GOV.UK

Policy paper

The UK digital identity and attributes trust framework

Published 11 February 2021

Contents

Print this page

This publication is available at https://www.gov.uk/government/publications/the-uk-digital-identity-and-attributes-trust-framework/the-uk-digital-identity-and-attributes-trust-framework

Ministerial foreword

Matt Warman MP, Minister for Digital Infrastructure

It has become increasingly important in this digital age to be able to establish trust, particularly online. This is the foundation thriving markets are built on. Having an agreed digital identity that you can use easily and universally will be the cornerstone of future economies.

There are times in day-to-day life when you may be asked to prove something about yourself to access a service or product. When buying alcohol you may need to prove you are over 18. When opening a bank account you need to certify who you are and where you live. When starting a new job you need to clear pre-employment screening.

This might be easy if you have a passport or driving licence and you are able to offer these face to face. At other times it can be difficult. You may not have recognised physical documents or may not be able to travel to prove you are who you say you are. Physical documents can also be stolen, falsified or misplaced. They can be expensive to replace and their loss can lead to identity theft and fraud.

This government is committed to solving these problems digitally and without the need for a national identity card.

In response to last year's Digital Identity Call for Evidence (https://www.gov.uk/government/consultations/digital-identity), we committed to:

- creating a clear framework of rules which show what 'good' digital identities look like — this will enable business to innovate, and help you to access products and services with ease, confident that there are standards in place to protect you from fraud and safeguard your privacy

- establishing a governance and oversight function to own these rules, keep them up to date, and make sure they are followed
- developing proposals to remove legislative and regulatory blockers to the use of secure digital identities and establish safeguards for citizens

This document, the first ‘working’ version of the UK digital identity and attributes trust framework, is an important step to meeting these commitments.

I want the trust framework to help facilitate a clear understanding between people using identity products, the organisations relying on the service and the service providers, letting each party know data is being used appropriately and kept safe.

Successfully combating fraud and cyber crime can only be achieved by government working with the private sector. This framework, which will need to be underpinned by further new robust legislative and regulatory mechanisms before it can be finalised, can help to strengthen how we work together to restrict opportunities for criminals and protect people.

The trust framework is being published now as a first stage industry prototype (or ‘alpha’) so that we can test it with services, industries, organisations and potential users. My department is taking this collaborative approach to make sure that when the final version is published it meets the needs of those who will rely on it.

Publishing an ‘alpha’ version allows these key stakeholders to continue to provide feedback as the document is iterated. It also gives service providers and relying parties early insight into the rules of the road and gives you, the user, confidence your digital identity and attributes will only be shared in a controlled and protected way. My department will actively seek feedback from across industry, civil society, other government departments, and the public sector over the coming months to develop the document further. All the trust framework joining requirements in the ‘alpha’ are subject to change in line with the feedback we receive.

The trust framework approach is gaining traction globally - Canada, Australia, Sweden and New Zealand are taking this route. We will continue to work with our international partners to make sure our standards are interoperable with those adopted abroad, so in the future you can use your digital identity around the world and UK businesses can trust digital identities created elsewhere.

It is not my department’s intention to provide any new or ready made solutions for actual products — we will be relying on the creative and innovative drive of industry to build these and the services that meet the needs of consumers from all walks of life. The trust framework is intended to set out the rules for these services, to provide the playing field on which business can operate. More detailed rules which are specific to their sector — what we call schemes — can develop within this framework.

The trust framework is also central to the Government Digital Service’s work with other government departments to develop a new cross-government single sign-on and identity assurance solution. This will ensure interoperability of identities and associated attributes between sectors in the longer term.

This document is just the beginning of building a trusted digital identity system for the UK. As detailed in the trust framework itself, we have further work to do on the governance structure to protect consumers and make sure the trust framework delivers on its intended benefits. We also need to clarify how liability is managed throughout the process. My department will underpin this structure in legislation and will consult privacy groups, industry and stakeholders in due course.

Our next steps on the trust framework are to incorporate feedback and publish a second iteration in short order. This updated version will contain the details for the certification process explaining how organisations can be assessed as meeting the requirements of the trust framework. These will allow

us to begin ‘sandbox style’ testing of the trust framework in partnership with sectors and organisations to ensure it meets their needs, while meeting our robust standards. Further details on plans for testing will be published alongside the next version.

We are excited to work together with industry, with civil society, and with you - the public - to iterate and improve the trust framework to make sure it works for everyone.

You can help us with this by reading this document and sending your feedback. Please provide your comments via the survey (https://dcms.eu.qualtrics.com/jfe/form/SV_4HZDsoOJSCWrV0q) by 12pm on Thursday 11 March 2021.

Matt Warman MP

Minister for Digital Infrastructure

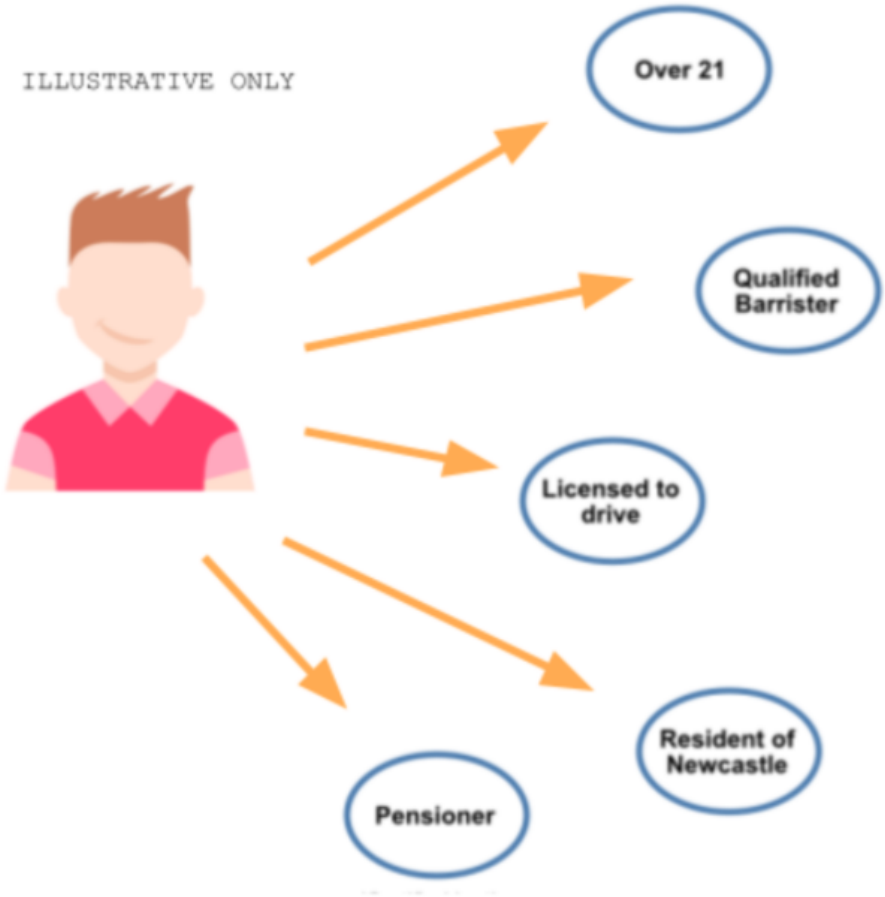
Background and context

What are digital identities and attributes?

A digital identity is a digital representation of who you are. It lets you prove who you are during interactions and transactions. You can use it online or in person.

Digital identities are not ID cards. We are not mandating how the market will develop digital identities, only that they are safe and secure.

One type of digital identity which could be developed under the trust framework is similar to a wallet, but created securely on your device. It lets you store various trusted pieces of information about yourself. We call these pieces of personal information “attributes” and you can choose when and with whom you share them — but probably never your whole ‘wallet’ of information. This could include disclosing details from the government – such as your legal name, date of birth, right to reside, to work, or to study — as well as details from other organisations, such as your professional qualifications, or employment history.



Another type of digital identity provides user authentication as an online service. When you need to prove your identity to a third organisation — for example, when you purchase age-restricted goods from an online retailer — you would securely sign in to your identity service provider and authorise them to release appropriate information to the organisation. Your service provider would then confirm to the organisation the information required — such as that you are over 18 — without releasing any more of your personal data.

Digital identities can place you in control of how much information you manage and share. They provide a better way of securing your personal data and they can prevent organisations obtaining information that you might prefer not to share with them.

In the same way that we use bank cards to authorise payment, digital identities will let us authorise the release of trusted information about ourselves.

Example

Sarah is in the queue for a nightclub and the door security guard asks for her ID. Instead of showing her passport, which contains lots of personal information, she instead uses her already created digital identity. She signs in on her phone using secure biometric authentication and shows the QR code to the security guard. The security guard can then scan this code, see it is a valid identity, and receive confirmation that Sarah is over 18 years old, without seeing any more details such as her date of birth or address.

Digital identities can also be used over the internet. They will remove the need to post documents to prove who you are, with all the risks of them being lost or stolen. Instead you will be able to use a digital identity to prove something about yourself — such as your name and address — when you are online.

You will also be able to use digital identities to ensure that the person or organisation you are dealing with is who they claim to be before releasing any of your information, making life much more difficult for scammers and other criminals.

Digital identity and attributes trust framework: what will it be and how will it help you?

A trust framework is a set of rules and standards which organisations agree to follow. If an organisation is part of the digital identity trust framework then you know they follow agreed requirements which safeguard your data and protect your privacy.

The UK digital identity and attributes trust framework sets out requirements so that organisations know what ‘good’ identity verification looks like. There are also rules for:

- making sure products and services are inclusive
- privacy and data protection
- fraud management
- security

We are publishing it as an ‘alpha’ (prototype) document to get feedback on whether the rules we’ve set out are the right ones for people, government, and industry.

By following these rules and standards, all organisations in the trust framework can be sure they work in a similar, trusted way. This means that, in future, if you were to create a digital identity it may be possible to use it in a variety of contexts — if you made a digital identity to open a bank account securely, you could use it to start a new job faster, or to rent a home without having to share all your personal identity data to your landlord or estate agent. Every step of the way, the aim is for you to be able to trust that each organisation is keeping your data safe, thanks to their adherence to the rules in the trust framework.

In the future you would be able to see if an organisation is part of the trust framework by looking for the trust mark. This would be a protected symbol which indicates the organisation follows the rules and has been checked and certified against these standards. The exact details of this process will be published as part of future guidance.

Example

Saanvi would like to open a bank account as well as rent a home. Instead of separately proving her identity to both the bank and estate agent, she decides to create a digital identity.

Saanvi finds an identity provider online. She sees the protected trust mark on their website, so knows the provider can be trusted with her data. She signs up with the identity provider and they create a digital identity, checking Saanvi’s identity documents and setting up a secure multi-factor authentication login for her.

Saanvi can then use this digital identity with a bank and an estate agent, without having to re-prove her identity. These organisations know they can trust the identity because it comes from a trusted identity provider who follows and has been certified against the trust framework.

The trust framework would be owned and run by a governing body established by the government. It will set the overarching procedures for joining the trust framework, and using its trust mark. The governing body will also make sure that organisations and schemes follow the rules, and decide what to do if they don't. The body will point you to sources of help for issues which can't be solved by trust framework members, and may get involved in redress cases.

You will have a choice over whether to create a digital identity or not. Our aim is for digital identities to be available for anyone who wants one, including those without traditional identity documents. The trust framework will set rules which facilitate services to be as inclusive as possible, for example by enabling partially offline solutions.

Example

Tom would like to apply for a loan. He doesn't own a passport or driving licence and he has limited digital skills.

Tom goes to his local library to ask for help. The library staff help him set up a digital identity by using a 'vouch' from his doctor to prove that Tom is who he says he is. The identity provider will contact Tom's doctor to confirm this.

Tom now has a digital identity that he can use to apply for a loan. The loan company will trust Tom's identity because his identity provider is part of the trust framework.

1. Introduction

This 'alpha' (prototype) of the UK digital identity and attributes trust framework is for organisations that want to provide or consume digital identity and attribute products and services. The Department for Digital, Culture, Media and Sport (DCMS) is looking for feedback from these organisations as well as other interested parties, such as civil society groups and academia.

This document explains what requirements organisations will need to meet to be certified against the trust framework in the future. These requirements will be updated after all of the feedback has been analysed.

Organisations must meet these requirements alongside the rules of any other contracts, policies or legislation that they already follow.

This document does not explain:

- what requirements (or 'certification profiles') organisations will be certified against - these will be published later this year following the first round of feedback
- what legislative or governance arrangements are needed to make sure the trust framework is ready for use in the economy

There are still some elements missing from this document. Based on feedback we've already received, we're now working on guidance about:

- limitations on liability (including unlimited liability, limited liability and excluded losses)

- how a trust mark might be used (including how it might be supported technically)
- encryption, public key infrastructure (PKI) and digital signatures
- digital identity and data portability
- how delegated authority can work in practice
- interoperability (including a recommended technical specification) ~* attributes metadata

Please fill in the feedback survey (https://dcms.eu.qualtrics.com/jfe/form/SV_4HZDsoOJSCWrV0q) to give us your comments by midday on Thursday 11 March 2021.

Terms and definitions

Whenever ‘you’ is used in this document, it refers to organisations that want to use the trust framework.

We use ‘user’ to refer to people who will use digital identity or attribute products and services to prove their identity or eligibility.

The word ‘must’ is used for any requirements that organisations have to prove they’ve met. The certification profiles will explain how they do this.

The word ‘should’ is used when it’s only recommended that organisations meet a requirement.

Read the glossary (https://www.gov.uk/government/publications/the-uk-digital-identity-and-attributes-trust-framework/the-uk-digital-identity-and-attributes-trust-framework#glossary-of-terms-and-definitions) for a full list of terms and definitions.

1.1 What are digital identities

A digital identity is a digital representation of a person. It enables them to prove who they are during interactions and transactions. They can use it online or in person. Organisations that let users use secure digital identities during interactions and transactions can trust that those users are who they say they are.

A digital identity is not the same as a user account or a ‘single sign on’, although a user might need to prove their identity to get one of these. A digital identity can only be created for a real person, who has evidence that shows they exist and are who they say they are.

Anyone can choose to create a digital identity. They do not have to do this.

Sometimes digital identities will be created for just one type of transaction. A user might create different digital identities to complete different interactions and transactions.

Example

Cliff needs to prove his identity to apply for a loan online. Doing this creates a digital identity.

Cliff can only use this digital identity to complete his application and open an account. He cannot use it to do anything else.

Other digital identities will be ‘reusable’, which means they can be used again and again for different interactions and transactions.

Example

Peggy is buying her first home. She creates a digital identity when she checks her credit score online with a credit scoring agency. The credit scoring agency is a member of a scheme in the trust framework.

Peggy decides to apply for a mortgage from a bank. The bank is also a member of a scheme in the trust framework. This means she can use her digital identity again to apply for the mortgage.

Peggy will need to prove who she is several times throughout the process of buying a house, for example when she interacts with the bank, estate agents and solicitors. If any of these interactions happen in real life, Peggy can show her digital identity on an app on her phone.

Using digital identities will mean users do not have to rely on offline channels (such as by post or over the phone) to interact with organisations or access services. Making these sorts of interactions and transactions available online can also:

- save organisations time and money
- reduce the risk of fraud to organisations and users
- be easier and quicker for users to complete
- reduce of the risk of errors that come from managing data manually
- encourage innovation by helping organisations develop more services

This government is committed to delivering these benefits digitally and without the need for a national identity card.

Social distancing caused by the coronavirus (COVID-19) pandemic has meant there are fewer opportunities for users to do things in person. This means it can be safer, as well as easier, for users to complete some interactions and transactions online.

1.2 What are attributes

Attributes are pieces of information that describe something about a person or an organisation. You can use a combination of attributes to create a digital identity. You must ‘bind’ an attribute to a person before you can do this.

An attribute could be something:

- a person or an organisation is
- a person or an organisation has
- that’s issued to a person or an organisation

Attributes could be related to:

- physical or digital documents such as a bank statement
- devices such as a mobile phone

- credentials such as a university degree
- someone’s health condition

Some examples of attributes are:

- the number of children someone has
- someone’s bank account number
- someone’s National Insurance number
- someone’s NHS number
- the number of people that work for a company
- a Companies House company number
- that someone is over 18

Attributes are not only used to create digital identities. They can also help prove a user is eligible or entitled to do something. In some situations, this proof can be added to an existing digital identity. In others, there will be no need for you to know the identity of the user before they can complete an interaction or transaction.

An organisation can check attributes against the eligibility criteria someone must meet to be able to complete an interaction or transaction:

Example

Carmen needs to travel to Ghana for work. She must prove that she’s had a yellow fever vaccination before she can enter the country.

Carmen will get an International Certificate of Vaccination or Prophylaxis (ICVP) that confirms she’s had the vaccination. Whoever gave Carmen the vaccine can add the information from this certificate as attributes to Carmen’s personal data store app (sometimes known as a ‘digital wallet’).

This attribute can be shared with the Ghana Immigration Service before Carmen arrives in the country. This will mean she has to take fewer documents with her when she travels and will spend less time at the border.

Attributes are created, collected and checked by an attribute service provider. An attribute service provider could be an organisation or a piece of software, like a digital wallet. Attribute service providers can share the attributes they keep with other organisations or individuals, as long as they have the user’s agreement.

Sharing attributes means:

- users can share information about themselves to access services more easily
- users and organisations do not have to update information in more than one place whenever something changes

1.3 What the UK digital identity and attributes trust framework does

The UK digital identity and attributes trust framework will let people use and reuse their digital identities. It will also give them a way to share their attributes with other people and organisations more easily.

One reason why this does not currently happen is because one organisation does not know how another creates digital identities or attributes. This means they're not able to trust if the processes the other organisation followed are secure.

The trust framework is a set of rules that different organisations agree to follow. This includes legislation, standards, Good Practice Guides (GPGs) and the requirements in this document. By following these rules, all organisations using the trust framework can describe digital identities and attributes they've created in a consistent way. This should make it easier for organisations and users to complete interactions and transactions or share information with other trust framework participants.

The trust framework is central to the Government Digital Service's work with other departments to develop a new secure system that will make it easier to prove who you are online to access government services. This will also support our longer-term goal of using digital identities flexibly between different sectors of the economy.

Rules of the trust framework

UK digital identity and attributes trust framework participants will be certified against a set of government-approved rules. This means that one organisation can trust that the information another shares with them is accurate and reliable.

To meet the rules of the trust framework, you will need to prove you're able to safely manage users digital identities or attributes. The rules will be 'outcome based'. By following them, you will achieve certain goals. The rules will not instruct you to use specific technologies or processes, but will recommend you follow open technical standards to strengthen interoperability between participants. This means you will be able to focus on innovating and developing products and services that work best for your users, without being restricted to using certain technologies.

1.4 What you get from being part of the trust framework

Being part of the UK digital identity and attributes trust framework will help your organisation:

- save time, effort and money
- improve the user experience of your existing services
- develop new services, which can create new revenue streams
- deal with data breaches and identity fraud
- show that you're committed to creating trustworthy and secure products and services
- share digital identities and attributes with other organisations from a variety of countries, industries and sectors

1.5 Benefits for users

Being able to share their digital identities and attributes with different organisations will make it easier for users to complete interactions and transactions digitally. This is because it will be much quicker to prove their identity and eligibility when they interact with a new organisation. The UK government plans to make it possible for this to happen across different industries, sectors and countries where it's safe and legal to do so.

The trust framework will include data protection requirements, which you must follow when developing and managing your products and services. These rules are designed to give users more control over what personal information they use to create a digital identity. You must also follow rules to develop accessible and inclusive products and services. These rules are designed to allow as many users as possible to create digital identities and manage their attributes.

In most circumstances, users will be able to choose which organisations can see and share their personal data, and how long they will have access to it for. They will not have a choice in specific situations, for example if they're the subject of a police investigation. They'll also know exactly who is involved in creating and maintaining their digital identity.

There will also be more opportunities for 'data minimisation'. This is when information is only shared if it's needed to give a user access to a service. For example, when buying age-restricted products, a retailer only needs to know that a user is over a certain age. They do not need to see the rest of the information on their identity document. Making sure personal information is shared and managed securely will put users and organisations at a lower risk of identity fraud.

1.6 Who runs the trust framework

The trust framework will be overseen by a governing body chosen by the UK government. The governing body will work with other bodies and organisations to make sure that using the trust framework is as straightforward as possible.

The governing body could be responsible for:

- deciding what rules and standards trust framework participants need to follow
- keeping rules and standards up to date
- making sure all participants follow the rules and standards
- deciding how to deal with any participants that do not follow the rules and standards
- deciding how to onboard, suspend, remove and reinstate participants
- deciding what operational guidance participants need to follow
- approving the creation of schemes and maintain oversight of them through the scheme operator
- system level security and fraud, including sharing information and early warnings about anything that could affect the security of the trust framework or its participants
- deciding how complaints from users will be handled
- encouraging participants to make their products and services as inclusive as possible
- working with regulators and international bodies
- creating and issuing a trustmark
- publishing who is approved to use the trust framework

1.6 Who can use the trust framework

Organisations can use the UK digital identity and attributes trust framework:

- by themselves as a single organisation
- as part of a 'scheme'

A scheme is made up of different organisations who agree to follow a specific set of rules around the use of digital identities and attributes. These organisations might work in the same sector, industry or region, which means they will build products and services for similar types of users. A scheme can

help organisations work together more effectively by making it easier for them to share information. They can do this by adding additional requirements to the rules of the trust framework.

Example

An estate agent might want to find out the best way to check identities of potential house buyers. They can join a scheme with other organisations that play a role in the house buying process.

Being part of the scheme will mean they have access to operational, technical and commercial guidance that's specific to their industry. This is more detailed than the requirements of the trust framework.

Some relevant schemes already exist or are being developed, while others could be developed in the future.

A scheme is created and run by a scheme operator. The scheme operator must follow the rules of the trust framework.

The scheme operator must not do anything that stops digital identities or attributes from being shared between members of the trust framework.

The scheme operator sets the rules of the scheme. This is known as a 'scheme specification' and must be based on the rules of the trust framework. It could include:

- what roles are available in the scheme
- how members should work together
- how members should process data about their users
- how members can work to create interoperability between schemes

The scheme operator is responsible for making sure all members follow the scheme specification. They will also be responsible for:

- keeping an up-to-date list of all organisations that are part of their scheme, which they will share with the governing body
- explaining how the scheme has been certified

They can also give members guidance and support on how to build products and services that are optimised for their users. They might choose to share this information with other scheme operators that are part of the trust framework.

Roles and responsibilities

Whether an organisation uses the trust framework on their own or as part of a scheme, they will need to perform at least one of the following roles, as set out in the paragraphs below:

- an **identity service provider**
- an **attribute service provider**
- an **orchestration service provider**
- a **relying party**

What your organisation needs to do to be certified against the trust framework will depend on which role you choose. If your organisation chooses to perform multiple roles, you must meet the legal, technical and policy requirements for each role.

Your organisation must be ‘certified’ before you can use the UK digital identity trust framework. To be certified, an independent certifying body will need to check that you meet all the requirements for the role you want to perform. You’ll get a trust mark after you’ve been certified and approved. This will:

- show other organisations that you meet the requirements
- help users feel more confident about using your product or service

Identity service providers

Identity service providers prove and verify users’ identities. They can do this using online or offline channels, or a combination of both. An identity service provider can be a public or private sector organisation. They can either:

- specialise in proving and verifying users’ identities
- offer identity proving and verification alongside other services - an example of this might be a bank, solicitor, library or postal organisation

An identity service provider might not need to do all parts of the identity checking process. They can specialise in designing and building components that can be used during a specific part of the process. For example, they could develop software that checks if identity evidence is genuine and valid.

Identity service providers can be authorised by a user to share the verified digital identity with relying parties. The relying party can then use this to give them access to the service or create an account. Other identity service providers might choose to create an account associated with a user’s identity. The user can then use and reuse this account to do different things with different relying parties.

Digital identities and attributes can only be associated with a digital account with the user’s agreement. There are no limits to the number of accounts a user can create, although organisations and schemes may set their own limits for security reasons.

Attribute service providers

Attribute service providers collect, create, check or share pieces of information that describe something about a user. Attribute service providers can share their attributes with relying parties and identity service providers, if they have the user’s agreement.

If an identity service provider is collecting, creating, checking or sharing attributes as part of their service, they will also be an attribute service provider. They will need to meet the requirements of both roles.

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

Orchestration service providers

Orchestration service providers make sure data can be securely shared between identity or attribute service providers and relying parties. Some examples of orchestration service providers include brokers and distributed ledger services.

Relying parties

Relying parties are organisations that get (or ‘consume’) products or services from other participants in the trust framework. This means that organisations such as airlines, banks and retailers do not have to check users’ identities or attributes themselves.

A relying party might need to make sure a user is who they say they are before letting them do something. To do this, the relying party can ask an identity service provider to prove a user’s identity. A relying party might also need to check if a user is eligible to do something. They can do this by requesting attributes, or information about attributes, from an attribute service provider.

2. Rules for identity service providers

Identity service providers must follow these as well as the rules for all trust framework participants (https://draft-origin.publishing.service.gov.uk/government/publications/the-uk-digital-identity-and-attributes-trust-framework/the-uk-digital-identity-and-attributes-trust-framework#rules-for-all-trust-framework-participants).

2.1 Create a digital identity

All identity service providers must follow the guidance on how to prove and verify someone’s identity (https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual). This is also known as Good Practice Guide (GPG) 45. You might not need to follow the whole guidance. Which parts of the identity checking process you need to do will depend on what your product or service does.

Create a reusable digital identity

If you are an identity service provider who wants to create a reusable digital identity, you must link the digital identity to an ‘authenticator’ (such as a password, piece of software or device). You must follow the guidance on using authenticators to protect an online service (https://www.gov.uk/government/publications/authentication-credentials-for-online-government-services/giving-users-access-to-online-services). This is also known as GPG 44.

If someone has already created an account to use another service you provide, you might be able to add a digital identity to it. For example:

- a bank could reuse a user’s details from when they signed up to online banking to help them create a digital identity
- a qualified trust service provider could use an existing electronic signature to create a digital identity for a user

You must get the user’s permission before you do this.

2.2 Manage digital identity accounts

You must manage any digital identity accounts users choose to create with your organisation. This means you’ll need a way to suspend, close, recover and make changes to accounts.

You can close an account if the user:

- has used the account to do something illegal
- has not followed the terms of use they agreed to
- wants to close it

- has died

You must also close the account if you have evidence it's being used by someone who should not have access to it. This usually happens because there's been a data breach (see section 5.11).

You must 'suspend' the account before you close it. The user will not be able to use their digital identity during this time. Suspending an account gives users the chance to recover the account if:

- they change their minds about closing it
- someone else accessed their account and closed it

You might need to suspend an account if:

- the account has been inactive for a period of time
- suspicious activity has been detected relating to the account
- you have been told the user has died

Recover digital identity accounts

You must take a user through an account recovery process if you suspect someone who should not have access to the account has either:

- signed in to their account
- used their digital identity or attributes to do something

You must let the user know what's happened. It's important to explain that they could be at risk of having their identity stolen.

You must ask the user to look at their recent account activity and check if there are any interactions they did not do. If it looks like someone other than the user has used the account, you must continue the account recovery process.

You must prove and verify the user's identity (https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual/identity-proofing-and-verification-of-an-individual) again. You should aim to get a higher level of confidence than you did when you first set up the digital identity account. This will help you be sure that the user is not an impostor.

The impostor might have already used information about the user to create other accounts or do other things. If this happens, you must have a way to:

- close down any accounts the impostor created with your organisation
- give the user information about any interactions or transactions the impostor completed using these accounts
- give the governing body or law enforcement agencies information about the impostor and the things they did

If a user makes changes to their digital identity

You must tell the user if any changes have been made to their digital identity. You must also tell them if you've had a request to close their digital identity account.

Avoid sending notifications to the user through your product or service unless it can only be accessed on a device that you know belongs to that user.

You should use a different channel to contact the user if you can, for example by phone, post or email. You should do this using contact details that you know belong to the person who created the digital identity.

If the user wants to change their contact details, you must do a ‘verification’ check (https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual/identity-proofing-and-verification-of-an-individual#verification) to make sure they’re the same person who created the digital identity. You will need to get at least the same score you currently have.

2.3 Make sure your products and services are inclusive

Making your products and services inclusive means everyone can use them no matter who they are or where they’re from. One of the aims of the trust framework is to make it as easy as possible for users to create and use digital identities (either online or in person).

All identity service providers must follow the Equality Act 2010 (https://www.legislation.gov.uk/ukpga/2010/15/section/4) by considering how to make sure no one is excluded from doing this because of their ‘protected characteristics’. There are notable exceptions to this, such as it being fair to restrict service access on account of someone’s age, e.g. you cannot buy certain products until you are 18.

There are many reasons why a user may be excluded from using a product or service. One common reason is because users are asked to provide specific evidence as proof of their identity.

Example

A service that only accepts a UK passport as proof of someone’s identity will exclude users who do not have, cannot find or cannot afford a passport.

You can prevent this happening by accepting a wide variety of evidence as proof of users’ identities and eligibility. You can also choose to accept a declaration from someone that knows the user (https://www.gov.uk/government/publications/how-to-accept-a-vouch-as-evidence-of-someones-identity) (known as a ‘vouch’) as evidence.

Requiring information to be checked against certain authoritative sources can also exclude some users from creating a digital identity.

Example

A service that only checks users’ information against a credit reference agency database will stop users who do not have much of a credit history from creating a digital identity. This could exclude users because of their age or income.

You can prevent this from happening by checking information about users against a wider range of sources.

Another reason why you might exclude users is if a product or service uses any third party software that’s only been tested with a specific user group.

Example

A service might check users' identities using an existing facial recognition system that was tested with a small sample of users. As most of these users were white men, the system was not taught how to recognise users of other genders or ethnicities.

By choosing this system, the service will exclude some users from proving their identity because of the way they look.

You can prevent this from happening by choosing software that you know has been tested with a variety of users from different demographics.

The first step to building an inclusive product or service is to find out as much as you can about the types of people who will use it. If you do not know who they are or what they need, you cannot be sure you have built the right product or service.

You must make sure that making your product or service more inclusive will not expose it or your users to any additional risks.

Submit an annual exclusion report

All identity service providers must submit an exclusion report to the governing body every year. The governing body will tell you exactly what information should go in the report. It will at a minimum need to say which demographics have been, or are likely to be, excluded from using your product or service. You must explain why this has happened or could happen.

Sometimes users will be excluded for a good reason. For example, users under 18 should not be able to create a digital identity to access a gambling website so it would be right to stop them from doing this. You must explain if this has happened in the report.

You must write the report based on evidence, for example findings from user research or data and analytics for your product or service. You do not need to collect any additional personal information from your users.

You must also explain what you'll do to improve the inclusion of your product or service in the report.

2.4 Make sure your products and services are accessible

You must follow the accessibility regulations (https://www.gov.uk/guidance/accessibility-requirements-for-public-sector-websites-and-apps) if you're a public sector organisation that's developing apps or websites. This includes any products or services that help users create digital identities or manage their attributes.

If you're a public sector organisation that develops products or services for users in Wales, you must also follow the Welsh Language Act 1993 (https://www.legislation.gov.uk/ukpga/1993/38/contents). This means your product or service must be available in Welsh.

You should also aim to develop products and services that everyone can use if you're not a public sector organisation. To help do this, we suggest you follow the:

- Web Content Accessibility Guidelines (https://www.w3.org/WAI/standards-guidelines/wcag/) (WCAG)

- new European Telecommunication Standards Institute (ETSI) standard on accessibility requirements suitable for public procurement of ICT products and services in Europe (https://www.etsi.org/newsroom/news/754-new-european-standard-on-accessibility-requirements-for-public-procurement-of-ict-products-and-services)

You should always make sure users have more than one way to use your product or service. For example, a user should have another way to create a digital identity if they're unable to use the online service.

Retiring your product or service

If you decide to retire your product or service, you must notify:

- any users who have created a digital identity with you
- relying parties that consume your digital identities
- the scheme operator (or the governing body, if you're not part of a scheme)

3. Rules for attribute service providers

Attribute service providers must follow these as well as the rules for all trust framework participants.

3.1 Create attributes

You must follow the guidance on how to create attributes (https://www.gov.uk/government/publications/attributes-in-the-uk-digital-identity-and-attributes-trust-framework).

You must:

- create the new attribute in an appropriate way
- bind it to a person or organisation
- score it to show how reliable and secure it is

All attribute service providers must link their attributes to a person or organisation using a process called 'binding'. This involves using another piece of information (sometimes called an 'identifier') to make a connection between an attribute and a person or organisation.

Example

When someone starts a new job they're given a unique employee number, which is an identifying attribute. This links the person with their job title (another attribute).

The HR department uses the identifying attribute to link the employee's other attributes to the employee. Their other attributes include their salary and how many hours they work a week.

For example, one office has 2 employees named Daniel Jones. When the HR department gets a phone call from one of them, the HR representative asks for their employee number. This helps them know which Daniel Jones they're talking to.

If you do not bind your attributes, other organisations will not be able to tell who they belong to. This will make them harder to use and less valuable.

Sharing attributes

Before you share an attribute, you must check:

- when the attribute was last updated
- you'll share it in a way that meets the privacy and data protection requirements (see section 5.13.)
- if the person or organisation requesting it has the right to see it

You can then share it in an appropriate way.

3.2 Scoring attributes

You must follow the guidance on how to score attributes (https://www.gov.uk/government/publications/attributes-in-the-uk-digital-identity-and-attributes-trust-framework).

Relying parties can use the scores to decide which attributes meet their needs. Scores should be recorded in the attribute's metadata. When you assign the scores, you will:

- check if the attribute is in the right format
- show how reliable the attribute is
- show how you've bound the attribute
- show how you've matched the attribute

3.3 Make sure your products and services are accessible

You must follow the accessibility regulations (https://www.gov.uk/guidance/accessibility-requirements-for-public-sector-websites-and-apps) if you're a public sector organisation developing apps or websites. This includes any products or services that help users create digital identities or manage their attributes.

If you're a public sector organisation that develops products or services for users in Wales, you must also follow the Welsh Language Act 1993 (https://www.legislation.gov.uk/ukpga/1993/38/contents). This means that your product or service must be available in Welsh.

You should also aim to develop products and services that everyone can use if you're not a public sector organisation. To help do this, we suggest you follow the:

- Web Content Accessibility Guidelines (https://www.w3.org/WAI/standards-guidelines/wcag/) (WCAG)
- new European Telecommunication Standards Institute (ETSI) standard on accessibility requirements suitable for public procurement of ICT products and services in Europe (https://www.etsi.org/newsroom/news/754-new-european-standard-on-accessibility-requirements-for-public-procurement-of-ict-products-and-services)

You should always make sure users have more than one way to use your product or service. For example, a user should have another way to create a digital identity if they're unable to use the online service.

3.4 Retiring your product or service

If you decide to retire your product or service, you must notify:

- any users that manage their attributes with your product or service
- any relying parties that consume attributes you've created
- the scheme operator (or the governing body, if you're not part of a scheme)

You must also decide how you will manage user's requests for 'data portability (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/)', which allows users to obtain and reuse their personal data for their own purposes across different services. Data portability requests may be more likely to occur when a product or service is being retired.

4. Rules for orchestration service providers and relying parties

There are no specific rules that orchestration service providers and relying parties need to follow. They should follow the rules for all trust framework participants (https://draft-origin.publishing.service.gov.uk/government/publications/the-uk-digital-identity-and-attributes-trust-framework/the-uk-digital-identity-and-attributes-trust-framework#rules-for-all-trust-framework-participants).

5. Rules for all trust framework participants

Anyone that wants to be part of the trust framework must meet these rules.

You must follow these alongside the rules of any other contracts, policies or legislation that you already follow.

5.1 Making your products and services interoperable with others

Future iterations of the trust framework will recommend technical specifications to encourage interoperability between organisations and schemes, in the UK and internationally. This means it will be easier for organisations and schemes to share digital identities and attributes with each other, as well as supporting mutual recognition.

The specifications should be followed by:

- all attribute service providers
- any identity service providers that create reusable digital identities
- all relying parties

You must be able to validate you are receiving messages from an approved organisation or scheme. You could do this by:

- having a database of approved providers or schemes
- running public key infrastructure (PKI)
- using a distributed ledger technology (DLT) model

How digital identities and attributes will be shared

Each organisation or scheme will need to provide enough information for another to be able to:

- identify the person
- decide if the person or business is eligible for something

If the digital identity or attributes belong to a person, the organisation or scheme might need to be able to provide:

- their date of birth
- their first name
- their last name
- a unique identifier, such as a user or account number

To check if a person is eligible to do something, a relying party might also ask an organisation or scheme for more information. This could include their:

- nationality
- place of birth
- name at birth
- email address
- address
- phone number
- gender
- occupation
- income
- citizen registration number (for people resident outside the UK or non-UK nationals)
- tax reference number
- biometric information
- passport number
- non-UK identity card number
- role in an organisation

An organisation or scheme should meet the privacy and data protection requirements (see section 5.13) when sharing this information.

The relying party will need to decide if the information is accurate enough for what they need. Knowing where the attribute comes from and how it has been checked could help them make this decision.

If the digital identity and attributes are linked to a UK or international business, the scheme must provide:

- its legal name
- a registered identifier, such as a Companies House number

To check if a business is eligible to do something, a relying party might also ask an organisation or scheme for more information. This could include:

- any email addresses associated with the business
- any addresses associated with the business
- the country of its incorporation
- its VAT number
- its turnover
- its Legal Entity Identifier (LEI)

- its Standard Industrial Classification (SIC) code
- its Economic Operators Registration and Identification (EORI) number
- its Excise Authorisation Verification (SEED) number
- its Data Universal Numbering System (DUNS) number
- its data protection registration number

An organisation or scheme should not share this information for any other purpose, unless they have a good reason to do so.

5.2 Check if a user can act on behalf of someone else

Be aware that some users might be acting on behalf of someone else when they interact with your organisation. This is known as ‘delegated authority’.

The user might have a formal agreement with the other person to complete interactions or transactions for them. For example, the user might have been appointed using a lasting power of attorney (LPA) to look after someone else’s money and property.

A user will only have delegated authority if they have been given permission to make decisions and complete tasks on behalf of the other person. A user does not have delegated authority if they’re helping someone do something. This could include:

- a user helping a friend who’s not confident using a computer to fill in an online form
- anyone who offers ‘assisted digital support’ to users of a product or service

You should check if the user has authority to act on someone’s behalf. The details of their agreement with the other person might exist as an attribute.

5.3 Respond to complaints and disputes

You must have a process for dealing with complaints and disputes. Disputes could involve your users or other trust framework participants.

5.4 Staff and resources

Your organisation must have a way to:

- make sure your staff (including contractors) have the right experience, training or qualifications needed to do their job
- do background checks on your staff
- make sure any personal, cryptographic or sensitive information you keep can only be accessed by authorised staff

5.5 Encryption

You must follow industry standards and best practice for encryption and cryptographic techniques. These could be the following National Institute of Standards and Technology (NIST) standards:

- FIPS 140-3 (https://csrc.nist.gov/publications/detail/fips/140/3/final)
- SP 800-175B (https://csrc.nist.gov/publications/detail/sp/800-175b/rev-1/final)
- SP 800-67 (https://csrc.nist.gov/publications/detail/sp/800-67/rev-2/final)

You should also follow current Digital Signature Standards (DSS), such as either:

- FIPS 186-5 (https://csrc.nist.gov/publications/detail/fips/186/5/draft)
- ETSI TS 119 312 (https://www.etsi.org/deliver/etsi_ts/119300_119399/119312/01.02.01_60/ts_119312v010201p.pdf) (opens as a PDF)

For guidance on hash functions, you can read the following NIST standards:

- FIPS 180-4 (https://csrc.nist.gov/publications/detail/fips/140/3/final)
- FIPS 202 (https://csrc.nist.gov/publications/detail/fips/202/final)
- NIST SP 800-107 (https://csrc.nist.gov/publications/detail/sp/800-107/rev-1/final)

You should also follow National Cyber Security Centre (NCSC) guidance on:

- using IPsec to protect data (https://www.ncsc.gov.uk/guidance/using-ipsec-protect-data)
- using TLS to protect data (https://www.ncsc.gov.uk/guidance/tls-external-facing-services)

You must follow the latest version of these standards.

You must also have:

- an encryption and cryptographic controls policy document
- a communications security (COMSEC) reporting policy that explains how you'll respond to any suspected or actual attacks

5.6 Quality management

You must have a quality management system (QMS) that follows a recognised industry standard, such as ISO 9001:2015 (https://www.iso.org/standard/62085.html). A QMS is a collection of documents that describe your organisation's objectives and explain how it will achieve them. These objectives could be about:

- your processes, for example you might aim to investigate and fix all faults within 2 hours
- your staff, for example you might want to make sure every member of staff completes 5 hours of security training every month

Your QMS will need to include information such as:

- who in your organisation is responsible for meeting the objectives
- what standards you will follow
- how you'll measure how well you've met your objectives
- what tools, funding, people and other resources you need
- how you'll plan to improve the quality of your products or services on an ongoing basis (known as 'continuous improvement')

5.7 Information management

Your organisation must have an information management system that follows an industry standard, such as ISO/IEC 27001:2017 (https://www.iso.org/isoiec-27001-information-security.html).

An information management system is a collection of documents that will need to explain:

- why your organisation needs to keep information it keeps
- how you create, organise and store information
- who has access to the information
- how you share information (including why it's shared, who it's shared with, how often it's shared, what format it's in and how it's protected)
- how you archive information

Archiving information

Your organisation must have have an archiving policy that:

- follows any legislation or regulations that your organisation needs to follow
- meets any requirements that an auditor has decided your organisation needs to meet
- follows any standards or best practice relevant to the industry or sector your organisation is part of

It must also explain:

- how archived information is used to support your organisation's work
- why your organisation needs continued access to archived information
- what are the risks of not having access to archived information
- how archiving information protects the interests and legal rights of your organisation and others you work with
- the relationship between this information and any other records, data or evidence you keep

Disposal schedule

You must have a disposal schedule that records how you manage and delete information. It should show:

- that your organisation meets any legislation or regulations about keeping and deleting information
- what information was created but later deleted
- what format the information is in (for example if it was physical or digital)
- where information is located
- how information is transferred for disposal, if this is relevant

Data management

You must have a data management policy that explains how you create, obtain, transform, share, protect, document and preserve data. It should include:

- file naming conventions
- how you create metadata

- how your organisation makes sure data is available when it's needed
- how you know data is accurate and complete
- how you maintain and secure your data

Your data management policy must cover the full data lifecycle. It should explain how architectures, policies, practices and procedures are implemented and maintained.

5.8 Information security

Your organisation must have an information management system that follows an industry standard, such as ISO/IEC 27001:2017 (https://www.iso.org/isoiec-27001-information-security.html). It must be based on the principles of:

- confidentiality
- integrity
- availability

You'll also need a number of security documents to support your information security policy. These include:

- technical controls
- organisational controls
- physical security controls

Confidentiality

You must make sure any information your organisation keeps can only be accessed by authorised users. For example, you could make it so users need an authenticator (such as a password) to access the information.

You could also use an access-control list or role-based access control to protect your organisation's information. These must specify:

- which users or systems can access your information
- how they are granted access
- what they can do with your information

This should be explained in your organisation's password control policy or access control policy.

Integrity

You must be able to show that you've done everything you can to maintain the integrity of any information your organisation holds. You might need to prove this for legal reasons, for example if you suffer a breach. Your organisation must have an information security policy that explains how you will:

- stop information from being modified, either by accident or on purpose (including how you'll protect it against malicious acts)
- keep information in its 'correct state' - the format or reason for collecting the information should not change
- restore information to its correct state if you suspect it's been tampered with

Availability

You must make sure that any information your organisation keeps is available to those that need it.

You will need:

- tools and processes that can cope with the amount of requests you expect to get
- a backup policy, in case you need to recover any information

You should explain how these work in your:

- data support and operations plan
- policy and business continuity plan
- disaster recovery plan
- information security policy

Technical controls

You must have a document that explains what hardware and software your organisation uses to protect information, such as firewalls, intrusion detection systems and encryption techniques. It should also explain what software you use to monitor and control access to information.

Organisational controls

You must have a document that explains how your organisation will continue to meet security requirements. For example, it could explain what information security training your staff will regularly have to complete. It should also explain what roles are in your organisation and what parts of the information security process they're responsible for.

Physical security controls

You must have a document that explains what security controls protect the physical locations where the following things are kept:

- any information your organisation has
- any technology that helps you provide your products or services

It could include how you:

- assessed the risks of hosting information in different locations
- secure any data centres or locations you use that are operated by third parties

Security governance

You must make sure your information security policy is followed at all times and that you have a way for managing security risks. This is also known as 'security governance'.

You must:

- make a security plan based on security risks you've identified
- have a process for investigating and responding to security risks

- report security risks in a way that's proportionate to your organisation and product or service
- have a robust assurance and review process

Use security measures to protect the information you collect

You must use technical and organisational safeguards to protect personal data. Your security measures must guarantee the confidentiality and integrity of information. This means they need to reliably protect information from:

- loss or misuse
- unauthorised use, access, modification or disclosure fraud

To do this, you must make sure that you:

- use safeguards (for example, pseudonymisation, anonymisation and encryption) that are robust
- use security measures that guarantee confidentiality, integrity and availability
- test your security measures regularly, using the same tests each time, and improve them whenever you can
- can quickly restore access to personal data if there's a physical or technical incident
- know how you'll tell people if there's a security breach, so they can protect themselves from potential identity theft

You must also show how you meet these requirements in your ongoing internal audits.

5.9 Risk management

Your organisation must have a risk management framework that follows industry standards, such as:

- ISO/IEC 27005:2018 (https://www.iso.org/standard/75281.html)
- ISO 31000:2018 (https://www.iso.org/iso-31000-risk-management.html)

You must follow the latest version of the standards.

Whichever standard you follow, your risk management framework must include guidance about how to:

- identify risks to your organisation, including where they can come from and the impact they could have
- identify risks to your users, such as phishing attacks
- find out how likely it is that risks could happen
- measure how effective your current processes are at managing risks
- compare any risks you've identified to the established risk criteria
- monitor risks
- report risks to your stakeholders
- measure residual risk
- write, implement and maintain your organisation's risk strategy

- protect your organisation from internal risks, including writing a bribery and corruption policy

5.10 Fraud management

Anyone that's part of the trust framework must follow best practice guidance on fraud management. For example, this could be:

- guidance from the Chartered Institute of Public Finance and Accountancy (CIPFA) (https://www.cipfa.org/policy-and-guidance)
- Government Functional Standard GovS 013: Counter fraud (https://www.gov.uk/government/publications/government-functional-standard-govs-013-counter-fraud)
- Government Internal Audit Agency's standards (https://www.gov.uk/government/publications/public-sector-internal-audit-standards)

As well as best practice, you must meet the following five requirements:

Fraud monitoring

You must have a way to regularly monitor threats and fraud. This must be assessed during internal audits, fraud audits and exceptional audits conducted by an independent internal auditor or a third party.

You must also have a way to identify, notify and support a user whose identity, attribute or account has been compromised.

Legal, policies and procedures for fraud management

You must make sure you have all relevant legal, policy and procedures for the sectors you work in or with including:

- thresholds for investigating
- data sharing agreements
- fraud dispute and resolution process
- interacting with individuals you believe or suspect have committed first party fraud

You must also have a clear understanding of legislative mechanisms for sharing fraud data. What these are will depend on which industry or sector you're working in.

Fraud reporting

You must:

- define a common set of contra-indicators to make sure reporting and analysis is consistent
- have a standardised, structured, clear reporting process for all connected services, organisations, users and agencies
- have minimum operational requirements for monitoring fraud and threat alerts
- send regular reporting and analysis to the relevant authorities to help manage the threat of identity fraud and identity misuse
- keep a log of any revoked or suspended accounts
- keep a log of any breaches

- advise when an external source has been breached

Intelligence and fraud analysis

You must have a way to:

- look for suspicious activity
- monitor transactions
- carry out threat intelligence

Sharing threat indicators (‘shared signals’)

You must:

- have a structured ‘shared signals’ framework that you can use to send and receive relevant identity data and intelligence
- notify all relevant parties, including the victim, if there’s a fraud incident
- sign up to an agreed shared signals approach for threat and fraud intelligence across the trust framework
- have a process for sharing information around detected and mitigated fraud threats
- have a process for reporting COMSEC incidents

If fraud or crime is suspected that meets the approved threshold for your industry or sector, you must save the relevant metadata and artefacts (allowing for privacy data protection and legal considerations) for investigation.

5.11 Respond to incidents

You must have a process for dealing with incidents that could have an impact on your product, service or users. These incidents might be related to:

- fraud, for example if a user’s identity is being used by someone else to sign in to your service
- service delivery, for example if users cannot use your product or service because it’s temporarily unavailable
- a data breach

Your process must follow industry best practice, such as the NCSC guidance on incident management (https://www.ncsc.gov.uk/collection/incident-management).

You might also have to help law enforcement agencies, the governing body or another organisation in the trust framework if they’re investigating an incident.

Respond to a fraud incident

You must follow industry best practice and established guidance if you suspect that fraudulent activity has taken place, for example if a user is:

- using a ‘synthetic’ (made up) identity
- pretending to be someone they’re not
- committing ‘first party’ fraud

You must have an incident response plan that:

- makes sure effective and timely action is taken if fraud happens
- explains who in your organisation will be involved in responding to the incident
- minimises losses
- collects the evidence for future investigations
- notifies the relevant organisations if an attribute is found to be fraudulent
- covers any necessary COMSEC requirements

Respond to a service delivery incident

You must have a process for managing and responding to service delivery incidents. This process must follow industry good practice, such as the Information Technology Infrastructure Library (ITIL) (https://www.axelos.com/best-practice-solutions/itil/what-is-itil) service management processes. Your process should cover how you will:

- log, categorise, prioritise and assign incidents
- create and manage tasks
- manage and escalate service level agreements (SLAs)
- resolve and close incidents

Responding to data breaches

You must follow data protection legislation on data breaches, as explained in the Information Commissioner Office's (ICO's) guidance on how to respond to data breaches (https://ico.org.uk/for-organisations/guide-to-dp/guide-to-the-uk-gdpr/personal-data-breaches/).

Data breaches can lead to:

- identity theft
- threats to a user's safety or privacy
- emotional or financial damage to a user

If a data breach happens, you must tell any users whose personal data might have been affected. You must contact them using a method that's appropriate for your users, product or service.

Taking part in an investigation

You might be asked to provide specific information as part of an investigation into an incident. Who's carrying out the investigation will depend on the industry or sector where the incident happened.

You will get some information about the user and will be asked to provide identifiers that match it. You might also be asked to provide any of the following information, if you have it:

- a user's name, date of birth, address or gender
- the IP address, phone number or email address a user was using during a specific time period
- the 'device fingerprint' and geolocation of the device a user was using during a specific time period
- the calling line identifier (CLI) a user was using during a specific time period
- the reference numbers assigned to the user's account

- unique references that identify the request you received
- contra-indicators and failure identifier (FID) codes
- unique identifiers related to a piece of evidence (for example a passport number)

To make sure you follow the Data Protection Act 2018 (https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted) and the UK GDPR (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/946117/20201102_-_GDPR_-__MASTER__Keeling_Schedule__with_changes_highlighted__V3.pdf) (which make up the 'data protection legislation') you must check that whoever's asking you for the information has a legitimate reason to request it.

5.12 Tell users about your product or service

You must make sure your users know exactly what your product or service does. You must clearly explain:

- any terms and conditions of use that the user needs to be aware of
- any fees that the user will need to pay to use your product or service

5.13 Privacy and data protection requirements

Personal data is information that can be used to identify a living person. It does not have to be written down, or even be true, to count as personal data. You must follow data protection legislation whenever you do anything with users' personal data. The Information Commissioner's Office (ICO) has a guide to data protection (https://ico.org.uk/for-organisations/guide-to-data-protection/) that explains what requirements you must meet. As well as these requirements, there are other privacy and data protection responsibilities set out below which you must meet to manage users' personal data if you want to be a trust framework participant.

Your responsibilities under data protection legislation

You must have a valid reason ('lawful basis') for collecting and processing users' personal data. You can only ask users for data that will help you achieve this. You must not collect any more data than you need.

You must decide which lawful basis is most appropriate for your organisation.

As part of your legal responsibility around the user's right to be informed (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/), you must make sure users can easily find out:

- why you're collecting their personal data
- what it will be used for
- who you might share it with

You must explain this clearly and write it in a way that users can understand. In some cases, users will be happier to share their data if it's clear why you need it. For example, a pension calculator might need to know the user's gender because the rules are different for men and women.

Do not mislead users about why you're collecting their personal data, and only handle it in ways they would reasonably expect. users who share their data with you should never be surprised about how it's used. When you ask users for personal data, you must consider how disclosing it could affect someone. A user might worry about being:

- discriminated against
- at risk if someone steals their data, for example for credit card fraud
- at risk if someone shares their data, for example if their home address is given to an abusive ex-partner

You must make sure any personal data you collect is accurate and secure.

Users must be able to see what data you have about them and ask for a copy of it. This is known as their 'right to access'. Follow the ICO guidance on how to handle right of access (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/).

After you've collected a user's personal data, they must be able to ask you to correct, update or delete it (depending on the lawful basis you've chosen).

You must protect users' personal data 'by design and by default (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/)'. This was previously known as 'privacy by design'.

Your privacy and data protection responsibilities as part of the trust framework

To be a trust framework participant, you must meet the following requirements as well as following data protection legislation.

Getting your users' agreement

You must choose a lawful basis that's connected to whatever their digital identity or attribute product or service does. Whichever legal basis you choose, you must get customers' to provide positive confirmation that they have understood how their personal data will be stored and in what conditions their digital identities or attributes will be shared or disclosed. You can ask for customers' positive confirmation in any way, as long as you're able to show that you've done it.

If you make substantive changes to the way your product or service handles users' data, you must ask the user to renew their agreement. You must have a way for the user to renew their agreement if:

- you make any changes to how your product or service handles users' data
- your product or service starts offering something different to what users might expect

You must not collect and process personal data to:

- 'profile' users of any age for marketing purposes
- create aggregate data sets that might be abused or could reveal sensitive information about users
- process digital identities or attributes without the user's agreement

Letting users access and update their personal data

You must have a way for users to:

- ask if you have personal data about them
- access any personal data you might have
- find out who has accessed their personal data and when it happened

You must take steps to make sure personal data is accurate and not misleading in any way.

In some cases you'll also need to check that it's up to date. What you need to do depends on the data, your purpose for collecting or processing it, and your systems. For example, an organisation might do this by:

- asking end users for two-factor authentication (2FA) before they can update their address online
- improving their computer system to make it easier to add information
- asking their employees to check their emergency contact details once a year

Using a privacy compliance framework

You must have a structure you can use to keep personal information secure. This is called a 'privacy compliance framework' (sometimes known as a privacy information management system, or PIMS). You must be able to show that your privacy compliance framework meets the following standards:

- BS 10012:2017 (https://shop.bsigroup.com/ProductDetail?pid=000000000030378574) from the BSI (British Standards Institution)
- ISO/IEC 27701:2019 (https://www.iso.org/obp/ui/#iso:std:iso-iec:27701:ed-1:v1:en) from the ISO (International Organization for Standardization)

If you do not have a privacy compliance framework, you'll need to set one up. The BSI and ISO standards both include information to help you create and maintain a framework.

You must also support your framework by making sure you have:

- a clear data protection policy, which is understood and followed at all levels
- a named data protection officer - you'll need to appoint one if you do not have one
- secure audit logs that do not introduce personal information risks
- a complaints procedure
- a process for doing Data Protection Impact Assessments (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/), also known as DPIAs or 'privacy impact assessments'

Appointing a data protection officer

You must appoint a data protection officer. They will be responsible for making sure your organisation follows your data protection policy. The data protection officer will need to carry out the tasks defined in article 39 of the UK GDPR (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/946117/20201102_-_GDPR_-__MASTER__Keeling_Schedule__with_changes_highlighted__V3.pdf).

They must also make sure DPIAs are completed for digital identity and attribute services. DPIAs can help you identify and minimise the privacy risks associated with new initiatives or changes. DPIAs must be kept and made available for external review at any time.

Using data protection processes

You must design or use a data protection process. Make sure you give equal attention to every step of building and running your service.

You must also use externally accepted standards to make your systems easier to review, such as the widely used terms and definitions in ISO/IEC 29100 (https://www.iso.org/obp/ui/#iso:std:iso-iec:29100:ed-1:v1:en).

5.14 Keep records

You must record what you did to create, manage, share or consume a digital identity or attribute. How you do this will depend on which legislation is relevant to the industry or sector your organisation is part of. You must, however, do this in a way that meets the requirements article 30 of the UK GDPR (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/946117/20201102_-_GDPR_-__MASTER__Keeling_Schedule__with_changes_highlighted__V3.pdf).

You must keep your own copies of any records. You must dispose of these records when you no longer have any use for them.

If an identity service provider is sharing a verified digital identity with a relying party, they might need to make sure the relying party gets a copy of any records about that digital identity.

Attribute service providers might also need to do this.

Before you start keeping records, you must have:

- clear rules for keeping, managing and disposing of them
- a records management policy and a disposal statement
- a named person in your organisation who oversees records management

You must have rules that cover your day-to-day records management. For example:

- which records to keep
- who should keep them
- how to keep them, covering the formats and media you use
- when to dispose of records - this is usually covered in a disposal statement

The rules for your organisation can be as detailed as you need them to be. These rules can be a part of your records management policy or maintained separately.

Records management policy

You must have a regularly updated and published records management policy. The policy must include:

- a commitment to managing records, including what’s covered and why
- the policy’s objectives (for example, to help you meet standards or legal requirements)
- how the records management policy relates to your organisation’s other policies, such as data security or fraud policies
- the job roles in your organisation and what their management responsibilities are specific plans for records that are particularly important or sensitive

It must be easy for anyone in your organisation to find and use the policy. This will help everyone understand why it’s important to follow the management rules and keep records correctly.

The records management policy must have been agreed at a senior level. It will usually be part of your wider information management strategy. You must choose a named person to check it's being followed and regularly review it.

Your other responsibilities

You must also:

- have guidance on common issues that the rules do not cover, such as naming conventions
- know how (and how often) you're going to check that your records are being managed according to your policy
- make sure that access to records is controlled and monitored

Disposing of records

Your organisation must have clear rules on how long to keep records which meet requirements in data protection legislation. When it's time to stop keeping them, you must dispose of them in an appropriate way. Before you decide whether to keep or dispose of a record, you must consider if you need it for:

- legal reasons
- performance analysis
- fraud analysis
- audits or other investigations

You might need to keep just part of the record. For example, a medical research organisation might need a record of someone's symptoms and what treatment they had. They can keep this and dispose of any other information that was part of the record.

Disposal statement

Your organisation must have a formal written disposal statement. It must include the types of record you handle and:

- how long you keep each type
- how you dispose of each type
- your processes for archiving and destroying records

What people in your organisation need to do

Anyone who handles records must follow the records management policy. This includes temporary staff and contractors. Everyone who works for your organisation must know:

- which information needs to be added to the record-keeping system
- what your records management policy is
- what they must do to follow data protection legislation and (if your organisation is a public authority) the Freedom of Information Act (https://www.legislation.gov.uk/ukpga/2000/36/contents)

Appointing a records manager

You must choose a named person to oversee your records management. They will be ultimately responsible for making sure your records are accurate, accessible and secure. They will need to:

- check your records are being managed according to the records management policy and disposal statement
- make sure you meet your legal and regulatory requirements
- set up or maintain your record-keeping systems
- identify important or sensitive records that need specific management plans
- set up a way to document who has accessed, added or changed a record act as a single point of contact for records management issues

5.15 Things you must not do as part of the trust framework ('prohibited conduct')

When doing anything related to the trust framework, you (including any third party using services from the framework) must not do anything that's illegal in the UK. This could include:

- selling illegal goods, substances or services
- promoting acts of violence or terror
- bribery
- fraud
- conspiracy
- copyright infringement
- breaching data protection legislation
- breaching financial regulations
- breaking the law in any other way

You must not:

- be misleading or deceptive
- contradict the terms of use
- target, with the intention to exploit, users who are suffering from physical, emotional or financial distress (for example promoting services like unaffordable loans to users that are in financial trouble)
- damage the reputation, image, goodwill or trustworthiness of the trust framework or the trustmark

Glossary of terms and definitions

Term	Definition
Attributes	Pieces of information that describe something about a person or an organisation.
Attribute service providers	Individuals or organisations that collect, create, check or share attributes.

Term	Definition
Authenticator	Something that users can use to access a service. It could be some information (like a password), a piece of software or a device.
Calling line identifier (CLI)	Something that lets whoever's receiving a phone call see the caller's number.
Certification	When an independent auditor checks that organisations follow the rules of the trust framework.
Communications Security (COMSEC)	A way of preventing unauthorised people from accessing telecommunications or written information that's transmitted or transferred.
Contra-indicators	A way of categorising any wrong or contradictory information that you might get from users.
Cryptographic	A way to guarantee the integrity and confidentiality of data transmitted over a public network. This is done by a combination of encryption and signing.
Delegated authority	When a user acts on behalf of someone else.
Digital identity	A digital representation of who a user is. It lets them prove who they are during interactions and transactions. They can use it online or in person.
Digital signatures	A type of electronic signature that's used to validate the authenticity and integrity of a message, like an email, credit card transaction or a digital document.
Digital wallet	An electronic device, online service or software program that allows one party to make electronic transactions with another party for goods and services.
Encryption	When data is intentionally made difficult to read so that it can be shared securely.
Failure identifier (FID)	A 4-character warning code that explains what's wrong with an identity or piece of evidence.
Firewall	A network security system that monitors and controls incoming and outgoing network traffic.
Hash function	When data is converted into a fixed-length value. A hash cannot be reversed to reveal the original data.
Identifier	A piece of information that can be used to make a connection between an attribute and a person or organisation.
Identity service providers	Identity service providers prove and verify users' identities. They might not need to do all parts of the identity checking process. They can specialise in designing and building components that can be used during a specific part of the process.

Term	Definition
Internet Protocol (IP) address	A numerical label assigned to any device connected to a computer network that uses Internet Protocol.
Intrusion detection system	Software that automatically looks for possible incidents during events in a computer system or network.
Metadata	Data that provides information about other data.
Phishing	When criminals attempt to trick users into submitting personal information by asking them to click on links within scam emails or text messages.
Pseudonymisation	When information within a data set that could easily be used to identify someone is replaced by something else.
Public Key Infrastructure (PKI)	A way to implement secure electronic transactions over insecure networks, such as the internet. It's used to authenticate identities for the purposes of data encryption and signing.
Qualified trust service	A service offered by a qualified trust service provider that meets the requirements in the UK electronic identification and trust services (eIDAS) regulation.
Relying party	Organisations that get (or 'consume') products or services from trust framework participants.
Scheme	A group of different organisations who agree to follow a specific set of rules around the use of digital identities and attributes.
Scheme operator	An organisation that creates, runs and sets the rules of a scheme.
Shared signals	When intelligence is shared across the trust framework to reduce the impact of fraud on its participants and users.
Trust framework	A set of rules and specifications that organisations agree to follow in order to achieve a common purpose.
Unique identifier	Unique data used to represent someone's identity and associated attributes.
User	People who use digital identity and attribute products and services to prove their identity or eligibility to do something.
User agreement	Something that confirms users have understood how their personal data will be stored and how their digital identities or attributes will be shared.

Print this page