Achieving 'qualified status' and ceasing to provide qualified trust services under the eIDAS Regulation

Information for trust service providers

ico.
Information Commissioner's Office

Achieving 'qualified status' and ceasing to provide qualified trust services under the eIDAS Regulation – information for trust service providers

This document is intended to provide practical information about how trust service providers can become qualified trust service providers under chapter three of Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market (the eIDAS Regulation).

It also provides information about how qualified trust service providers should renew their qualified status, what to do if they make changes to their qualified trust service and how they should proceed when they cease to provide a qualified trust service.

Obtaining qualified status

The process in brief:

- A conformity assessment must be carried out by a Conformity Assessment Body;
- the conformity assessment will result in a conformity assessment report which must be submitted to the ICO;
- the ICO will analyse the report to verify that all relevant requirements have been met;
- if the ICO is unable to verify compliance with the requirements of the regulation then you will have an opportunity to take corrective action and resubmit your application;
- once the ICO has verified your compliance you will be added to the UK's Trusted Service List; and
- you may use an EU trust mark to demonstrate you have achieved qualified status to stakeholders.

The process in more detail:

Conformity assessment body accreditation

It is your decision as to which conformity assessment body you choose to work with. However, in order to carry out conformity assessments

conformity assessment bodies must be suitably accredited by the UK's National Accreditation Body, UKAS. They should contact UKAS directly to arrange accreditation prior to conducting a conformity assessment.

The conformity assessment

The exact conformity assessment process will be determined by the conformity assessment body you have chosen to work with. However, you should expect an audit-like approach and therefore the conformity assessment body may want to interview staff, observe practices and review processes and policies.

The conformity assessment should assess whether your organisation and the trust services you provide comply with the requirements for qualified trust service providers and qualified trust services set down in the eIDAS Regulation.

A number of requirements apply to all qualified trust services and qualified trust service providers, but there are also some which apply to specific types of qualified trust services. A table of the requirements is provided as appendix 1 to this guidance.

The conformity assessment report

The findings of the conformity assessment should be set out within a conformity assessment report.

As a minimum, conformity assessment reports must contain the following details:

- Name and address of the Trust Service Provider;
- name and address of the conformity assessment body;
- the dates during which the conformity assessment took place;
- a statement confirming that the conformity assessment body has carried out a conformity assessment of the trust service provider and that the trust service provider complies with the requirements laid down in the eIDAS Regulation, in particular the requirements for qualified trust service providers and for the qualified trust services they provide;
- the name of the trust service;
- a short description of the trust service including how it works and its purpose;
- a list of the requirements complied with and a statement explaining how each requirement has been met by the trust service provider

and by what means this was ascertained by the auditor e.g. interview, observation, testing; and

- the date of when the next conformity assessment is due.

The report must be signed by someone within your organisation with appropriate seniority who will be accountable for the conformity assessment.

For guidance, we have produced a template report which is at appendix 2. It may be used as a guide, although conformity assessment bodies may prefer to use their own conformity assessment report structure.

The ICO's verification process

The ICO must analyse the conformity assessment report to ensure that all relevant requirements have been satisfied and that this has been evidenced appropriately within the report.

Once you have received the conformity assessment report you must submit it to the ICO along with a completed notification form within three working days.

It will be assigned to a lead auditor within our assurance team who will carry out a review of the report and verify that each requirement has been met satisfactorily. In addition to this, the lead auditor will review a limited amount of evidence. As a minimum this will consist of:

- Your information security breach management policy;
- your information security policy; and
- your termination plan in relation to the trust service subject to the conformity assessment.

The lead auditor will also request **at least two more pieces of evidence,** which they will select after an initial reading of the conformity assessment report. The additional evidence requested by the lead auditor may be either documentary evidence or a short phone interview with a relevant contact from your organisation. These should be provided within five working days of the request.

In addition the lead auditor may contact you for further information or clarification around any of the points raised in the report.

The ICO aims to complete the verification process within three months of receipt and will contact you if we think there will be a delay.

Granting qualified status

If the ICO verifies that the requirements of the Regulation have been met in regard to the provision of a qualified trust service then we will email you to indicate this and provide you with a formal letter to this effect. We will also request that you be added to the UK's Trusted Service List. Once you receive confirmation that you have been added the trusted list your qualified status will take effect. After this point you may display a European trust mark to demonstrate that you have achieved qualified status.

Please note there are rules around the trust mark's use, for example where it is displayed a link to the UK's trusted list must also be displayed. These rules are set out in legislation. A user guide to the trust mark and a link to the relevant legislation can be found on the European Commission's website.

Refusing qualified status

If we are unable to verify that the requirements of the Regulation have been met we will contact you to explain how we have reached our decision setting out which requirements have not been met and why.

You will be allowed an opportunity to remedy the situation. Within one month of receiving our decision, you should take corrective action and resubmit your report with an appendix setting out the action you have taken. The corrective action should be re-assessed and signed off by the conformity assessment body.

Renewing qualified status

To retain the qualified status of a trust service you must undergo a conformity assessment and verification process every 24 months.

Changes to qualified trust services

If any significant changes to the provision of qualified trust services are made, you should notify the ICO, who will make a decision as to whether qualified status should be retained or if a new conformity assessment and verification process should be undertaken.

Ceasing to provide a qualified trust service.

In brief

When you decide that you want to stop providing a qualified trust service you must:

- Implement your termination plan;
- notify the ICO; and
- provide a summary to the ICO of how you have implemented the termination plan.

In more detail

When you decide to stop providing your qualified trust service, you must implement your termination plan and then notify the ICO. Your notification must detail the type of information you intend to keep in relation to the data you have issued and received in the course of providing a qualified trust service and how long you intend to keep the information for. You should keep this information for an appropriate period of time in case you are required to provide evidence in legal proceedings and for continuity of service.

Your notification will be assigned to a lead auditor within the ICO's assurance team who will verify whether you have implemented the termination plan appropriately, inform you of their decision and highlight any remaining concerns or risks.

You must then take action within one month to address these concern and risks. If the ICO's concerns are not addressed, enforcement action may be considered.

Interim measures carried forward from Directive 1999/93/EC

If a trust service which you provide was granted qualified status under Directive 1999/93/EC, you will need to undergo a conformity assessment and submit a conformity assessment report for verification to the ICO before 01 July 2017. Your organisations qualified status will remain until the process has been completed.

Appendix 1

eIDAS requirements for qualified trust service providers

General requirements for all QTSPs

eIDAS reference	Requirement
Art.15	Where feasible, trust services provided and end-user products used in the provision of those services shall be made accessible for persons with disabilities.
Art.19.1	Qualified and non-qualified trust service providers shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide. Having regard to the latest technological developments, those measures shall ensure that the level of security is commensurate to the degree of risk. In particular, measures shall be taken to prevent and minimise the impact of security incidents and inform stakeholders of the adverse effects of any such incidents
Art.19.2	Qualified and non-qualified trust service providers shall notify the supervisory body, and where applicable other relevant bodies without undue delay and within 24 hours of becoming aware of any data breach, security breach or a loss of integrity that has had a significant impact on the trust service provided, Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the trust service provider shall also notify the natural or legal person of the breach or loss of integrity without undue delay. Where appropriate, in particular if a breach of security or loss of integrity concerns two or more EU member states, the notified supervisory body shall inform the supervisory bodies in the member states concerned and ENISA. The notified supervisory body shall inform the public or require the trust service provider to do so, where it determines that disclosure of the breach of security or loss of integrity is in the public interest
Art.20.1	Qualified trust service providers shall be audited at their own expense at least every 24 months by a conformity assessment body. The purpose of the audit shall be to

	confirm that the qualified trust service providers and the qualified trust services provided by them fulfil the requirements laid down in the Regulation. The qualified trust service providers shall submit the resulting conformity assessment report to the supervisory body within the period of three working days after receiving it.
Art 23.2	When using the EU trust mark for the qualified trust services referred to in paragraph one, qualified trust service providers shall ensure that a link to the relevant trusted list is made available on their website.
Art.24.1	When issuing a qualified certificate for a trust service, a qualified trust service provider shall verify, by appropriate means and in accordance with national law, the identity and, if applicable any specific attributes of the natural or legal person to whom the qualified certificate is issued. The information referred to in the first subparagraph shall be verified by the qualified trust service provider either directly or by relying on a third party in accordance with national law.
Art.24.1.a	by the physical presence of the natural person or of an authorised representative of the legal person;
Art.24.1.b	remotely, using electronic identification means, for which prior to the issuance of the qualified certificate, a physical presence of the natural person or of an authorised representative of the legal person was ensured and which meets the requirements set out in Article 8 with regard to the assurance levels 'substantial' or 'high';
Art.24.1.c	by means of a certificate of a qualified electronic signature or of a qualified electronic seal issued in compliance with point (a) or (b); or
Art.24.1.d	by using other identification methods recognised at national level which provide equivalent assurance in terms of reliability to physical presence. The equivalent assurance shall be confirmed by a conformity assessment body.
Art.24.2	A qualified trust service provider providing qualified trust services shall:
Art.24.2.a	inform the supervisory body of any change in the provision of its qualified trust services and an intention to cease those activities;
Art.24.2.b	employ staff and, if applicable subcontractors who possess the necessary expertise, reliability, experience,

	and qualifications and who have received appropriate training regarding security and personal data protection rules and shall apply administrative and management procedures which correspond to European or international standards;
Art.24.2.c	with regard to the risk of liability for damages in accordance with Article 13, maintain sufficient financial resources, obtain appropriate liability insurance or both in accordance with national law;
Art.24.2.d	before entering into a contractual relationship, inform in a clear and comprehensive manner, any person seeking to use a qualified trust service of the precise terms and conditions regarding the use of that service, including any limitations on its use;
Art.24.2.e	use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them;
Art.24.2.f	use trustworthy systems to store data provided to it, in a verifiable form so that: (i)they are publicly available for retrieval only where the consent of the person to whom the data relates has been obtained, (ii)only authorised persons can make entries and changes to the stored data, and (iii) the data can be checked for authenticity.
Art.24.2.g	Take appropriate measures against forgery and theft of data;
Art.24.2.h	record and keep accessible for an appropriate period of time, including after the activities of the qualified trust service provider have ceased, all relevant information concerning data issued and received by the qualified trust service provider, in particular for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service. Such recording may be done electronically;
Art.24.2.i	have an up-to-date termination plan to ensure continuity of service in accordance with provisions verified by the supervisory body under point (i) of Article 17(4);
Art.17.4	The relevant part of Article 17 (4) says: the tasks of the supervisory body shall include in particular to verify the existence and correct application of provisions on termination plans in cases where the

	qualified trust service provider ceases its activities, including how information is kept accessible in accordance with point (h) of Article 24(2);
Art.24.2.j	ensure lawful processing of personal data in accordance with Directive 95/46/EC; and
Art.24.2.k	in case of qualified trust service providers issuing qualified certificates, establish and keep updated a certificate database.
Art.24.3	If a qualified trust service provider issuing qualified certificates decides to revoke a certificate, it shall register such revocation in its certificate database and publish the revocation status of the certificate in a timely manner, and in any event within 24 hours after the receipt of the request. The revocation shall become effective immediately upon its publication
Art.24.4	With regard to paragraph three, qualified trust service providers issuing qualified certificates shall provide to any relying party information on the validity or revocation status of qualified certificates issued by them. This information shall be made available at least on a per certificate basis at any time and beyond the validity period of the certificate in an automated manner that is reliable, free of charge and efficient

Requirements for specific types of QTSPs

e-Signatures

Requirements for qualified certificates issued for electronic signatures.

eIDAS reference	**Requirement**
Art.28.1	Qualified certificates for electronic signatures shall meet the requirements laid down in Annex I
Art.28.1 – Annex I	Qualified certificates for electronic signatures shall contain:
Art.28.1 – Annex I.a	an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for electronic signature;
Art.28.1 – Annex I.b	a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least, the Member State in which that provider is established and: • for a legal person - the name and, where applicable, registration number as stated in

	the official records • for a natural person - the person's name;
Art.28.1 – Annex I.c	at least the name of the signatory, or a pseudonym. If a pseudonym is used, it shall be clearly indicated;
Art.28.1 – Annex I.d	electronic signature validation data that corresponds to the electronic signature creation data;
Art.28.1 – Annex I.e	details of the beginning and end of the certificate's period of validity;
Art.28.1 – Annex I.f	the certificate identity code, which must be unique for the qualified trust service provider
Art.28.1 – Annex I.g	the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;
Art.28.1 – Annex I.h	the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (g) is available free of charge;
Art.28.1 – Annex I.i	the location of the services that can be used to enquire about the validity status of the qualified certificate; and
Art.28.1 – Annex I.j	where the electronic signature creation data related to the electronic signature validation data is located in a qualified electronic signature creation device, an appropriate indication of this, at least in a form suitable for automated processing.
Art.28.3	Qualified certificates for electronic signatures may include non-mandatory additional specific attributes. Those attributes shall not affect the interoperability and recognition of qualified electronic signatures.
Art.28.4	If a qualified certificate for electronic signatures has been revoked after initial activation, it shall lose its validity from the moment of its revocation, and its status shall not in any circumstances be reverted.

Requirements for qualified electronic signature creation devices

eIDAS reference	Requirement
Art 29	Qualified electronic signature creation devices shall meet the requirements laid down in Annex II.
Annex II	Qualified electronic signature creation devices shall ensure, by appropriate technical and procedural means, that at least:
Annex II.1.a	the confidentiality of the electronic signature creation data used for electronic signature creation is reasonably assured;
Annex II.1.b	the electronic signature creation data used for electronic signature creation can practically occur only once;
Annex II.1.c	the electronic signature creation data used for electronic signature creation cannot, with reasonable assurance, be derived and the electronic signature is reliably protected against forgery using currently available technology;
Annex II.1.d	the electronic signature creation data used for electronic signature creation can be reliably protected by the legitimate signatory against use by others;
Annex II.2	Qualified electronic signature creation devices shall not alter the data to be signed or prevent such data from being presented to the signatory prior to signing.
Annex II.3	Generating or managing electronic signature creation data on behalf of the signatory may only be done by a qualified trust service provider.
Annex II.4	Without prejudice to point (d) of point 1, qualified trust service providers managing electronic signature creation data on behalf of the signatory may duplicate the electronic signature creation data only for back-up purposes provided the following requirements are met:
Annex II.4.a	the security of the duplicated datasets must be at the same level as for the original datasets; and
Annex II.4.b	the number of duplicated datasets shall not exceed the minimum needed to ensure continuity of the service.

Requirements for the validation of qualified electronic signatures

eIDAS reference	Requirement
Art 32.1	The process for the validation of a qualified electronic signature shall confirm the validity of a qualified electronic signature provided that;
Art 32.1. a	the certificate that supports the signature was, at the time of signing, a qualified certificate for electronic signature complying with Annex I;
Art 32.1.b	the qualified certificate was issued by a qualified trust service provider and was valid at the time of signing;
Art 32.1.c	the signature validation data corresponds to the data provided to the relying party;
Art 32.1.d	the unique set of data representing the signatory in the certificate is correctly provided to the relying party;
Art 32.1.e	the use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing;
Art 32.1.f	the electronic signature was created by a qualified electronic signature creation device;
Art 32.1.g	the integrity of the signed data has not been compromised; and
Art 32.1.h	the requirements provided for in Article 26 were met at the time of signing.
2.	The system used for validating the qualified electronic signature shall provide to the relying party the correct result of the validation process and shall allow the relying party to detect any security relevant issues.

Qualified validation service for qualified electronic signatures

eIDAS reference	Requirement
Art.33.1	A qualified validation service for qualified electronic signatures may only be provided by a qualified trust service provider who:
Art.33.1.a	provides validation in compliance with Article 32(1); and
Art.33.1.b	allows relying parties to receive the result of the validation process in an automated manner, which is reliable, efficient and bears the advanced electronic signature or advanced electronic seal of the provider of the qualified validation service.

Requirements for qualified preservation service for qualified electronic signatures

eIDAS reference	Requirement
Art.34.1	A qualified preservation service for qualified electronic signatures may only be provided by a qualified trust service provider that uses procedures and technologies capable of extending the trustworthiness of the qualified electronic signature beyond the technological validity period.

e-seals

Qualified certificates for electronic seals

eIDAS reference	Requirement
Art 38.1	Qualified certificates for electronic seals shall meet the requirements laid down in Annex III
Art 38.1 Annex III	Qualified certificates for electronic seals shall contain:
Art 38.1 Annex III.a	an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for electronic seal;
Art 38.1 Annex III.b	a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least the Member State in which that provider is established and • for a legal person - the name and, where applicable, registration number as stated in the official records;

	• for a natural person - the person's name;
Art 38.1 Annex III.c	at least the name of the creator of the seal and, where applicable, registration number as stated in the official records;
Art 38.1 Annex III.d	electronic seal validation data, which corresponds to the electronic seal creation data;
Art 38.1 Annex III.e	details of the beginning and end of the certificate's period of validity;
Art 38.1 Annex III.f	the certificate identity code, which must be unique for the qualified trust service provider;
Art 38.1 Annex III.g	the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;
Art 38.1 Annex III.h	the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (g) is available free of charge;
Art 38.1 Annex III.i	the location of the services that can be used to enquire as to the validity status of the qualified certificate; and
Art 38.1 Annex III.j	where the electronic seal creation data related to the electronic seal validation data is located in a qualified electronic seal creation device, an appropriate indication of this, at least in a form suitable for automated processing.
Art 38.2	Qualified certificates for electronic seals shall not be subject to any mandatory requirements exceeding the requirements laid down in Annex III.
Art 38.3	Qualified certificates for electronic seals may include non-mandatory additional specific attributes. Those attributes shall not affect the interoperability and recognition of qualified electronic seals.
Art 38.4	If a qualified certificate for an electronic seal has been revoked after initial activation, it shall lose its validity from the moment of its revocation, and its status shall not in any circumstances be reverted.

Requirements for qualified electronic seal devices

eIDAS reference	**Requirement**
Art 39.1	Article 29 shall apply mutatis mutandis to requirements for qualified electronic seal creation devices.

Requirements for validation and preservation of qualified electronic seals

eIDAS reference	Requirement
Art 40	Articles 32, 33 and 34 shall apply mutatis mutandis to the validation and preservation of qualified electronic seals.

Time stamps

Requirements for qualified electronic time stamps

eIDAS reference	Requirement
Art 42.1	1. A qualified electronic time stamp shall meet the following requirements:
Art 42.a	a) it binds the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably
Art 42.b	b) it is based on an accurate time source linked to Coordinated Universal Time; and
Art 42.c	c) it is signed using an advanced electronic signature or sealed with an advanced electronic seal of the qualified trust service provider, or by some equivalent method.

e-delivery services

Requirements for qualified electronic registered delivery services

eIDAS reference	Requirement
Art.44.1	Qualified electronic registered delivery services shall meet the following requirements:
Art.44.1.a	they are provided by one or more qualified trust service provider(s);
Art.44.1.b	they ensure with a high level of confidence the identification of the sender;
Art.44.1.c	they ensure the identification of the addressee before the delivery of the data;
Art.44.1.d	the sending and receiving of data is secured by an advanced electronic signature or an advanced electronic seal of a qualified trust service provider in such a manner as to preclude the possibility of the data being changed undetectably;
Art.44.1.e	any change of the data needed for the purpose of sending or receiving the data is clearly indicated to the sender and addressee of the data; and
Art.44.1.f	the date and time of sending, receiving and any

	change of data are indicated by a qualified electronic time stamp.
Art.44.1	In the event of the data being transferred between two or more qualified trust service providers, the requirements in points (a) to (f) shall apply to all the qualified trust service providers.

Website authentication certificates
Requirements for qualified certificates for website authentication

eIDAS reference	**Requirement**
Art 45. 1	Qualified certificates for website authentication shall meet the requirements laid down in Annex IV.
Art. 45 annexe IV	Qualified certificates for website authentication shall contain:
Art. 45 annexe IV.a	an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for website authentication;
Art. 45 annexe IV.b	a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least the Member State in which that provider is established and • for a legal person - the name and, where applicable, registration number as stated in the official records, • for a natural person - the person's name;
Art. 45 annexe IV.c	For natural persons: at least the name of the person to whom the certificate has been issued, or a pseudonym. If a pseudonym is used, it shall be clearly indicated; for legal persons: at least the name of the legal person to whom the certificate is issued and, where applicable, registration number as stated in the official records;
Art. 45 annexe IV.d	elements of the address, including at least city and State, of the natural or legal person to whom the certificate is issued and, where applicable, as stated in the official records;
Art. 45 annexe IV.e	the domain name(s) operated by the natural or legal person to whom the certificate is issued;
Art. 45 annexe IV.f	details of the beginning and end of the certificate's period of validity;
Art. 45 annexe IV.g	the certificate identity code, which must be unique

	for the qualified trust service provider;
Art. 45 annexe IV.h	the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider; and
Art. 45 annexe IV.i	the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (h) is available free of charge;
Art. 45 annexe IV.j	the location of the certificate validity status services that can be used to enquire as to the validity status of the qualified certificate.

Appendix 2

eIDAS Conformity Assessment Report

For the purpose of certifying compliance with requirements of eIDAS and in particular with the requirements for qualified trust service providers and for the qualified trust services they provide.

Certification statement

We:

[Name of Conformity Assessment Body]

of:

[Address of Conformity Assessment Body]

certify that the trust service provider:

[Name of Trust Service Provider]

of:

[Address of Trust Service Provider]

complies with the requirements of eIDAS and in particular with the requirements for qualified trust service providers and for the qualified trust services they provide.

Declaration made by:

[Name and job title of appropriate member of staff at Conformity Assessment Body]

[Date]

1. Introduction

1.1 The eIDAS regulation sets out that Trust Service Providers may obtain 'qualified' status if they are able to demonstrate compliance with the requirements for Trust Service Providers laid down in the Regulation, and in particular, with the requirements for qualified trust service providers and the qualified trust services they provide.

1.2 In order to demonstrate compliance, a conformity assessment must be carried out by a conformity assessment body which must result in a conformity assessment report.

1.3 The conformity assessment report must be submitted to the Supervisory Body, the Information Commissioner's Office (ICO) for verification and 'qualified' status will be granted where appropriate.

1.4 This is the conformity assessment report for [name of Trust Service Provider] which sets out how compliance with the Regulation has been achieved and will be submitted by [name of Trust Service Provider] to the ICO for verification.

1.5 [Name of Conformity Assessment body] carried out a conformity assessment at the premises of [name of Trust Service Provider] between [dates of conformity assessment]

2. Scope of the audit

2.1 The conformity assessment was limited to the trust service described below.

2.2 Name of the trust service:

2.3 Type of trust service under eIDAS: (delete as appropriate)

Qualified certificate for electronic signature (Art. 28 of the eIDAS Regulation)
Qualified certificate for electronic seal (Art. 38 of the eIDAS Regulation)
Qualified certificate for website authentication (Art. 45 of the eIDAS Regulation)
Qualified validation service for qualified electronic signatures (Art. 33 of the eIDAS Regulation)
Qualified validation service for qualified electronic seals (Art. 40 of the eIDAS Regulation)
Qualified preservation service for qualified electronic signatures (Art. 34 of the eIDAS Regulation)
Qualified preservation service for qualified electronic seals (Art. 40 of the eIDAS Regulation)
Qualified electronic time stamps (Art. 42 of the eIDAS Regulation)
Qualified electronic registered delivery services (Art. 44 of the eIDAS Regulation

2.4 The service is provided for the following purpose/purposes:

2.5 It works in the following way:

3.0 Conformity Assessment Findings

Please note the information contained within the table is displayed by way of an example as to how the table should be completed and should not be taken as guidance in regard to the specific type of assurances that should be sought in relation to compliance with the eIDAS requirements.

eIDAS reference	How requirement met	How ascertained e.g. interview, observation, testing
Art.19.2	The TSP has an up to date security incident policy which includes a breach handling procedure. It is held on the intranet and is regularly communicated to staff. This which says that where staff become aware of an information security breach or a breach of integrity in regard to the trust service, they must report it to the service desk immediately. Service desk staff will risk assess the reported breach and will ……. etc	• Interview with staff • Observation and examination of information security incident policy • Viewing staff intranet etc….
Art.24.2 A qualified trust service provider providing qualified trust services shall		
Art.24.2.a	The TSP is aware of the requirement to inform the ICO of any change in the provision of its qualified trust services and an intention to cease those activities. This is reflected in the Qualified	• Interview • Observation of policy.etc…

	Trust Service Policy…. etc.	
Art.24.2.b	The project manager for the trust service is suitably qualified possessing x, y and z qualification and having worked with trust services for 10 years etc…… There are also two project officers who have xyz qualifications and over 2 years of experience each etc…	• Interview • Review of HR records etc….

4.0 Conclusion

4.1 The findings commented upon in this report were accurate at the time of the conformity assessment.

4.2 Any substantial change to the qualified trust service should be reported to the supervisory body, the Information Commissioner's Office, so that they may decide whether it compromises the qualifed status of the trust service and determine whether a new conformity assessment should be carried out.

4.3 In any case, a conformity assessment must be carried out again by [insert date 24 months from the date of this conformity assessment]