

# Guide to eIDAS

**ico.**

Information Commissioner's Office

About the Guide to eIDAS	3
What is the eIDAS Regulation?	4
Key definitions	6
Security and accessibility of trust services	11
Breach reporting	14
Qualified trust services	17
Qualified trust service provider obligations	20
Becoming a qualified trust service provider	23
Using the UK Trusted List	27
UK Trusted List	30
Enforcement	33
Approved qualified trust service providers	34

# About the Guide to eIDAS

## ■ [Latest changes](#)

### 06 March 2023

- Additional requirements and guidance added in the “Becoming a qualified trust service provider” section.

### 29 September 2022

- From the 1 October 2022, the ICO has responsibility for the management and publication of the trusted list.
- We have added the binary (DER) and text (Base64 encoded) format certificates for the UK Trusted List.

### 19 August 2022

- Brief description added to explain the trusted list is an authoritative source of information for qualified trust providers and their services.
- Individual sections updated to say the ICO will be taking responsibility for the trusted list from 1 October 2022 and describing any impact.
- Within the “Using the UK Trusted List” section we have replaced the word ‘hash’ with ‘digest’.
- Added new **UK Trusted List page**. This contains a download link to the UK trusted list, information on the trusted list and the rules under which it operates.

The UK eIDAS Regulations provide the legal framework for the use of electronic trust services offered within the UK and recognise equivalent services offered in the EU.

Electronic trust services can be used in a number of ways to provide security for electronic documents, communications and transactions e.g. to help ensure that documents sent electronically have not been altered in any way and that the sender can be easily recognised. Electronic trust services allow for such security properties to be applied and then validated and thus help ensure confidence in the electronic transfer of information.

This guide is for organisations providing trust services in the UK such as certificates for electronic signatures, certificates for electronic seals, certificates for website authentication, electronic time stamps and, electronic registered delivery services.

It gives a brief introduction to the UK eIDAS Regulations, summarises the requirements for trust services, and explains the ICO’s role in supervising trust service providers in the UK.

# What is the eIDAS Regulation?

## At a glance

- The UK eIDAS Regulations set out rules for UK trust services and establishes a legal framework for the provision and effect of electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and certificate services for website authentication.
- Trust services increase confidence in the use of electronic transactions through mechanisms such as verifying the identity of individuals and businesses online and verifying the authenticity of electronic data e.g. documents.
- The UK eIDAS Regulations are an amended form of the EU eIDAS Regulation and retain many aspects of the EU regulation but are tailored for use within the UK.
- Although the UK eIDAS Regulations allows the legal effect of EU eIDAS qualified services to continue to be recognised and used in the UK, no reciprocal agreement currently exists. This means UK eIDAS Regulation qualified trust services are not automatically recognised and accepted as equivalent in the EU.
- The UK Regulation includes no provisions relating to electronic identification schemes and excludes chapter II of the EU eIDAS regulation.
- The ICO is the supervisory body for UK trust service providers. We can carry out audits, grant qualified' status, and take enforcement action.

## In brief

- [What does 'eIDAS' mean?](#)
- [What is the eIDAS Regulation?](#)
- [What does it cover?](#)
- [What is the ICO's role?](#)

## What does 'eIDAS' mean?

'eIDAS' is shorthand for 'electronic identification and trust services'. It refers to a range of services that include verifying the identity of individuals and businesses online and verifying the authenticity of electronic documents.

Read the key definitions section of this guide for more detail on specific types of trust services.

## What are the UK eIDAS Regulations?

The eIDAS Regulation is [Regulation \(EU\) 910/2014 on electronic identification and trust services for electronic transactions in the internal market](#). Following the UK withdrawal from the EU the eIDAS Regulation was adopted into UK law and amended by [The Electronic Identification and Trust Services for Electronic Transactions \(Amendment etc.\) \(EU Exit\) Regulations 2019](#). In addition, the existing UK trust services legislation, [The Electronic Identification and Trust Services for Electronic Transactions Regulation](#)

[2016 \(2016 No.696\)\)](#) was also amended. Taken together, these regulations are referred to in this guidance as the UK eIDAS Regulations.

If you offer trust services in the EU (rather than the UK), you will need to comply with the EU eIDAS Regulation, including operating under the supervision of a supervisory body from another EU member state.

Although the UK eIDAS supervisory body has no EU eIDAS regulatory obligations it continues to work closely with other EU supervisory authorities.

For background information on the EU eIDAS Regulation and relevant binding implementing decisions adopted by the European Commission, visit the [Commission webpages on trust services and eID](#).

Further expert advice and recommendations on the implementation of the EU eIDAS Regulation, trust service providers and trust services can be found on the [European Union Agency for Network and Information Security \(ENISA\)](#) web site. Although these materials refer to the EU eIDAS Regulation, they are a useful resource for understanding the requirements of the UK eIDAS regulations

## What does it cover?

Chapter III of the Regulation sets out requirements for trust services. It also sets out what trust service providers need to do if they wish to gain qualified status, which entitles them to be listed on the UK trusted list as a qualified trust service provider.

This guide focuses on the trust service provisions in Chapter III of the eIDAS Regulation.

## What is the ICO's role?

The ICO has responsibility for supervision of the trust service provisions of the UK eIDAS Regulations. The ICO can grant and revoke qualified status for trust service providers established in the UK, approve or reject qualified trust services, report on security breaches, carry out audits and take enforcement action.

# Key definitions

## At a glance

In this guide we've tried to keep jargon to a minimum. However, there are a few key defined terms, including:

- trust service: a service designed to protect electronic data and demonstrate that it can be trusted. For example, by showing that data is authentic, or hasn't been tampered with, or by identifying the originator of the data e.g. a person or organisation.
- qualified trust service: a trusted service, supported by UK law, that meets the requirements of the UK eIDAS Regulations and is offered by a 'qualified' trust service provider.
- trust service provider: any organisation or person providing trust services;
- qualified trust service provider: an organisation or person providing qualified trust services and granted qualified status by the ICO.

## In brief

- [What is a 'trust service'?](#)
- [What is a 'qualified trust service'?](#)
- [What is a 'trust service provider'?](#)
- [What is a 'qualified trust service provider'?](#)
- [What is an 'electronic signature'?](#)
- [What is an 'electronic seal'?](#)
- [What is an 'electronic time stamp'?](#)
- [What is an 'electronic registered delivery service'?](#)
- [What is a 'certificate related to those services'?](#)
- [What is a 'certificate for website authentication'?](#)
- [What is a 'conformity assessment body'?](#)

## What is a 'trust service'?

Trust services aim to ensure trust, security and legal certainty in electronic transactions. For example, an electronic service which helps to confirm that electronic data e.g. a document, is sent from a trusted source, is authentic and hasn't been tampered with.

There are five specific types of trust service covered by the UK eIDAS Regulations:

- electronic signatures;
- electronic seals;
- electronic time stamps;
- electronic registered delivery services; and

- website authentication certificates.

The full definition of trust service is in UK eIDAS Regulations Article 3:



“an electronic service normally provided for remuneration which consists of:

- (a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or
- (b) the creation, verification and validation of certificates for website authentication; or
- (c) the preservation of electronic signatures, seals or certificates related to those services”.

### What is a ‘qualified trust service’?

Qualified trust services are trust services which have been assessed by an eIDAS accredited assessment body and granted qualified status by the ICO. By meeting the requirements set out in the UK eIDAS Regulation they provide a high degree of confidence and trustworthiness e.g. via stringent methods of authentication and validation of service users, adoption of strong operational security controls etc. Qualified trust services have special recognition in UK law and can only be offered by qualified trust service providers.

### What is a ‘trust service provider’?

A trust service provider is anyone who provides a trust service. This term includes both qualified and non-qualified trust service providers.

### What is a ‘qualified trust service provider’?

A qualified trust service provider is an organisation providing qualified trust services that has been granted qualified status by the ICO. For any UK eIDAS defined qualified trust service, a trust service provider must comply with the requirements for trust service providers set out in the UK eIDAS Regulations and demonstrate their compliance via a process which involves an assessment by an eIDAS accredited assessment body and approval by the ICO.

Following ICO approval, qualified trust service provider information and the qualified services they provides are published on a ‘trusted list’. This list can be used to verify the qualified status of a trust service

### What is an ‘electronic signature’?

An electronic signature is defined in UK eIDAS Regulation article 3 as:



“data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign”.

As you might expect, this means an electronic signature is any method an individual uses to ‘sign’ an electronic document. This covers a wide range of measures, from the simple act of affixing text or a digital image, to more sophisticated hi-tech methods which meet specific criteria set out in the UK eIDAS Regulation for advanced or qualified electronic signatures. Electronic signatures are admissible as evidence in court.

Advanced electronic signatures meet the extra requirements set out in UK eIDAS Regulation Article 26. They are required to uniquely link to the person signing the data in electronic form and can detect any changes made to the data within the document afterwards.

Qualified electronic signatures have the same features as advanced electronic signatures, but are created using more sophisticated technology, meet a higher standard of security, meet stricter validation criteria, and are supported by a more detailed certificate. They have the same legal effect as a handwritten signature.

## What is an ‘electronic seal’?

An electronic seal is defined in UK eIDAS Regulations Article 3 as:



“data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter’s origin and integrity”.

Electronic seals allow companies and other corporate bodies to ‘seal’ electronic documents and certify them as genuine, in the same way as an individual can use an electronic signature. They are admissible as evidence in court. As with electronic signatures, there are advanced and qualified electronic seals offering additional benefits over basic electronic seals.

Advanced electronic seals meet the extra requirements set out in UK eIDAS Regulation Article 36. They are more reliably linked to the organisation creating the seal, and like advanced and qualified electronic signatures allow detection of any changes made afterwards to the sealed data.

Qualified electronic seals have the same features as advanced electronic seals, but are created using more sophisticated technology, meet a higher standard of security, meet stricter validation criteria, and are supported by a more detailed certificate.

## What is an ‘electronic time stamp’?

An electronic time stamp proves that particular data existed at a particular time and hasn’t been changed since then. It is defined UK eIDAS Regulation Article 3 as:





“data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time”.

Qualified electronic time stamp services must be operated by a qualified trust service provider and are required to meet the UK eIDAS requirements for qualified electronic time stamps.

### What is an ‘electronic registered delivery service’?

An electronic registered delivery service is defined in UK eIDAS Regulation Article 3 as:



“a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations”.

In other words, electronic registered delivery services act as a kind of secure online proof of posting or recorded delivery service. They provide proof that information was sent and received electronically, and that it was not intercepted or altered on the way.

Qualified electronic registered delivery services must be operated by one or more qualified trust service providers and are required to meet the UK eIDAS Regulation requirements for qualified electronic registered delivery services.

### What is a ‘certificate related to those services’?

A certificate for an electronic signature or seal is an “electronic attestation” containing the data that verifies the signature or seal is valid and links it back to a specific named person (for signatures) or organisation (for seals). In very basic terms, a certificate in this context is the underlying digital data that makes a trust service work and confirms the origin and authenticity of signed or sealed data e.g. a document.

A qualified certificate must be issued by a qualified trust service provider and include the specific information set out in the annexes to the UK eIDAS Regulation.

A certificate for electronic signature or seal is different from a certificate for website authentication.

### What is a ‘certificate for website authentication’?

Certificates for website authentication identify the person or company behind a website and help to verify that the website is genuine. They are defined in UK eIDAS Regulation Article 3 as:




“an attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued”.

In this guide we generally use the term ‘website authentication certificates’.

Qualified website authentication certificates must be issued by a qualified trust service provider and are required to meet the UK eIDAS Regulation requirements for qualified web authentication certificates.

### What is a ‘conformity assessment body’?

Conformity assessment bodies play a key role if you want to become a qualified trust service provider. If you want to gain qualified status, you must first ask a conformity assessment body to look at whether you meet the relevant UK eIDAS Regulation requirements for trust service providers and the trust service(s) you wish to provide. The conformity assessment body will conduct an assessment and produce a ‘conformity assessment report’ that is provided to the ICO for review. Read the section of this guide on [becoming a qualified trust service provider](#) for more on this process.

UK conformity assessment bodies must be formally accredited by the the [UK Accreditation Service \(UKAS\)](#) . The ICO is not involved in accrediting or overseeing these bodies. You can contact UKAS for more information on organisations that have been accredited by UKAS as UK eIDAS Regulation conformity assessment bodies.

# Security and accessibility of trust services

## At a glance

- You must take appropriate measures to safeguard the security of trust services. This means identifying security risks and taking reasonable action to mitigate them.
- Qualified trust service providers need to take some specific security measures.
- Wherever feasible, you should make trust services accessible for people with disabilities.

## In brief

- [What does the law say about security measures?](#)
- [What must we do to comply?](#)
- [What are 'appropriate measures'?](#)
- [Do qualified trust service providers need to do more?](#)
- [When do we need to 'inform stakeholders of adverse effects'?](#)
- [What are the rules on accessibility?](#)

## What does the law say about security measures?

The UK eIDAS Regulation sets out trust service providers' security obligations. Article 19(1) says:



“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.”

## What must we do to comply?

If you are a trust service provider, you need to have appropriate security measures to prevent the services you offer being accidentally or deliberately compromised. In particular, you need to:

- carry out regular risk assessments of the security of your trust services;
- identify and classify security risks according to degree of risk posed and the harm that could result;
- make sure you have appropriate technical security and organisational measures to mitigate those risks, including robust policies and procedures and reliable, well-trained staff; and
- respond to any security incidents that do occur swiftly and effectively to help prevent and minimise their impact.

## What are ‘appropriate measures’?

An appropriate measure is one that is proportionate to the risks it safeguards against. You should consider the current developments in security technology when choosing appropriate measures to protect your trust service, and you should regularly review your security measures as technology develops.

ENISA has published a set of [detailed guidelines on security requirements, risk assessments and risk mitigation for trust service providers](#) which may be relevant to your assessment of appropriate security measures.

Most EU organisations seeking to provide qualified trust services use the ETSI trust service provider standards as the basis for the development and evaluation of their services. These are highly detailed and comprehensive standards which cover all of the EU and UK eIDAS Regulations’ defined trust services.

You may find it useful to refer to the [security section of the ICO’s guide to UK GDPR](#) to understand the ICO’s approach to ‘appropriate technical and organisational measures’ to safeguard personal data.

## Do qualified trust service providers need to do more?

All trust service providers must take appropriate security measures, but if you are a qualified trust service provider you also need to comply with specific minimum security requirements set out in UK eIDAS Regulations Article 24(2). You should look at these carefully as the requirements are detailed and require specific consideration, but in summary you need to:

- employ reliable staff and subcontractors with the necessary expertise, experience and qualifications;
- ensure staff and subcontractors have received appropriate security and data protection training;
- use trustworthy, secure and reliable products and systems;
- ensure your systems have appropriate access controls to protect data from unauthorised access or modification and ensure that unauthorised changes are detectable;
- implement internal processes and procedures that support the security of the trust service and protect against forgery and theft;
- ensure personal data is processed in line with data protection legislation.

The ENISA guidance and ETSI standards referenced in the previous section are also very useful here.

## When do we need to ‘inform stakeholders of adverse effects’?

You need to consider whether it is necessary to inform your customers and anyone else who might be affected by a security incident about the harm that could be caused by the incident. In some cases this could include a public statement. Read the [Breach reporting](#) section of this guide for more information.

## What are the rules on accessibility?

You must make trust services accessible for people with disabilities wherever it’s feasible to do so.

In particular, you need to comply with any relevant UK equality laws (such as the Equality Act 2010) to ensure your trust service is accessible to people with a disability.

ETSI standard EN 301 549 may support your assessment of the accessibility of your trust service.

# Breach reporting

## Report a breach

Trust Service Providers and Qualified Trust Service providers must report notifiable breaches of the eIDAS regulation, pursuant to Article 19 (2) of the Regulation.

[Report an eIDAS breach](#) 

## At a glance

- If a security breach has a 'significant impact' you must notify the ICO within 24 hours.
- You must also notify your users if they are likely to be affected.
- In some circumstances you or the ICO may also need to inform the wider public about a breach.

## In brief

- [What is a breach under eIDAS?](#)
- [What must we do if there is a breach?](#)
- [When and how do we notify the ICO?](#)
- [When and how do we notify those affected?](#)
- [Will the ICO notify anyone else?](#)

## What is a breach under eIDAS?

A breach under eIDAS is:



“any breach of security or loss of integrity that has a significant impact on a trust service provided or on the personal data maintained therein.”

A breach may occur if there is a deliberate attack compromising the integrity of your service. But a breach can also occur if there is an unauthorised access within your organisation or an accidental loss of integrity.

Not every incident relating to a lapse in security or integrity of a trust service is a breach. If there is no harm caused, or there is only a minimal effect, this will not qualify as a breach. However, you should still review your security measures.

## What must we do if there is a breach?

Breach reporting rules are set out in UK eIDAS Regulation Article 19. You do not need to report every incident relating to a lapse in security or integrity of a trust service. However, where you have reason to believe that an incident has or is likely to have a significant (more than minimal) impact on the trust service or the personal data you hold, you need to:

- notify the ICO;
- consider whether to notify your users; and
- consider whether to inform anyone else who might be affected.

If you are not sure about whether the impact of an incident is significant or not, it is safer to report the breach.

## When and how do we notify the ICO?

You must notify the ICO within 24 hours of becoming aware of the breach, or sooner if it's reasonable to do so.

Please use our [eIDAS breach notification form](#).

If there has also been a personal data breach, there is no need to fill out a separate data protection security breach form as well. You should however include relevant details on the eIDAS breach notification form, and we may call you back if we need more information.

Please read the ICO's guide to UK GDPR for more information on [personal data breaches](#).

## When and how do we notify those affected?

If the breach is likely to adversely affect your users, you will also need to notify them of the breach without undue delay.

You don't need to use a specific format for this. You can choose how you prefer to communicate with your customers, as long as it reaches them promptly. We advise you to include:

- your name and contact details;
- the date of the breach;
- a summary of the incident;
- the likely effect on them;
- any measures you have taken to address the breach; and
- any steps they can take to protect themselves from harm.

You should also consider whether you can take measures to inform other people of the effects of a security breach who may have been affected by a security incident but are not your direct customers. For example, any end users relying on the integrity of the trust service.

We may require you to disclose information to the public about a breach if we think it is in the public interest to do so.

## Will the ICO notify anyone else?

---

If a breach has an impact outside the UK we may choose to inform relevant overseas authorities.

We may require the trust service provider to inform the public about the breach or we may inform the public of a breach ourselves if we think it is in the public interest to do so.



# Qualified trust services

## At a glance

- Qualified trust services can only be offered by a qualified trust service provider.
- They provide a high degree of confidence and trustworthiness in the service and must comply with the UK eIDAS Regulations requirements for qualified trust services.

## In brief

- [What are the rules on qualified electronic signatures?](#)
- [What are the rules on qualified electronic seals?](#)
- [What are the rules on qualified electronic time stamps?](#)
- [What are the rules on qualified electronic registered delivery services?](#)
- [What are the rules on qualified website authentication certificates?](#)

## What are the rules on qualified electronic signatures?

Qualified electronic signatures must:

- meet the specific requirements for an advanced signature;
- be created using a qualified signature creation device; and
- be based on a qualified certificate.

The requirements for advanced and qualified electronic signatures are set out in UK eIDAS Regulation Article 26. Advanced and qualified electronic signatures must be uniquely linked to an identifiable signatory who has sole control of the data used to create the signature. They must also ensure that any changes made to the signed data can be detected.

Qualified electronic signature creation devices (the hardware or software used to create the signature) must meet the requirements in annex II of the UK eIDAS Regulation, must be certified by an approved body (designated as such by the UK), and must conform to the security assessment standards stated in UK eIDAS Regulation Article 30.

Qualified certificates for electronic signatures (the supporting data that verifies the signature is valid and links it to the named signatory) must include all of the details listed in annex I of the UK eIDAS Regulation, including the advanced electronic signature or seal of the qualified provider.

The validity of a qualified electronic signature can be confirmed by following the validation criteria in UK eIDAS Regulation Article 32. If you are a qualified trust service provider, you can offer qualified validation services if your process gives automated, reliable and efficient results which bear your advanced electronic signature or seal.

You can also offer a qualified preservation service to guarantee qualified electronic signatures for an

extended period of time, if you have the procedures and technology to do so. See UK eIDAS Regulations Article 33.

## What are the rules on qualified electronic seals?

The rules on qualified electronic seals are essentially the same as those on qualified electronic signatures. They must:

- meet the specific requirements for an 'advanced' seal;
- be created using a 'qualified electronic seal creation device'; and
- be based on a qualified certificate.

The requirements for advanced and qualified seals are set out in UK eIDAS Regulation Article 36. They must be uniquely linked to an identifiable organisation who has control of the data used to create the seal. They must also ensure that any changes made to the sealed data can be detected.

Qualified electronic seal creation devices are governed by the same rules as qualified signature creation devices discussed in the previous section.

Qualified certificates for qualified electronic seals (the supporting data that verifies the seal is valid and links it to the named organisation) must include all of the details listed in annex III of the UK eIDAS Regulation.

The validity of a qualified electronic seal can be confirmed by following the validation criteria in UK eIDAS Regulation Article 32. If you are a qualified trust service provider, you can offer qualified validation services if your process gives automated, reliable and efficient results which bear your advanced electronic signature or seal.

You can also offer a qualified preservation service to guarantee qualified electronic seals for an extended period of time, if you have the procedures and technology to do so. See UK eIDAS Regulation Article 33.

## What are the rules on qualified electronic time stamps?

The requirements for qualified electronic time stamps are stated in UK eIDAS Regulation Article 42. To provide a qualified electronic time stamp service you must:

- be a qualified trust service provider;
- use a method of binding the date and time to the data that is reasonably certain to prevent undetectable changes;
- use a time source linked to [Coordinated Universal Time \(UTC\)](#); and
- sign or seal it with your advanced electronic signature or seal.

## What are the rules on qualified electronic registered delivery services?

The requirements for qualified electronic registered delivery services are stated in UK eIDAS Regulation Article 44. To provide this service you must be a qualified trust service provider and the service must:

- ensure the identity of the sender 'with a high level of confidence';
- ensure the identity of the receiver of the document before delivery;
- apply your own advanced electronic signature or seal to the data being delivered (e.g. a document) to prevent any undetectable changes in transit;
- clearly indicate any changes to the data required to support its sending or receipt; and
- use a qualified electronic time stamp to indicate when data is sent, received or changed.

## What are the rules on qualified website authentication certificates?

Qualified website authentication certificates must include all of the details listed in annex IV of the UK eIDAS Regulation, including the advanced electronic signature or seal of the qualified trust service provider issuing the certificate.

# Qualified trust service provider obligations

## At a glance

As well as meeting the requirements for qualified trust services, if you are a qualified trust service provider, you must:

- take specific minimum security measures;
- have clear and comprehensive terms and conditions;
- have robust identity verification for your qualified certificates;
- keep a qualified certificate database;
- keep good records of other relevant data;
- be able to cover any legal claims for damages;
- notify the ICO of any changes to your services; and
- have an up-to-date termination plan.

## In brief

- [What specific security measures should we take?](#)
- [What information should we include in our terms and conditions?](#)
- [How should we verify the identity of our customers?](#)
- [What is a 'qualified certificate database'?](#)
- [What other records do we need to keep?](#)
- [Do we need liability insurance?](#)
- [What do we need to tell the ICO?](#)
- [What is a 'termination plan'?](#)

### What specific security measures should we take?

You must always take all appropriate security measures, but there are some specific minimum security requirements for qualified trust service providers set out in UK eIDAS Regulation Article 24(2). Read the section in this guide on security measures for more information.

### What information should we include in our terms and conditions?

From the outset, you need to provide clear and comprehensive terms and conditions to anyone seeking to use your service. In particular, your terms and conditions must include any limitations on the use of your service.

Although you need to include sufficient detail, you should make your terms as concise as possible, use clear and straightforward language and try to avoid off putting legal or technical jargon wherever you can.

## How should we verify the identity of our customers?

If you are a qualified trust service provider, UK eIDAS Regulation Article 24(1) requires you to verify the identity of any individual or organisation to whom you issue a qualified certificate. It sets out four verification options:

- in person, by the physical presence of the person or authorised representative of the organisation;
- using electronic ID that was itself originally verified in person, and meets the eIDAS assurance level of “substantial” or “high” set out in EU eIDAS Regulation Article 8;
- using a certificate of a qualified electronic signature or seal that was itself verified in person or using electronic ID as set out above; or
- using another method recognised by the UK government which is confirmed by a conformity assessment body as being as reliable as verification in person. If you choose this option you will need to provide evidence that this is the case.

You can carry the verification out yourself or use a subcontractor.

## What is a ‘qualified certificate database’?

If you issue qualified certificates (for electronic signatures, seals or website authentication), you must establish a database of those certificates and keep it up to date.

This enables you to keep track of the status of the qualified certificates you issue. It’s up to you to decide exactly what details you include, but as a minimum it should show the status of each certificate – that is, whether it is valid, suspended, expired or revoked. You will therefore need to include a certificate’s issue date, expiry date, and any revocation date.

If you revoke a qualified certificate, you must record the fact in the database and publish this information as soon as possible and within 24 hours. Certificates are considered to have been revoked as soon as this information is published.

You must provide free, reliable, automated information on the status of a qualified certificate to anyone relying on it. This must be available even after a certificate has expired.

## What other records do we need to keep?

You must keep accessible records of all relevant information concerning data you have issued and received, to be used as evidence in court if required and to ensure the continuity of the service.

You must keep these records for an appropriate period of time, even if you stop providing trust services.

## Do we need liability insurance?

People who rely on your services could take legal action against you if they have suffered damage as a result of you failing to comply with the UK eIDAS Regulation. As a qualified trust service provider, you would need to prove that the damage was not deliberate and was not caused by your negligence.

The UK eIDAS Regulation requires you to either maintain sufficient funds to cover any legal claims, or obtain appropriate insurance cover for this risk.

## What do we need to tell the ICO?

You need to [report any security breaches](#) to us within 24 hours.

You also need to tell us about any changes to the services you offer, or if you intend to stop offering those services.

## What is a 'termination plan'?

You need to create a plan to deal with the issues that will arise if and when you decide to stop providing a qualified trust service. In particular, the plan needs to set out what records you will keep after termination to provide continuity of service and to provide evidence in court if necessary. You also need to include how long this information will be retained for. You must keep the plan updated.

# Becoming a qualified trust service provider

## At a glance

- To become a qualified trust service provider you need to demonstrate to a 'conformity assessment body' that you meet the relevant requirements for qualified trust service providers and the trust services you wish to provide, and submit a conformity assessment report to the ICO for verification.
- If you make significant changes to your qualified trust service, or intend stopping the service, you must tell the ICO.
- The ICO has additional requirements and guidance for prospective UK eIDAS qualified trust service providers to consider.

## In brief

- [How do we become a qualified trust service provider?](#)
- [What is the trusted list?](#)
- [What if we need to change a qualified trust service?](#)
- [What happens if we stop providing a qualified trust service?](#)
- [What are the additional ICO requirements and guidance for prospective UK qualified trust service providers?](#)

## How do we become a qualified trust service provider?

In summary, you need to apply to a conformity assessment body who will assess your compliance against the requirements for qualified trust service providers and qualified trust services. The conformity assessment body will produce a conformity assessment report, demonstrating how the requirements have been met. You then submit this report to the ICO for verification. The ICO will analyse the report to ensure all requirements have been met, and will grant you qualified status if appropriate.

The conformity assessment body must be accredited by UKAS for undertaking conformity assessments against the UK eIDAS Regulations.

The following organisations are currently accredited.

### **BSI Assurance UK Ltd**

Kitemark Court  
Davy Avenue  
Knowlhill  
Milton Keynes  
MK5 8PP

Email: [\[email protected\]](#)

When a conformity assessment body is accredited both in the UK and the EU, for any trust service provider

seeking QTSP status in the UK and the EU, a single conformity assessment may (subject to approval by the relevant EU supervisory body) be used as the basis for a conformity assessment report issued against the UK eIDAS Regulations and a separate conformity assessment report issued against the EU eIDAS Regulation.

If you gain qualified status, you will be added to the UK's trusted list.

To maintain qualified status you will need to undergo the conformity assessment process at least every two years, at your own expense.

If you are considering becoming a qualified trust service provider, you can contact the ICO at [\[email protected\]](#) for further information and guidance.

## What is the trusted list?

The trusted list is a published list of all qualified trust service providers and qualified trust services granted qualified status in the UK by the ICO.

## What if we need to change a qualified trust service?

If you make changes to your qualified trust service you should [contact the ICO](#) to determine whether your qualified status is still valid and whether or not you should undergo a new conformity assessment.

## What happens if we stop providing a qualified trust service?

If you decide to stop providing a qualified trust service you need to notify the ICO of your intention to stop the service. To stop providing a qualified trust service you are required to use your termination plan. After you have implemented your termination plan you need to provide to the ICO a description of how you have implemented the provisions in your termination plan.

You can contact the ICO at [\[email protected\]](#) for further information and guidance on this process.

## Additional ICO requirements and guidance

The requirements and guidance listed here is for use by prospective qualified trust service providers and their conformity assessment bodies in meeting the requirements of the UK eIDAS Regulation for qualified services operating in the UK.

The ICO strongly advises all prospective qualified trust service providers to discuss their services with the ICO before they submit their notification. This will allow the ICO to describe the notification process in more detail, allow it to better understand the prospective qualified trust service provider's intentions and services for the UK, and allow any questions or issues to be addressed.

## UK qualified trust service providers

- UK qualified trust services may only be operated under supervision of the ICO. It is not possible for a trust service to be supervised by an alternative supervisory body or by more than one supervisory body. This means, for example, that qualified trust services offered by trust service providers (TSPs) established in the UK cannot also be supervised by an EU member state supervisory body operating



under the EU eIDAS Regulation.


- An existing EU qualified trust service provider wishing to operate in the UK may provide the same or different service types as those offered in the EU. UK services of the same type must be legally separate however from the EU services. For example, an EU eIDAS approved qualified trust service provider issuing qualified certificates may also provide the same type of service in the UK i.e., issuing UK qualified certificates from the UK service approved by the ICO.
- Notifying trust service providers must be established in the UK. For example, a limited company would need to have a UK establishment and be registered or incorporated within the UK. A limited partnership or a limited liability partnership would need to be registered at Companies House and an unincorporated business would need to demonstrate that it has a permanent place in the UK where it carries out its business activities.

## Conformity assessment

- Conformity assessment bodies approved to undertake conformity assessments against the UK eIDAS Regulation must be accredited by [UKAS](#), the UK national accreditation body.
- Trust service provider notifications for UK qualified trust services shall only be accepted with a full conformity assessment report. Surveillance audits, or surveillance audits supported by additional supporting information such as service changes notices, are not a sufficient basis for notification and assessment. This applies to all existing qualified trust service providers who currently provide trust services in other jurisdictions e.g., in the EU, who have an established audit regime with an approved conformity assessment body, and who wish to provide similar services in the UK under the UK eIDAS Regulation.
- Conformity assessment reports for qualified trust service providers wishing to operate in the UK must be specifically produced against the UK eIDAS Regulation and for the trust service provider UK established legal entity. The subject of a conformity assessment report must be a UK legal entity owning the trust services. This means a conformity assessment report produced for an existing non-UK qualified trust service provider, eg, an EU qualified trust service provider, cannot be accepted directly by the ICO as part of the required notification process documentation.
- Conformity assessment reports produced by an EU accredited conformity assessment body may be used by a UK accredited conformity assessment body as part of its assessment for UK based services. This would require the UK conformity assessment body to have an outsourcing agreement with the EU conformity assessment body (See ISO 17065, 6.2.2), satisfy itself that the EU produced conformity assessment report was fit for purpose, and carry out any additional auditing to meet the UK requirements.
- Where a conformity assessment body is accredited in the UK for performing UK eIDAS assessments and also accredited in the EU for undertaking EU eIDAS assessments, the ICO will accept a conformity assessment report issued against the UK eIDAS Regulations which is based on the results of a single conformity assessment undertaken by the conformity assessment body which covers both jurisdictions. It is expected this would also require approval of the relevant EU supervisory body should a trust service provider and conformity assessment body wish to pursue this approach.
- Conformity assessment reports for UK qualified trust service providers must contain the information specified by the ICO in its qualified trust service provider notification form.

## Qualified services

- UK services must be identified as such in trust service provider documentation e.g., certificate policy and certification practice statement documents for qualified certificate services.

- Where a qualified trust service provider operates services in the UK and the EU, it is not necessary for separate service documents to exist e.g., a separate certificate policy for the UK services and one for the EU services. All documentation however should clearly distinguish UK services and EU services. For example, it is not possible to use an existing EU based certificate policy directly for a UK service without modification to make the policy applicable to both EU and UK services.
- Qualified trust service provider services users (subscribers, relying parties) shall contract with the qualified trust service provider UK legal entity for the provision of the services. Any associated documentation e.g., subscriber or relying party agreement, should also support this.
- It should be clear to service users that trust service outputs e.g., qualified certificates for signatures or seals issued from UK qualified trust service provider services, are issued in compliance with the UK eIDAS Regulation. These are legally distinct from those issued under the EU eIDAS Regulation.
- ICO approved qualified services operating in accordance with UK eIDAS Regulations are not recognised within the EU, therefore UK qualified trust service outputs e.g., qualified certificates for signatures or seals, do not carry qualified status under the EU eIDAS Regulation. The UK however recognises qualified trust services operating under the EU eIDAS regulation and thus EU qualified trust service provider trust service outputs are recognised as legally equivalent e.g., a qualified electronic signature created using an EU issued qualified certificate would have the same legal recognition as a qualified electronic signature created using a UK qualified trust service provider issued qualified certificate.
- UK qualified trust services must use separate trusted list service digital identities if the same service types are also provided under the EU eIDAS Regulation or other regime.
- UK qualified certificate based services should use different certificate policy object identifiers (OIDs) if the equivalent services are also provided under the EU eIDAS Regulation or other regime.
- Qualified trust service provider termination plans must align with the ENISA guidelines. See [Guidelines on Termination of Qualified Trust Services — ENISA \(europa.eu\)](#) .
- A qualified trust service provider may provide services in the UK and the EU using shared service components and practices, provided the UK eIDAS Regulation is met for UK provided services, the EU eIDAS Regulation is met for EU provided services, and any risks introduced to services through the use of such sharing are identified and addressed as part of the qualified trust service provider's risk management process. Prospective UK qualified trust service providers who currently provide equivalent services under the EU eIDAS Regulation or other regime, or intend to do so, are advised to check with the relevant body in other jurisdictions regarding the use of shared service components and practices.
- Qualified signature creation devices (QSCDs) certified in accordance with the EU eIDAS regulation are acceptable for use in the UK.
- Where remote identity proofing is used, the ICO shall review and approve the mechanisms used before their first use in qualified services.

# Using the UK Trusted List

## At a glance

- You can use the UK trusted list to check the details and status of qualified trust service providers.
- You can download the trusted list, authenticate it to check it is legitimate and monitor it to determine when its content changes.

## In brief

- [What is the UK trusted list?](#)
- [How can I check the details and status of a qualified trust service?](#)
- [Where can I get the trusted list?](#)
- [How can I check the authenticity of the trusted list?](#)
- [How can I check when the trusted list changes?](#)
- [Why has the trusted list moved to the ICO?](#)
- [Will tScheme continue to also publish the trusted list?](#)
- [What is the 'final EU UK' trusted list'?](#)
- [Will the ICO publish a PDF version of the list?](#)
- [How can I get more information of the trusted list move?](#)

## What is the UK trusted list?

The UK trusted list shows whether a trust service provider has been granted qualified status and which of its services are qualified. The trusted list is the single authoritative source you can use to verify that the ICO has granted a trust service provider, and one or more of its services, with qualified status.

## How can I check the details and status of a qualified trust service?

The trusted list contains an entry for each qualified trust service provider. This entry contains details such as:

- the qualified trust service provider name and address;
- when qualified status was granted;
- the types of services that have been approved as qualified;
- what the services can be used for, and
- associated historical information (where applicable) on the provided services.

When you are verifying a trust service output, eg a qualified electronic signature, you may need to check the UK trusted list as part of your verification procedures.

## Where can I get the trusted list?

[The ICO hosts the trusted list](#). It is available in a machine-readable format (XML). To support publication of the trusted list there is also a SHA256 digest file of the list to support monitoring of changes to the list, and a list verification digital certificate to verify the digital signature on the list.

## How can I check the authenticity of the trusted list?

You can check the authenticity of the trusted list by verifying the digital signature on the list using the ICO verification certificate. You can download the certificate in either [binary \(DER\)](#) or [text \(Base64 encoded\) format](#). The certificate thumbprint is a3 ad 36 4f 7f af d5 7b f7 0c e0 3d e0 f4 89 33 d7 12 07 a2.

The verification certificate may be changed up to 1 year prior to expiry and you can check these pages before that time for notification of any change.

## How can I check when the trusted list changes?

You can monitor for changes to the trusted list content, eg the addition of a newly qualified trust service provider or a change in the status of an existing one, by checking [the SHA256 digest value](#) of the currently published trusted list against a locally cached version.

## Why has the trusted list moved to the ICO?

The Department for Culture Media and Sport (DCMS), the UK Government department responsible for eIDAS, decided to transfer the responsibility for management and publication of the trusted list to the ICO. The ICO has been the UK trusted list scheme operator and the UK Supervisory Body for eIDAS since 1 October 2022.

## Will tScheme continue to also publish the trusted list?

From 1 October 2022, the trusted list will no longer be available from the tScheme website and [will only be available from the ICO website](#).

## What is the ‘final EU UK’ trusted list’?

At the end of the Brexit transition period tScheme published a final version of the EU UK trusted list. This will continue to be available on the tScheme website.

## Will the ICO publish a PDF version of the list?

The ICO does not publish a PDF version of the list. The machine readable (XML) version of the list has a well-defined structure and contains qualified trust service provider and qualified trust service data that can be presented, searched and navigated in web browsers.

## How can I get more information of the trusted list move?

If you need additional information on the trusted list move or the trusted list in general, please contact the

ICO at [\[email protected\]](#).

# UK Trusted List

## Download the UK Trusted List

You can use the UK trusted list to check the details and status of qualified trust service providers.

[You can download the trusted list](#), authenticate it to check it is legitimate and monitor it to determine when its content changes.

## Trusted list scheme information

The present list is the trusted list including information related to the qualified trust service providers which are supervised by the United Kingdom, together with information related to the qualified trust services provided by them, in accordance with the relevant provisions laid down in [Regulation \(EU\) No 910/2014 of the European Parliament and of the Council of 23 July 2014](#) on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

## Trusted list scheme rules

### The UK Trusted List

The ICO must create a trusted list including information related to the qualified trust service providers that are under supervision, together with information related to the qualified trust services provided by them, in accordance with the relevant provisions laid down in [Regulation \(EU\) No 910/2014 of the European Parliament and of the Council of 23 July 2014](#) on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

### Policy and rules for the assessment of the listed services

The ICO must supervise qualified trust service providers as laid down in [Chapter III of Regulation \(EU\) No 910/2014](#) to ensure that those qualified trust service providers and the qualified trust services that they provide meet the requirements laid down in the Regulation. The trusted list includes as a minimum, information specified in Articles 1 and 2 of Commission Implementing Decision (EU) 2015/1505. The trusted list includes both current and historical information about the status of listed trust services. The trusted list must provide information on the supervisory scheme and where applicable, approval (e.g. accreditation) scheme(s) under which the trust service providers and the trust services that they provide are listed.

### Interpretation of the Trusted List

The general user guidelines for applications, services or products relying the trusted list published in accordance with Regulation (EU) No 910/2014 are as follows: The "qualified" status of a trust service is indicated by the combination of the "Service type identifier" ("Sti") value in a service entry and the status according to the "Service current status" field value as from the date indicated in the "Current status

starting date and time". Historical information about such a qualified status is similarly provided when applicable. Regarding qualified trust service providers issuing qualified certificates for electronic signatures, for electronic seals and/or for website authentication: A "CA/QC" "Service type identifier" ("Sti") entry (possibly further qualified as being a "RootCA-QC" through the use of the appropriate "Service information extension" ("Sie") additionalServiceInformation Extension)

- indicates that any end-entity certificate issued by or under the CA represented by the "Service digital identifier" ("Sdi") CA's public key and CA's name (both CA data to be considered as trust anchor input), is a qualified certificate (QC) provided that it includes at least one of the following:
  - the id-etsi-qcs-QcCompliance ETSI defined statement (id-etsi-qcs 1),
  - the 0.4.0.1456.1.1 (QCP+) ETSI defined certificate policy OID,
  - the 0.4.0.1456.1.2 (QCP) ETSI defined certificate policy OID,
  - and provided this is ensured by the Member State Supervisory Body through a valid service status (i.e. "undersupervision", "supervisionincessation", "accredited" or "granted") for that entry.
- and IF "Sie" "Qualifications Extension" information is present, then in addition to the above default rule, those certificates that are identified through the use of "Sie" "Qualifications Extension" information, constructed as a sequence of filters further identifying a set of certificates, must be considered according to the associated qualifiers providing additional information regarding their qualified status, the "SSCD support" and/or "Legal person as subject" (e.g. certificates containing a specific OID in the Certificate Policy extension, and/or having a specific "Key usage" pattern, and/or filtered through the use of a specific value to appear in one specific certificate field or extension, etc.). These qualifiers are part of the following set of "Qualifiers" used to compensate for the lack of information in the corresponding certificate content, and that are used respectively:
  - to indicate the qualified certificate nature:
    - "QCStatement" meaning the identified certificate(s) is(are) qualified under Directive 1999/93/EC;
    - "QCForESig" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), is (are) qualified certificate(s) for electronic signature under Regulation (EU) No 910/2014;
    - "QCForESeal" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), is (are) qualified certificate(s) for electronic seal under Regulation (EU) No 910/2014;
    - "QCForWSA" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), is (are) qualified certificate(s) for web site authentication under Regulation (EU) No 910/2014.
  - to indicate that the certificate is not to be considered as qualified:
    - "NotQualified" meaning the identified certificate(s) is(are) not to be considered as qualified; and/or
    - to indicate the nature of the SSCD support:
      - "QCWithSSCD" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have their private key residing in an SSCD, or
      - "QCNoSSCD" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have not their private key residing in an SSCD, or
      - "QCSSCDStatusAsInCert" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), does(do) contain proper machine processable information about whether or not

their private key residing in an SSCD;

- to indicate the nature of the QSCD support:
  - "QCWithQSCD" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have their private key residing in a QSCD, or
  - "QCNoQSCD" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have not their private key residing in a QSCD, or
  - "QCQSCDStatusAsInCert" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), does(do) contain proper machine processable information about whether or not their private key is residing in a QSCD;
  - "QCQSCDManagedOnBehalf" indicating that all certificates identified by the applicable list of criteria, when they are claimed or stated as qualified, have their private key is residing in a QSCD for which the generation and management of that private key is done by a qualified TSP on behalf of the entity whose identity is certified in the certificate; and/or
- to indicate issuance to Legal Person:
  - "QCForLegalPerson" meaning the identified certificate(s), when claimed or stated as qualified certificate(s), are issued to a Legal Person under Directive 1999/93/EC.
- Note: The information provided in the trusted list is to be considered as accurate meaning that:
  - if none of the id-etsi-qcs 1 statement, QCP OID or QCP + OID information is included in an end-entity certificate, and
  - if no "Sie" "Qualifications Extension" information is present for the trust anchor CA/QC corresponding service entry to qualify the certificate with a "QCStatement" qualifier, or
  - an "Sie" "Qualifications Extension" information is present for the trust anchor CA/QC corresponding service entry to qualify the certificate with a "NotQualified" qualifier,
  - then the certificate is not to be considered as qualified.

"Service digital identifiers" are to be used as Trust Anchors in the context of validating electronic signatures or seals for which signer's or seal creator's certificate is to be validated against TL information, hence only the public key and the associated subject name are needed as Trust Anchor information. When more than one certificate are representing the public key identifying the service, they are to be considered as Trust Anchor certificates conveying identical information with regard to the information strictly required as Trust Anchor information.

The general rule for interpretation of any other "Sti" type entry is that, for that "Sti" identified service type, the listed service named according to the "Service name" field value and uniquely identified by the "Service digital identity" field value has the current qualified or approval status according to the "Service current status" field value as from the date indicated in the "Current status starting date and time."



# Enforcement

## At a glance

- The ICO upholds information rights in the public interest.
- The ICO aim to help you comply with the law and promote good practice by offering advice and guidance.
- The ICO can take action if you breach the eIDAS Regulation, including the power to impose fines of £1,000.

## In brief

There are a number of tools available to the ICO for taking action to enforce eIDAS, set out in the [UK eIDAS](#) which are set out in the UK eIDAS Regulations and Data Protection Act 2018. They include non-criminal enforcement and audit. The ICO also has the power to serve a monetary penalty notice imposing a fine of £1,000.

The ICO may take enforcement action during the course of its supervisory responsibilities in respect of qualified trust services or in instances where there is evidence that any trust service provider based in the UK has not complied with the regulations.

These powers are not mutually exclusive. The ICO will use them in combination where justified by the circumstances. The ICO can:

- conduct an audit to check you are complying with your obligations as a trust service provider, and make recommendations;
- serve an Enforcement Notice order if there has been a breach, requiring an organisation to take specified steps to comply with the law;
- issue a Monetary Penalty Notice requiring you to pay £1,000;
- prosecute you if you fail to comply with an Enforcement Notice (except in Scotland, where the Procurator Fiscal brings prosecutions); and
- report to Parliament on issues of concern.

If you fail to comply with an ICO Enforcement Notice, an Assessment Notice (for a compulsory audit) or an Information Notice (requiring you to provide the ICO with information for our investigation) – the ICO also has the power to impose more substantial fines of up to £17.5 million, or 4% of your total worldwide annual turnover, whichever is higher.

For more information, see the ICO's regulatory action policy.

# Approved qualified trust service providers

We have granted the trust service providers listed with qualified status for one or more of their services.

## GMO Global Sign

GMO GlobalSign Ltd.

Springfield House

Sandling Road

Maidstone, Kent

ME14 2LP.

GMO GlobalSign Ltd is a qualified trust service provider for the provision of the following services:

- Qualified certificates for electronic signatures.
- Qualified certificates for electronic seals.
- Qualified certificates for website authentication.
- Qualified electronic time stamps.