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

Identity providers in the identity and attributes exchange (IAX): what you must do

As an identity provider, you're responsible for checking users' identities when they want to do things online.

Any identity providers that want to take part in the trust framework must follow the rules in this guidance.

Before they can do this, they must already follow the rules in the guidance about:

- proving and verifying someone's identity
- using authenticators to protect an online service

Setting up a digital identity account

To set up a digital identity account for someone you need their:

- 'official' name (this is the name on any official documents they have, such as their passport)
- date of birth
- address
- email address
- phone number

You can ask the user for more information if you want to personalise the user experience. This might include any other names the user goes by, for example TJ instead of Tom.

Collecting more information can also make it:

- easier for buyers to match users to existing records
- quicker for users to access new services

If someone already uses a service you provide, you might be able to add a digital identity account to their existing account. For example, a user might have signed up to do online banking with a bank. The bank could reuse the user's details to help them set up their digital identity.

You can let a user pause their progress when they set up an account and come back to it later.

This can help users create an account if they:

- do not have all the information they need with them at the time
- need to show some information to someone in person as part of the process

However, this can also give fraudsters the opportunity to look up information about the person they're pretending to be.

If a user makes changes to their account

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

Do not only send notifications to the user through your product or service. You should also contact them using a different channel, for example by phone, post or email. You should do this using contact details that you know belong to the person who set up the account.

If the user wants to change their contact details too, you must check they are the same person who created the account by doing a 'verification' check.

Proving and verifying a user's identity

This section explains what all identity providers in the trust framework must do to prove and verify someone's identity.

Get evidence of the claimed identity ('strength')

You must check the strength of any evidence you have of the user's identity.

As an identity provider on the trust framework, you'll be able to accept an expired UK passport as proof of someone's identity.

It will still be valid as proof of the user's identity up to 18 months after the date it expired, but the security features can no longer be trusted. This means it will only have a score of 2 instead of a score of 4.

Check the evidence is genuine or valid ('validity')

You must make sure any evidence you have of the user's identity is genuine or valid.

As an identity provider on the trust framework, you'll need to do some extra checks on certain pieces of evidence.

Check the format of a European driving licence

All driving licences issued in Europe should use the same reference numbers. This will make it easy for you to tell what information is on it, even if the licence is in another language.

The licence should include the following reference numbers and pieces of information:

- 1 - the driver's surname
- 2 - the driver's first name
- 3 - the driver's date and place of birth
- 4a - the date the licence was issued
- 4b - the date the licence expires
- 4c - the department or organisation that issued the licence

It might also include:

- 8 - the driver's address
- an issue number

Read the European Directive 2006/126/EC to find out more about these reference numbers.

Check 'compound identifiers'

Some pieces of information include a series of numbers and letters that are specific to that type of evidence. This is known as a 'compound identifier'.

When you check a piece of evidence, you must make sure that the format of the compound identifier is correct.

The compound identifiers you'll most likely need to check are:

- someone's Driver and Vehicle Licensing Agency (DVLA) driver number
- the issuer identification number on a payment card

DVLA driver number

All driving licences issued in England, Scotland and Wales include a DVLA driving licence number. The number always follows a certain pattern.

If a driver number does not follow this pattern, it's likely the driving licence will not be genuine.

The number is 18 characters long. The first 5 characters are the first 5 letters of the driver's surname. If their surname has less than 5 letters, the rest of the characters will be the number 9 (for example FOX99). Some names might be spelled differently on purpose to make the driver number more unique, for example MC instead of MAC.

The next character is the decade from the driver's date of birth, for example '8' for 1985.

The next 2 characters are the month from the driver's date of birth, for example '05' for May. If the driver's gender is female, a 5 will be added to the first number of the month, for example '60' instead of '10' for October.

The next 2 characters are the day from the driver's date of birth, for example '14' for 14 August.

The next character is the last digit of the year from the driver's date of birth, for example '5' for 1985.

The next 2 characters are the first 2 initials of the driver's name, for example 'DJ' for David Jacob. If the driver does not have any middle names, the second character will be the number 9.

The next character is usually a 9, but DVLA might change it to another number to make the driver number more unique. The next 2 characters are randomly generated by DVLA.

The final 2 characters are the licence issue number.

> **Example**
> Marjorie Jacqueline Harris was born on 14 September 1956. Her DVLA driver number is HARRI559146MJ93122.

Issuer identification number

Most payment cards, including debit or credit cards, will include an issuer identification number (IIN). The number can be up to 18 characters long and follows the numbering system explained in ISO/IEC 7812.

If the IIN does not follow this numbering system, it's likely the document will not be genuine.

The first character will be the major industry identifier (MII). This changes depending on which type of organisation issued the evidence. For example, a bank card number should begin with 4 or 5.

The next 5 characters will be the 'Register of Card Issuer Identification Numbers'. These are followed by the user's account number, which can be up to 12 characters long.

The last character is always a 'check digit' that's been created using something called the Luhn algorithm. This is explained in annex B of ISO/IEC 7812.

How often you need to check the evidence

If you've checked a piece of evidence was valid with an authoritative source, you must do the same check:

- 6 months after the account was set up if you want medium confidence in the person's identity
- 3 months and 6 months after the account was set up if you want high confidence or very high confidence in the person's identity

Remember that there's always a risk the piece of evidence could have been lost or stolen when the account was set up - it just might not have been reported at the time.

If the piece of evidence is not valid, you must ask the user for another piece of evidence. You must check this is valid and do the necessary follow up checks.

Check the claimed identity has existed over time (‘activity’)

You must design your own process to check if a claimed identity has existed over time. You must do each check in exactly the same way to make sure your process is consistent.

Check if the claimed identity is at high risk of identity fraud (‘identity fraud’)

You must make sure the claimed identity is not at a higher than usual risk of identity fraud or is a made up ('synthetic') identity.

Whenever a new user sets up an account, you must check their details against your own records and an authoritative, counter-fraud data source. What checks you need to do will depend on the identity profile you're trying to meet.

You must also look out for any fraudulent activity when users sign in to your service. You must do this check at least every 6 months.

Check that the identity belongs to the person who's claiming it ('verification')

You must prove that the person who's going through your identity checking process is the claimed identity.

Pausing and resuming knowledge-based verification (KBV) challenges

If a user can pause their progress while they're completing KBV challenges, to protect your service you must make sure:

- the user can only pause and resume their progress twice
- you do not tell them if the answers they've given so far are right until they've completed all the KBV challenges

You must not ask the user to complete the same KBV challenges you asked them before they paused their progress.

You must ask the user to complete more challenges if you do not know what challenges they were given before they paused their progress. How many challenges you ask them to complete depends on:

- the quality and type of the KBV challenges
- if it's the first or second time the user is resuming their progress

Type of KBV challenge	Number of extra challenges (first time)	Number of extra challenges (second time)
Low quality	2	2
Low quality multiple choice	3	4
Medium quality	1	1
Medium quality multiple choice	1	2

High quality	1	1
High quality multiple choice	1	1

Matching someone to biometric information: false match and false non-match rates

A 'false match' happens when a system incorrectly matches a user to someone else. The system you use must have a false match rate of 0.01% or less. This means only 1 user in 10,000 could be incorrectly matched to someone else. This applies to all types (or 'modalities') of biometric information.

A 'false non-match' happens when a system cannot find a match for a user, even though it has already collected that user's biometric information. The system must have a false non-match rate of:

- 3% or less if it collects high quality biometric information
- 10% or less if it collects medium quality biometric information

You must make sure the system has the right false match and non-match rate. You must do this before you use the system for the first time.

How you check the system depends on how much confidence you need in someone's identity.

If you need low confidence, you will need to choose a system that has the required false match and false non-match rates. You do not need to do any additional tests.

If you need medium confidence, you must test the system in a way that follows ISO/IEC 19795-1. You will need to submit a report to show you've done this.

If you need high confidence or very high confidence, the system must be tested by an independent testing lab. The lab will need to follow ISO/IEC 19795-1.

Matching someone to biometric information: detecting presentation attacks

A presentation attack (also known as 'spoofing') is when someone uses an 'artefact' to try to convince a system that they're someone else. An artefact could be something like a fake fingerprint, a mask or a recording of someone else's voice.

There are different types of artefacts. An artefact will be a different type to another if it was made using different materials or processes. This is true even if both artefacts are designed

to look like the same body part.

For example, a face mask made out of latex, a face mask made out of paper and a face mask based on an image taken from a user's social media account are considered to be different types of artefact.

There are different levels of presentation attack. Whether they're successful depends on:

- how skilled the attacker is and what resources they have
- how effective the system is at detecting different presentation attacks that use different types of artefacts

> Read the National Institute of Standards and Technology's (NIST's) Strength of Function for Authentication (SOFA) framework guidance to find out about the different levels of presentation attack.

You must measure the success of an attack using an impostor attack presentation match rate (IAPMR). This calculates how successful the attack is at convincing the system that the user is a specific person (also known as a 'target').

Most of the time a system should be able to recognise when an artefact is being used. But sometimes an artefact can be used that a system finds more difficult to recognise. You should use a system that aims to get a minimum IAPMR for most of the artefacts and a higher IAPMR for all of the artefacts.

> **Example**
> You might use a system that fails to recognise an artefact 3 times out of 10. This is an IAPMR of 30%.

How you measure the success of an attack depends on how much confidence you need in someone's identity.

If you need low confidence, you just need to choose a system that offers some protection against presentation attacks. You do not need to do any additional tests.

If you need medium confidence, you must test the system in a way that follows ISO/IEC 30107-1. You will need to submit a report to show you've done this.

If you need high confidence or very high confidence, the system must be tested by an independent testing lab. The lab will need to follow ISO/IEC 30107-1.

Testing IAPMRs

Any testing must be done with a group of at least 10 people. These people will need to provide biometric information, which will be used to create different types of artefact to test the system with.

For each person, you or the lab must create and test:

- 6 level A artefacts
- 4 level B artefacts
- one level C artefact (very high confidence only)

If you need medium confidence, you must use a system that has an IAPMR of less than:

- 30% for 5 out of 6 of the level A artefacts
- 50% for all 6 level A artefacts
- 30% for 3 out of 4 of the level B artefacts
- 50% for all 4 level B artefacts

If you need high confidence, you must use a system that has an IAPMR of less than:

- 20% for at least 5 out of 6 of the level A artefacts
- 50% for all 6 level A artefacts
- 20% for 3 out of 4 of the level B artefacts
- 50% for all 4 level B artefacts

If you need very high confidence, you must use a system that has an IAPMR of less than:

- 20% for at least 5 out of 6 of the level A artefacts
- 50% for all 6 level A artefacts
- 20% for 3 out of 4 of the level B artefacts
- 50% for all 4 level B artefacts
- 30% for 1 level C artefact

Check information about a user is accurate

You must check the information the user gives you is accurate before you let them access services with their digital identity account.

It's important that you do this when the user:

- first sets up their account
- makes any changes to their account

You must check the information is accurate again during the time the account is being used. When you need to do this depends on how much confidence you need in someone's identity.

You will need to check the information:

- once a year if you need medium confidence
- once every 6 months if you need high confidence
- once every 3 months if you need very high confidence

Name

You must make sure the user gives you their current 'official name'. This is usually the name that appears on any official documents they have, such as their passport.

You must also ask the user if they've changed their name in the last year. If they have, you must ask them to give you any names they were known by during this time.

The user does not have to provide this information if they changed their name because of gender reassignment. You must make this clear to comply with section 7 of the Equality Act 2010.

You must check at least one of these names is accurate by proving the user's identity. Read the guidance about identity proofing and verification to find out how to do this.

You must then link the user's previous name to their current name. To do this, you can either:

- ask the user to give you a piece of evidence that includes both their names (such as a marriage or civil partnership certificate) and make sure it's valid
- check if an authoritative source already has a record of the name change

Date of birth and other dates

You must make sure the user's date of birth is a real date and not something like 29 February 1987. This applies to any other dates you might ask for when the user creates an account, such as the date a document expires.

It's unlikely that a user will ever need to change their date of birth. They might need to do this if their actual date of birth was:

- unknown when a piece of identity evidence was issued to them (for example this can happen if they're an asylum seeker)

- recorded incorrectly

If the user has changed their date of birth, you must make sure it's accurate by either:

- asking the user to give you a piece of evidence that includes their new date of birth and checking it's valid
- checking if an authoritative source already has a record of the new date of birth

Address

You must ask the user for their address. If they have more than one current address (for example they live in different places during the week and weekends), you'll need all of their current addresses.

You must check the user's postcode is real and matches the address they gave you with an authoritative source.

You must also ask the user if they've changed their address within the last year. If they have, you must ask them to give you any addresses they lived at during that time. You must be able to confirm that the user lived at one of these addresses.

If you cannot prove the user's identity using a current address, you must link it to one of their previous addresses. You can do this by either:

- asking the user to give you a piece of evidence that includes their name, new address and some information that's unique to them (such as their photo) and checking the evidence is valid
- checking if an authoritative source already has a record of the address change

Email address and phone number

You must check the user's email address and phone number work and belong to the right person by either:

- sending the user an activation link or code which they can use to confirm they have access to the account or number
- checking their details with an authoritative source (this might be your organisation if the user has already signed up to use another of your products or services)

You must also make sure the user has not already used that email address to set up a digital identity account with your service. If they have, you should let them know they have another account and tell them to use that.

If the user gives you wrong or contradictory information

You must look up the relevant 'contra-indicator' to find out what to do if a user gives you information that:

- is wrong
- contradicts information that you or an authoritative source already has about that user or the person they're claiming to be (the 'claimed identity')

Give users a way to access your service

You must give a user an 'authenticator' which they can use to access your service. An authenticator could be some information (like a password), a piece of software or a device.

Follow the guidance about using authenticators to protect your service to choose an authenticator that will give you the level of protection you need. This guidance will also tell you what to do if a user has lost access to their account.

You must also make sure a user cannot make changes to their account without signing in with an authenticator.

Closing an account

You must have a way to close an account if either:

- the user wants to close it
- it's inactive

A user should be able to create a new account to use your service after their original account is closed. They must not be able to reopen a closed account.

If the user wants to close their account

You must make sure the user is the same person who created the account before you let them close it. You can do this by asking the user to sign in to their account.

If they cannot do this, you must instead do the same sort of verification checks that you did when you first proved the user's identity.

You must temporarily 'suspend' the account for at least 1 month before you close it. This means the user cannot use it to access services.

You must contact the user during this time to let them know their account will be closed. They must have the chance to reactivate their suspended account. This will help prevent an account being closed by anyone other than the user who set it up.

If the account is inactive

If a user has not used their account for 3 years, you can choose to close it.

You must contact the user to let them know at least 3 months before you plan to close their account. If you do not hear back from the user within this time, you can close their account.

Keeping records of closed accounts

You must comply with the Data Protection Act 2018 by not keeping records of closed accounts any longer than your organisation needs them.

Show the user when they last signed in to their account

You must show a user the time and date when they last signed in. They can use this information to check that no one else has signed in to their account.

If you cannot access a data source to check information

You'll often need to check information with other data sources, including authoritative sources. If a data source is unavailable, you can delay checking some information for up to 5 days.

For example, a user might move house and need to update their address in their account. If the data source you need is unavailable, you can let the user make this change without checking the new information is accurate.

You must check the information as soon as the data source is available. If you cannot do this within 5 days of the change being made, you will need to suspend the account.

You cannot delay checking information:

- when the user first sets up their account
- if there's a problem with your service

If you cannot check information with a data source in these situations, you must not let the user create or sign in with their account.

Support you must provide

You must offer support to users and other participants in the trust framework. One way you can do this is by running a help desk.

To make sure you do not exclude users with different access needs, you must have more than one way to offer support.

Protecting your staff

As they check users' identities, the people you work with might come across:

- things they find distressing
- indecent images or videos

You must make sure:

- your staff have the right training and support to cope with these incidents
- you have a process for handling these incidents

Protecting vulnerable users

You must look out for users who you think might be vulnerable or unable to give their consent. For example, this might be because they're under 13, which is the age of consent in relation to information society services.

The user should not be allowed to have an account unless a responsible person (like a parent or carer) gives consent on their behalf.

You must also look out for users who are being visibly forced or coerced into creating an account. If this happens, you must:

- not let them create an account

- report the incident to the relevant authorities

Records you must keep

You must make sure you keep records of any:

- events related to a user's account
- interactions a user has with your help desk
- information you collect when you prove a user's identity

Read the guidance about records management to find out what your responsibilities are when it comes to keeping records.

Events related to a user's account

You must create a record whenever:

- a user creates a new digital identity with you
- a user updates their account details
- a user's account is deleted
- a user's account is temporarily suspended
- a user's account is unsuspended
- a user recovers a forgotten, lost or stolen authenticator
- the level of assurance of an account changes

You must make sure each record includes all of the following information:

- the time and date the event took place
- how you checked the user's identity when you first set up their account
- any reference numbers you assign to the user's account
- the reason why the event took place (for example a user's account might be suspended because they entered the wrong password)
- through which channel the event took place (for example online, over the phone or in person)
- any specific identifiers related to the channel (for example an IP address)
- the details of any help desk operators that were involved in the event

Interactions with your help desk

You must keep a record of all interactions users and other participants in the trust framework have with your help desk. You will need these records to:

- carry out an audit of interactions if there's an investigation
- create a report on events
- investigate fraudulent activity carried out by people using the help desk
- investigate fraudulent activity carried out by help desk operators

You must make sure the record includes all the following information:

- the time and date the interaction took place
- if you or the user started the interaction
- the user's calling line identifier (CLI), if you spoke to them over the phone
- the user's IP address, if you spoke to them online using something like webchat
- the help desk operator's details (including their IP address)
- what the user asked you to do and if you did it
- the details of the user's account (including reference numbers assigned to the user's account)
- the details of the channel you used to respond to the user's request (for example phone number or email address)

Information you collect when you prove a user's identity

You must keep a record of all information the user gives you.

If the user provided a physical piece of evidence at any point during the identity checking process, you must at least keep a record of the information on it. For example, if the user showed you their passport, you must keep a record of the details that appeared on it.

You must also keep a record of all reference numbers assigned to the user's account.

Responding to incidents

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

- identity 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 service because it's temporarily unavailable

You might also have to help the police, the authoritative body or another organisation in the trust framework if they're investigating an incident.

Respond to an identity fraud incident

You must follow the guidance on responding to an identity fraud incident if you suspect that a user is:

- using a 'synthetic' (made up) identity
- pretending to be someone they're not

Respond to a service delivery incident

You must have a process in place for managing and responding to service delivery incidents. This process must follow industry good practice, such as the Information Technology Infrastructure Library (ITIL) service management processes.

Taking part in an investigation

You might be asked to provide specific information if an investigation into an incident is happening. You must respond within 7 days (or 24 hours if the request is 'urgent').

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:

- 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, contra-indicator scores and failure identifier (FID) codes
- unique identifiers related to a piece of evidence (for example a passport number)

Managing how much confidence you have in someone's identity

You might need to increase how much confidence you have in someone's identity over time. This will depend on what services the user needs to access with their digital identity account.

You must meet an identity profile for the level of confidence you need. You do not need to do each part of the identity checking process again - you might be able to build on checks you've already done. For example, you can use a piece of evidence you've already checked as part of meeting a new profile.

You'll have less confidence in someone's identity if you do not keep doing the checks you need to have a higher level of confidence. For example, not checking a piece of evidence again 6 months after the account was set up will mean you'll have low confidence instead of medium confidence in someone's identity.

If you cannot complete a part of the identity checking process, you should not change the account to a lower level of confidence than the one you originally chose.

For example, if you need medium confidence in someone's identity but find out a piece of evidence is known to be stolen, you must not ignore this and let the user create a low confidence account instead. As you've failed to prove that a piece of evidence is valid, you must ask the user for a different piece of evidence and carry on checking their identity.