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

Understanding, sharing and maintaining attributes

You should read this guidance if you collect or create attributes and want to become an 'attribute provider'. Attribute providers can share attributes they hold.

Anyone from any industry who collects or creates attributes can become an attribute provider.

This guidance will tell you:

- what attributes are
- what the benefits of sharing attributes are
- how to create (or 'enrol') attributes
- how to make sure your attributes are good quality

What are attributes

Attributes are pieces of information that describe something about a person, business or thing (such as a computer or device).

Attributes can be something that a person, business or thing has, like:

- the number of children someone has
- the number of people that work for a company
- a computer's operating system

These types of attributes will usually change over time, but some might not. For example, someone will not be able to change their natural eye colour and the date a company was founded will always stay the same.

Attributes can also be something that's issued to a person, business or thing by another organisation, like:

- someone's bank account number, which comes from their bank
- a UK company number, which comes from Companies House
- a computer's serial number, which comes from the manufacturer

It's usually difficult for anyone apart from the organisation that created and issued the attribute to make changes to it.

Sometimes an attribute can just confirm that a person, business or thing has something without giving away too much information about them. For example, an attribute could confirm that someone is over 18 but not reveal their date of birth.

The information about the attribute is captured in the attribute metadata. You can use the metadata to assess the strength of the attribute.

> For example, using the metadata to check the expiry date on a passport to make sure you can still use the facial biometric data.

The benefits of sharing attributes

Minimises user input by re-using attribute data across services

Sharing attributes reduces the time spent by the user entering and re-entering information and the time taken for the service to process this data.

Services can currently check this by asking a user to provide some information about themselves. This can sometimes be frustrating for the user and put them off using a service, especially if the user:

- has already provided the same information at an earlier point in the service
- cannot easily find or get the information they need

By sharing attributes across services, the user can minimise entering duplicate information multiple times.

> Example: If a user is over 60, attributes could be reused by the local authority to automatically calculate the user's eligibility for free public transport entitlement.

Reduces risk of using and relying on incorrect attributes

There's also a risk that the user could give the service the wrong information. This could happen by accident, for example if they spell something wrong. But a user might do this on purpose if they want to access a service they're not eligible to use.

A service can get more reliable information about a user by checking if it already exists as an attribute. The service will need to go to an attribute provider to do this. An attribute provider will then share an attribute, or information about an attribute, with the service.

> **Example**
> Some users can apply for a Blue Badge from their local council online. To do this, they might need to show proof they receive a particular benefit like Personal

Independence Payment (PIP). The local council will then need to check this information is correct with the Department for Work and Pensions (DWP).

Information about what benefits someone receives is an attribute. Some local councils have checked if a user is eligible for a Blue Badge by requesting this attribute from DWP, who are the attribute provider.

This has improved the user experience of the service, as it means users do not have to spend time finding the documents they need to prove their eligibility. It's also reduced the amount of time and effort the local council and DWP need to spend checking the user's eligibility.

Enables access to authoritative attribute data which reduces fraud

Through sharing attributes, services will have access to attribute data from authoritative sources which they might not otherwise have access to, for example HM Passport Office's passport numbers records. This means services using the data can be sure the attribute has been assured by an authoritative source and do not have to assure the data themselves.

When services share attribute data from authoritative sources, it means someone acting fraudulently will be more likely to be picked up because they will not have access to or be able to copy data from an authoritative source.

Enrolling an attribute

You 'enrol' an attribute when you first input it into a system, for example a database or a distributed ledger.

When you enrol an attribute, you must make sure it links to a person, business or thing by 'binding' it. Binding links a user to an attribute.

Binding an attribute

The binding process will vary depending on the service which is performing the binding and the process should involve confirming the correct person has been identified.

You can bind an attribute to a person, business or thing using:

- an identifier, for example linking an email address to a reference number when booking online
- a combination of identifiers, for example linking a name, date of birth and email address to a reference number when booking online

This link can either be:

- temporary, if the attribute is something that's likely to change, like a phone number
- permanent, if the attribute never changes, like the date someone started in their job

The strength of binding the attribute to a person, business or thing will vary depending on:

- whether there is a clear association between the user's account and the attribute
- the attribute's source
- the attribute to a particular level of assurance, depending on a range of circumstances
- the attribute's uniqueness and durability, for example hair colour is an attribute that is widely shared and can be easily changed which means the binding is weaker

The activity the service is using the attribute for will influence the strength of binding which is needed.

> For example, Blue Badge applications will need a higher strength of binding because they involve sensitive attribute data relating to the users' health. It's possible to reduce the strength of binding if you ask for confirmation that the applicant has an eligible health condition rather than needing the actual condition itself to be declared.

Chris comment: Include comment on the importance of metadata e.g. date of attribute enrolment

Assessing the quality of your attributes

Different services need different quality attributes, depending on what the service lets users do. Some services will be able to accept the risk of using lower quality attributes.

To find out the quality of an attribute, you should check:

- the quality of the source the attribute came from (for example a document)
- if the attribute is unique
- if you're able to match the attribute to the right record

Your attributes will be more valuable to services if they're higher quality.

You can also give your attributes a score. Higher quality attributes have a higher score. Services might use this score to choose an attribute provider or decide which attributes they request.

You do not have to score your attributes, but it's more likely services will request your attributes if you do.

Check the quality of the source the attribute came from

If the attribute does not originally come from your organisation, you can get it from another source, such as a document issued by another organisation. For example, a bank card could be a source that would give you any of these attributes:

- someone's name
- someone's bank card number
- someone's bank account number
- someone's bank's sort code

How much you can trust these attributes will depend on the quality of the source. To find this out, read the guidance about how to check if documents are genuine or valid.

Check the attribute is unique

An attribute is 'unique' if it's unlikely it will belong to more than one person, business or thing.

Score 1

You know the combination of the attribute and person, business or thing is not unique. For example, hair colour is not a unique attribute because a lot of people have the same hair colour.

Score 2

The combination of the attribute and the person, business or thing is unique within your data store for your attributes.

Score 3

7.3.1 The combination of the attribute and the person, business, or thing is unique within a defined industry, for example a collection of pension providers.

Score 4

7.4.1 There is only one combination of that attribute and person, business or thing in the world, for example a mobile phone number.

Check you can match the attribute to the right record

When a service wants to request an attribute (or information about an attribute) from you, it will send you some information they've collected about a user. If this matches the identifiers

you collected when you enrolled the attribute, you'll be more likely to find the right attribute in your database.

Score 1

You'll get a score of 1 if the identifier the service gives you has been 'self declared'. This means the user has given the service the information, but the service is not checking if it's accurate.

Score 2

You'll get a score of 2 if you have checked the attribute against a paper document, for example a bank statement or benefits letter

Score 3

You'll get a score of 3 if you have checked the attribute against a document with security features, for example a bank card or driver's license

Score 4

You'll get a score of 4 if you have checked the attribute against an authoritative source, for example checking a passport number against HM Passport Office (HMPO) records

Keeping your attributes up to date

Some attributes can change over time. These types of attributes are more likely to be accurate if you checked them recently. You should keep a record of when you last checked an attribute.

Services will be more likely to use your attributes if they're up to date. It's the service's responsibility to define a time period for when they will still trust an attribute to be accurate.

Note: Would it be useful to the user to have an overall scoring system similar to the identity profiles in GPG 45? If so, what should it look like?

Understanding consent when sharing attributes

You should consider consent when sharing attributes. There needs to be a lawful basis to share personal data and data subjects need to be told:

- when this information is collected
- how it will be processed

- why you will use their data
- the categories of organisations you may share user’s data with