This is a draft
Your feedback will help us improve it.

An introduction to the trust framework for identity and attributes

Digital identity is an important part of the UK's digital economy and society.

Anyone should be able to create a digital identity which they can use to do things securely online. A digital identity might also help someone with interactions or transactions in the real world, for example proving how old they are when they buy age-restricted goods.

Your organisation can use digital identities to help users do more things online and improve your existing services. Not using digital identities will mean people have to continue to interact and do things with your organisation through other channels, such as over the phone or by filling in a paper form. These can:

- be expensive
- be inefficient
- put people off completing the transaction
- put people and your organisation at risk of fraud

As well as being sure that someone is who they say they are, many organisations also need to know if someone is eligible to do certain things. They can do this by finding and checking additional information about someone (also known as 'attributes') along with, or separately from, their digital identity.

Our vision for digital identities and attributes

We want people to be able to create, use and reuse their digital identities with organisations across the public and private sectors. We also want them to be able to easily and securely share their attributes with other people and organisations.

This does not currently happen because one organisation cannot know or trust how another has created a digital identity or attribute. This means people often have to spend a lot of unnecessary time and effort proving their identity and eligibility whenever they want to do something new online.

Having a shared set of standards and rules will help organisations check identities and share attributes in a consistent way. A group of organisations might agree to follow the same rules and work together by joining a scheme.

The UK government supports a scheme which is managed by an independent authoritative body.

Becoming a trusted provider

You can choose to become any of the following trusted providers and supply products or services to other organisations in the scheme:

- identity provider
- attribute provider
- broker

You must be certified by an independent auditor to become a trusted provider. The auditor will make sure the products or services you supply were built to follow the necessary standards and rules.

You'll be given a trustmark when your organisation has been certified. This tells other organisations that you have met the necessary requirements to become a trusted provider.

Join the scheme

You can join the scheme as soon as you've been certified.

You can also join the scheme if you're a qualified trust service provider (QTSP). You must have been certified by a conformity assessment body before you can join.

You must follow the rules of the scheme. These explain how you should share digital identities and attributes with other organisations that are part of the scheme.

The authoritative body will manage the scheme and make sure organisations follow the rules at all times. If you do not follow these rules, you can be removed from the scheme.

Getting a scheme mark

You'll be given a scheme mark when your organisation joins the scheme. This tells users that they can reuse a digital identity they created with your service or product to do other things online.

Roles in the scheme

Your organisation will need to perform at least one role to be part of the scheme.

What your organisation needs to do to join the scheme will depend on which role you choose. If your organisation chooses to perform multiple roles, you must follow the rules for every role it does.

Buyers

Buyers are public or private sector organisations that:

- buy services or products from other organisations in the scheme
- build services that let users do things online

A buyer might need to make sure a user is who they say they are before giving them access to a service. To do this, the buyer might need to pay the identity provider to check and prove a user's identity.

A buyer might also need to check if a user is eligible to use their service. They can do this by requesting attributes, or information about attributes, from an attribute provider. The buyer might also need to pay a fee to do this.

A buyer must have the user's consent before they pass a user’s details on to an attribute provider.

Identity providers

Identity providers build products and services that let users create digital identities. Once a user has created a digital identity, they'll be able to do things online with any organisation that accepts digital identities from the scheme.

Identity providers will also need some information about the user before they can check their identity. An identity provider can:

- ask the user for this information and check it against information held by an attribute provider
- check any information they already have with an authoritative source (this could be an attribute provider)
- check if an attribute provider has this information already

Identity providers must have the user's consent before they do this.

Attribute providers

Attribute providers collect or create pieces of information that describe something about a user.

If an attribute provider collects an attribute from the user directly, they must check it belongs to the right person.

Attribute providers can share their attributes with identity providers and services.

Attribute providers must also describe the quality of the attributes they keep. Identity consumers and identity providers will use this information to choose which attribute provider they request attributes from.

Brokers

Brokers connect consumers to identity providers and attribute providers. They also give users a way to choose between identity providers.

The broker must make sure it protects users' privacy when their details are passed between a consumer and an identity provider or attribute provider.

How the roles work together

Buyers can connect to a broker if they want to:

- avoid maintaining separate connections to each identity provider in the scheme
- use an existing component that helps users pick an identity provider, instead of designing and building one

The broker can connect the buyer to:

- one or more identity providers, when the service needs a user to create a digital identity
- all identity providers, when the service needs to let users sign in with their digital identity
- an attribute provider, if the service needs to request attributes

Which broker a buyer chooses depends on:

- how much the broker will charge to get the information they need
- what type of attribute providers the broker has relationships with

Each broker must connect to every identity provider in the scheme. If the identity provider no longer follows the rules of the trust framework, they will no longer be trusted by the broker. This might mean the identity provider has to leave the scheme.

A broker can choose which attribute providers it connects to. An attribute provider can connect to multiple brokers.