you** for an extension of scope before its service may become an **underpinning service** of either type.

12.2.3 First-party while labelling

12.2.3 a A product, service or process **shall** be considered as a **first-party white label service** if all of the following conditions apply:

12.2.3.a (i) the product, service or process operated directly by the organisation seeking certification (that is, the **First-party** service provider)

12.2.3.a (ii) the product, service or process primarily and prominently displays the branding of a **second-party** to give the appearance that the product was produced and is operated by the **second-party**

12.2.3.a (iii) the **first-party** service provider applies for certification of that **white label service**

12.2.4 Second-party white labelling

12.2.4 a A product, service or process **shall** be considered as a **second-party white label** service if all of the following conditions apply:

12.2.4.a (i) the **underpinning service** is not produced directly by the organisation seeking certification (that is, it is a **second-party** relying on a certified **underpinning service** as part of its supply chain)

12.2.4.a (ii) the product, service or process primarily and prominently displays the branding of the **second-party**

12.2.4.a (iii) the **second-party** applies for certification of that **white label** service itself, and not the **first-party** service provider

that built or is operating the **underpinning service**

12.2.5 **Other approaches**

12.2.5 a **We** do not permit any other approaches to **white labelling** under the scheme, however, **co-branding** is permitted (. Refer to Section 12).

12.3 **Liability for white label services**

12.3.1 Regardless of the approach to **white labelling** adopted between the two parties, the organisation that holds the certificate for a service **shall** be considered liable for implementing the trust framework rules, unless liability is transferred to another party through an appropriate legally-enforceable mechanism; such as a contract.

12.4 **Evaluation approach**

12.4.1 Contracts underpinning **white label services:**

12.4.1 a **White label services** rely upon contractual and legal arrangements between the **first-party** that builds and operates the **underpinning service** and the **second-party** that has its brand applied to the service.

12.4.1 b **You shall** assess the contractual and legal relationship between **first-parties** and **second-parties** to ensure that they attribute responsibility, accountability and liability to one or both parties for implementing the requirements of the scheme. The contract or other legal arrangements **should** cover all aspects of the trust framework and **shall not** conflict with the requirements of the trust framework or this **scheme** in any way.

12.4.2 **Evaluation of service providers that operate underpinning services for white labelling**

12.4.2 a To conform to the requirements of **the trust framework**, **you shall** evaluate service providers that operate **underpinning service** for the purposes of **white labelling** to ensure that:

12.4.2.a (i) the service provider is not misrepresenting the **certified, registered** or **trust marked** status of any service it operates as a **first-party white label** service provider

12.4.2.a (ii) the service provider has effective processes and procedures in place to ensure that any **second-party** does not misrepresent the **certified, registered** or **trust marked** status of their rebranded service(s)

12.4.2 b The service provider can demonstrate conformity through documentation including policies and contracts with **second-parties**. The service provider can also demonstrate conformity by showing evidence of where it has directly acted to prevent misrepresentation of **certified, registered** or **trust marked** status by **a second-party** it is contracted with.

12.4.2 c **You shall** rely on the methodology in Annex B to sample the documentation and activities of service providers in relation to **white labelling**.

12.4.2 d **You shall** consider any misrepresentation of **certified, registered** or **trust marked** status as a non-conformity under **the scheme**. **You shall** decide whether such misrepresentation is a major or minor non-conformity, and timelines for remediation, in line with the wider requirements of the scheme.

12.4.2 e A non-conformity **can** result in loss of **certified, registered** or **trust marked** status for the **underpinning service** and any **white label** service that relies on the **certified** status of it.

12.4.3 **Evaluation of white label services**

12.4.3 a **White label** services **certified** under this **scheme** rely upon the original **underpinning service** maintaining its **certified** status.

12.4.3 b **You shall** evaluate whether an organisation seeking certification for its **first-party** or **second-party white label** service has processes, procedures and arrangements in place to monitor the ongoing **certified** status of any **underpinning service**.

12.4.3 c For organisations seeking certification for **second-party white label** services, **you shall** follow the below rules:

12.4.3.c (i) Any organisation seeking to provide a **certified** service that is a **white label** service **shall** apply to you as if it were any other service seeking certification

12.4.3.c (ii) If the service being **white-labelled** is for an identity service provider role then Section 5 plus Part 3 of the UK digital verification services trust framework 1.0 are applicable as appropriate to the service being offered

12.4.3.c (iii) If the service being **white-labelled** is for an attribute service provider role then Section 6 plus Part 3 of the UK digital verification services trust framework 1.0 are applicable as appropriate to the service being offered

12.4.3.c (iv) If the service being **white-labelled** is for a holder service provider role then Section 7 plus Part 3 of the UK digital verification services trust framework 1.0 are applicable as appropriate to the service being offered

12.4.3.c (v) The **white label** service provider **shall** tell **you** if they assert that any of the requirements are not appropriate, and **shall** provide **you** with their reasoning. **You shall** decide whether the reason(s) are valid and evaluate accordingly.

12.4.3.c (vi) Provided the evaluation concludes that the new service complies with all appropriate requirements, **you shall** follow the normal certification process.

12.5 **Surveillance of white label services**

12.5.1 **You shall** monitor the **certified** status of **underpinning services**, to ensure that **white label** services remain legitimately certified under **the scheme**.

12.5.2 In addition to the ordinary surveillance requirements and timetable, **you shall** confirm that an **underpinning** certificate supporting the **white label service** remains in place on or around the anniversary date for the certificate applicable to the **white label** service each year. **You may** schedule this surveillance activity plus or minus 15 days of the anniversary date.

*Example: Service A is certified as an **underpinning service** offered to the market and operated by Company A. Service A was certified on 1st January 2025. Its surveillance is due on 1st January each year.*

*Company A applies for certification for Service B as a **first-party white label** service, having contracted with Company B to use its brand. Service B is certified by its CAB on 1st June 2025.*

*Service B **shall** have an ordinary surveillance audit on or around 1st June each year. It **shall** also have a surveillance audit to confirm the ongoing validity of **underpinning service**'s certification on or around 1st January each year.*

12.6 **Impact of loss of certification of an underpinning service**

12.6.1 If an **underpinning service** supporting one or more **white label** services is no longer **certified**, for any reason:

12.6.1 a **You shall** treat this as a major non-conformity for all relevant **white label** services

12.6.1 b **You shall** suspend or withdraw certificates for any **white label** service that relied upon the **underpinning service.**

12.6.2 **You shall** suspend a certificate for a **white label service** if the **underpinning service** loses its **certified** status. If the provider of the **underpinning service** resolves the non-conformity within 30 days and has its certified status reinstated, **you may** reinstate the **white label service**'s **certified** status and resume its existing certification cycle. If the provider of the **underpinning service** does resolve the non-conformity within more that 30 days, the **white label** organisation **shall** apply to **you** again for certification.

12.6.3 Otherwise, **you shall** follow the usual non-conformity procedure. You shall determine whether surveillance activity is required once the service provider has addressed the non-conformity.

*Example: Service X is operated by Company X and is certified as an **underpinning service**. Company Y has engaged in **second-party white labelling** and applied its brand to Service X, creating new Service Y. Company Y obtains certification for Service Y.*

Service X loses its certification on 1 January due to a major non-conformity found during a recertification evaluation.

As a result of Service X losing its certification, you suspend Company Y's certificate for Service Y. You decide to suspend Service Y's certificate for 30 days.

We remove both Service X and Service Y from the register, because neither holds a valid certificate for the purpose of registration.

You restore Company X's certification on 15 January, following a correction of its major non-conformity.

You restore Company Y's certificate for Service Y on 16 January.

Both service providers are able to reapply to us to have their services listed on the register.

12.7 **Certificate production and certification feedback report**

12.7.1 **Rules for service provider operating an underpinning service**

12.7.1 a When certifying an **underpinning service**, **you shall**:

12.7.1.a (i) record that the service is allowed to be used for the purpose of **white labelling** on the certificate of the **underpinning service**

12.7.1.a (ii) record this in the certification feedback report for the **underpinning service**

12.7.1 b **You shall** follow the method of recording this information as defined in:

12.7.1.b (i) Certificate requirements

12.7.1.b (ii) Certification feedback report

12.7.2 **Rules for white label services**

12.7.2 a When certifying a **white label service**, irrespective of whether that service is a **first-party** or **second-party white-label** service, **you shall**:

12.7.2 b record on the certificate:

12.7.2.b (i) the legal name of the **first-party** service provider that provides the **certified underpinning service**

12.7.2.b (ii) the name of the **underpinning service** provided by the **first-party** service provider

12.7.2.b (iii) the expiry date of the **underpinning** certificate associated with the **first-party certified** service

12.7.2 c record in the certification feedback report:

12.7.2.c (i) the legal name of the **first-party** service provider that provides the **certified underpinning service**

12.7.2.c (ii) the name of the **underpinning service** provided by the **first-party** service provider

12.7.2.c (iii) the name of the CAB that certified the **underpinning service**

12.7.2.c (iv) the expiry date of the **underpinning** certificate associated with the **underpinning service**

12.7.2 d When there is a change in the information recorded on the **underpinning** certificate, in line with Section 10.6.2., **you shall**

reflect this information in an updated certificate and certification feedback report for the **white label** service following each surveillance activity or recertification.

13 Co-branding

13.1 **Co-branding** exists where a **certified** service is **co-branded** by another organisation so that the user is still aware of the **underpinning service**. It is not considered **white labelling** where an **underpinning service** is not visible to the user.

13.2 In order to conform to the requirements of **the trust framework**, **you shall** evaluate service providers that operate **underpinning service** for the purposes of **co-branding** to ensure that:

13.2.1 the service provider is not misrepresenting the **certified**, **registered** or **trust marked** status of any service it operates as a **first-party** service that is co-branded with another service

13.2.2 the service provider has effective processes and procedures in place to ensure that a **second-party** does not misrepresent the **certified**, **registered** or **trust marked** status of their co-branded service(s)

13.3 The service provider **can** demonstrate conformity through documentation including policies and contracts with **second-parties**. The service provider **can** demonstrate conformity by showing evidence of where it has directly acted to prevent misrepresentation of **certified**, **registered** or **trust marked** status by **second-party** it is contracted with.

14 Annex A – methods for evaluation time calculations

14.1 General

14.1.1 This annex provides further guidance on developing a formula to calculate evaluation time. Section 13.2 classification of factors for calculating evaluation time gives an example of a classification of factors that can be used as the basis for calculating evaluation time and section 13.3 calculation of evaluation time how this feeds into the calculation of evaluation time.

14.2 Classification of factors for calculating evaluation time

14.2.1 These tables gives the impact on evaluation effort for the main factors related to the calculation of evaluation time, as listed in section 10.4.12 evaluation time 10.4.12a (i) to (ix)

a) Size of the operation and impact of effort (as detailed in section 10.4.12a (i))

	Reduced effort	Normal effort	Increased effort
Number of information systems	Single information system	2 or 3 information system	4 or more information systems
Number of employees	Fewer than 10 employees	11 to 50 employees	More than 50 employees
Number of activities	Only UKDVSTF service (no supplementary schemes)	UKDVSTF service plus 1 supplementary scheme	UKDVSTF service plus more than 1 supplementary scheme

b) Complexity of the service and impact of effort (as detailed in section 10.4.12a (ii))

	Reduced effort	Normal effort	Increased effort
Number of trust framework roles	Single role	2 roles	3 or more roles

GPG 45 level of confidence	Low level of confidence only	Medium level of confidence only	High or very high level of confidence
White labelling/co-branding	White label	Not applicable	Underpinning or co-branding
Component service provision (CPS)	Not applicable	1-5 clients relying on CSP	Above 5 clients relying on CSP

c) Diversity of technology and impact of effort (as detailed in section 10.4.12a (iii))

	Reduced effort	Normal effort	Increased effort
Verification of evidence	Face to face verification	Remote verification	Face to face and remote verification
GPG 44	Low quality authenticator	Medium quality authenticator	High quality authenticator
GPG44	Low level of protection	Medium level of protection	High or very high level of protection

d) Number of sites and impact of effort (as detailed in section 10.4.12a (iv))

	Reduced effort	Normal effort	Increased effort
Face to face service delivery	None or single site	2 to 20 sites	More than 20 sites
Sites hosting IT systems	single site	2 or 3 sites	More than 3 sites
Administrative functions only	single site	2 to 5 sites	More than 5 sites

e) Previous UKDVSTF certification performance and impact of effort (as detailed in section 10.4.12a (v))

	Reduced effort	Normal effort	Increased effort

Previous UKDVSTF certification performance	Recently certified	Recent surveillance evaluation	No certification

f) Extent of outsourcing and impact of effort (as detailed in section 10.4.12a (vi))

	Reduced effort	Normal effort	Increased effort
Degree of outsourcing	No outsourcing	Outsourced administrative function(s)	Outsourced service function(s)
Third-party arrangements	No third-party arrangements	Third-party admin staff	Third-party staff providing service functions

g) Number of profiles and impact of effort (as detailed in section 10.4.12 (viii))

	Reduced effort	Normal effort	Increased effort
Number of profiles	0 to 5	6 to 10	More than 10

h) Risk and impact of effort (as detailed in section 10.4.12a (ix))

	Reduced effort	Normal effort	Increased effort
Risk	Low	Medium	High

14.3 **Calculation of evaluation time**

14.3.1 **You shall** use this classification to derive an impact factor based upon identifying the number of factors that imply reduced effort, the number that imply normal effort and the number that imply increased effort. Whichever of these numbers is the largest determines the overall impact factor. Where equal number of factors occur in two columns the higher effort column **shall** apply.

14.3.2 Starting with the number of days given in the ISMS audit time column of table c.1 in ISO/IEC 27006-1:2024 then, if the above calculation implies a reduction in effort, reduce the relevant entry by 25% but, if the above

calculation implies an increase in effort, then increase the relevant entry by 50%.

15 Annex B – Sampling method for the underpinning service documentation

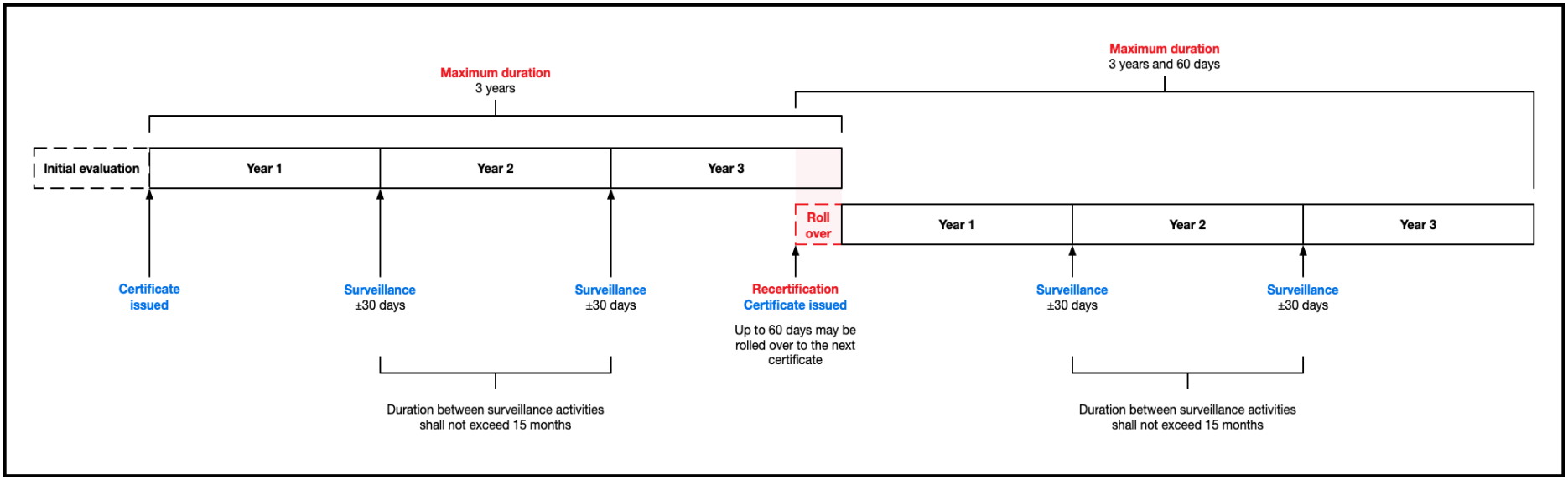
15.1 Where contracts are relied upon as evidence of conformity, the **auditor shall** review a random sample of no less than 10% of contracts that are in place or 5, whichever is greater. Where fewer than 5 contracts are in place, all contracts **shall** be reviewed. The sample **shall** include the most recent contract put in place and the oldest, longest-running contract that is in place.

15.2 In addition to reviewing the **first-party** service provider's processes and procedures, the **auditor shall** also assess a sample of the marketing materials published by **second-parties** relying upon the **underpinning service**. The **auditor shall** review a random sample of websites, brochures or other marketing materials for no less than 10% of contracted **second-party** organisations. The organisations, services and information sampled **shall** be recorded in the certification feedback report.

15.3 If the **auditor** finds evidence that any **second-party** is misrepresenting the **certified, registered** or **trust marked** status of any of its **white label** services, this **shall** be treated as a minor non-conformity for the **first-party** service provider, and you should give them time to rectify it. If the **first-party** service provider fails to resolve the issue within the allotted timeframe, the **auditor shall** treat this as a major non-conformity. In addition, if you have also certified the sampled **second-party white label** service, it **shall** treat this as a minor non-conformity for the **second-party** service. If it did not certify the **second-party white label** service, it **shall** inform us, such that we can raise it with the appropriate CAB.

16 Annex C – certification cycle

16.1 The below diagram describes certification cycle from first certification to recertification and the maximum duration of the certification cycle for both permitted under **the scheme.**



17 Annex D – letter of approval template

[CAB Name]

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<Contact Email Address>

XX Month 202X

Our ref: XXXX

Dear <<Contact Name>>,

Appointment of [CAB Name] as approved conformity assessment body under the UK digital verification service trust framework certification scheme.

The Department for Science Innovation and Technology, scheme owner of the UK digital verification service trust framework (UKDVSTF) certification scheme, approves [CAB Name] to act as conformity assessment body (CAB) under the scheme. The table below indicates the scope of approval for [CAB Name], against which they can apply for accreditation with the UK Accreditation Service (UKAS).

We require [CAB Name] to confirm its acceptance of approval and the terms and conditions of its **approved** status (contained in this letter) before commencing any conformity assessment activity in respect of this scheme. We will not publish the approval on GOV.UK until we receive this confirmation. [CAB name] should email its confirmation to digital.identity.register@dsit.gov.uk

Yours sincerely

[Authorised person]

[Scheme owner]

Department for Science, Innovation and Technology

Terms and conditions of appointment

[CAB Name] will be appointed in respect of the product, process, and/or service categories and conformity assessment procedures set out below and aligned with UKAS accreditation schedule:

Product	Standard
Attribute service provider	UK Digital Identity and attributes trust framework beta version (to be agreed with DSIT) UK DIATF CSR Certification Requirements for Conformity Assessment Bodies version xxxxx UKDIATF ASCR Assessor Skills and Competency Requirements version xxxxx
Component service provider New Role for UKDIATF 0.4 and subject to extra uplift assessment by UKAS should the pilot CABs wish to deliver	UK Digital Identity and attributes trust framework beta version (to be agreed with DSIT) UK DIATF CSR Certification Requirements for Conformity Assessment Bodies version xxxxx UKDIATF ASCR Assessor Skills and Competency Requirements version xxxxx
Holder service provider New Role for UKDIATF 0.4 and subject to extra uplift assessment by UKAS should the pilot CABs wish to deliver Including the sub categories of: (delete as appropriate) Disclosure and Disbarring Service Right to Rent Right to Work	UK Digital Identity and attributes trust framework beta version (to be agreed with DSIT) UK DIATF CSR Certification Requirements for Conformity Assessment Bodies version xxxxx UKDIATF ASCR Assessor Skills and Competency Requirements version xxxxx Supplementary Code – Disclosure and Barring Service – version xxxxx Supplementary Code – Right to Rent – version xxxxx Supplementary Code – Right to Work – version xxxxxx

1. We will make the approval of [CAB Name] public on GOV.UK.

2. The approval will remain in force until we withdraw it under paragraph 4 or after the lapse of a period of 180 days after the [CAB Name] has notified us in writing that it wishes to withdraw from the UK Digital verification services trust framework certification scheme (the scheme) and for the approval to be terminated under paragraph 5.

3. This approval is subject to the following conditions:

a. [CAB Name] must at all times carry out the duties and functions of CAB under the UK digital verification services trust framework certification scheme to our satisfaction, where those duties and functions are not ones which are, or are able to be, assessed by UKAS as part of the accreditation process

b. [CAB Name] must always hold the necessary accreditation for the functions and products, processes, and/or services for which it has approval or otherwise be able to demonstrate its suitability for approval

c. We continue to be satisfied as to [CAB Name]'s suitability, including its status and competence, to be a CAB in connection with this scheme. At all times, [CAB Name] must, at our reasonable request, submit itself for immediate reassessment of its suitability for approval

d. [CAB Name] must submit itself to annual surveillance for the purpose of making sure that they are performing their duties and functions in accordance with the approval and accreditation; provided always that we may require more frequent surveillance

e. [CAB Name] must submit itself every 4 years for a full reassessment and/or re-accreditation, for us to be satisfied that they remain suitable for approval

f. For the purposes of reassessment, reaccreditation or maintenance of accreditation and surveillance, [CAB Name] acknowledges and accepts that UKAS will carry out an assessment and will submit a report to us

g. [CAB Name] must comply with the relevant obligations as stated in the scheme and in addition:

    i. [CAB Name] must have documented procedures covering all aspects of its work relating to the conformity assessment procedures which it carries out, adequate internal organisation and adequate procedures in place to give confidence in the quality of its services

h. Where [CAB Name] receives a request for information relating to a conformity assessment activity from a market surveillance or enforcement authority they shall inform us of such request

i. [CAB Name] must have a process in place for achieving consistency in cases where it needs to (implicitly or explicitly) exercise judgement or interpret a standard or requirement in a decision to grant or withhold certification

j. [CAB Name] must authorise, at any reasonable time, access by us, or on our behalf to:

    i. all documentation arising out of its duties and functions under this approval. [CAB Name] shall comply with any reasonable request made by or on behalf of us, for information regarding the exercise of those duties and functions, where compliance with those duties and functions is not, or is not able to be verified by UKAS;

    ii. its premises, for the purpose of verifying its compliance with the conditions and with the minimum criteria.

k. [CAB Name] must take part in CAB co-ordination activities that we may choose to establish. If, exceptionally, [CAB Name] is unable to send a representative or a suitable substitute to a co-ordination activity, it shall without delay explain the reasons for its non-attendance to us

l. [CAB Name] must maintain its impartiality and independence from all applicants for its services and in no circumstances should it take on the role of authorised representative for any applicant

m. [CAB Name] must inform us of any changes which have a bearing upon its status as a CAB or its ability to perform the duties and functions of a CAB under the scheme.

n. [CAB Name] must inform us of the following events as soon as they occur:

    i. [CAB Name] is unable to pay their debts as they fall due, or are deemed unable to pay their debts or becomes insolvent within the meaning of the Insolvency Act 1986 section 123 or any other enactment.

    ii. A winding up or an administration order is made in relation to the [CAB Name], or [CAB Name] petitions or apply to the court for such an order, passes a resolution to present such a petition or

application, or convenes a meeting for the purpose of considering such a resolution.

iii. Any steps are taken with a view to proposing any kind of composition, scheme of arrangement, compromise or arrangement involving [CAB Name] and its creditors generally, or any class of them

iv. Any administrative receiver, receiver, manager or other person with functions like those of an administrative receiver, receiver or manager is appointed to [CAB Name] or any significant part of its assets, or [CAB Name] requests the appointment of such a person.

v. The directors of [CAB Name] take any steps to obtain a moratorium for the company within the meaning of the Insolvency Act 1986.

vi. [CAB Name] becomes a subsidiary of any company of which it is not a subsidiary at the date of this letter or ceases to be a subsidiary of any company of which it is a subsidiary at the date of this letter. The word 'subsidiary' shall be interpreted in accordance with the definitions in Section 1159 of the Companies Act 2006.

o. Documentation to be retained:

i. We require [CAB Name] to maintain an up to date record of all certifications it has issued, whom it has been issued to and to what it applies to. You shall retain these records and make them available to us, (or such other person as may be authorised by us, subject to the usual provisions relating to confidentiality) on request. You must annex a list of the relevant technical documentation to the certificate and keep a copy. We require that [CAB Name] keep available on request a complete electronic copy of all the information detailed above. You shall supply this to us on the event of you ceasing to be CAB, or at other time as we direct.

4. We may, by notice in writing, add conditions or vary or delete any conditions, to this approval. Such additions, variations or deletions shall have effect 30 days after the date of that notice unless we agree a different period with you in writing.

5. We will withdraw or suspend this approval immediately if there is evidence that [CAB Name] no longer meets the requirements relating to CABs, as specified under the scheme and/or the terms of this letter.

6. In the case of suspension, the approval of [CAB Name] as CAB may be reinstated subject to [CAB Name] satisfying us that steps have been taken to address the non-conformity with the requirements relating to CABs (as specified under the scheme and/or the terms of this letter).

7. We will terminate this approval in accordance with the scheme requirements at the request of [CAB Name] upon the expiry of 180 days' notice in writing to us.

8. This approval is subject to the following additional conditions in the event of it being withdrawn or terminated under paragraphs 5, 6 or 7:

    a. [CAB Name] must prepare a report, in writing, on the exercise of its duties and functions under the scheme. You must:
        i. submit this to us within three calendar months of the date on which the termination of the approval takes effect or, if appropriate, of the date of withdrawal
        ii. provide in the report, such information as may have been agreed in writing between us and [CAB Name]

    b. [CAB Name] must follow the transfer process for its clients that have been certified under the scheme as defined in the scheme's documentation.

9. If the above terms and conditions of approval are acceptable, the [CAB Name] should signify its consent by email to digital.identity.register@dsit.gov. We will confirm our approval once we have received [CAB Name]'s consent.

10. Once we receive your acceptance email we shall add you onto the list of approved CABs on GOV.UK