Cabinet Office
Government Digital Service

Identity proofing and verification of an individual

Document reference: Good Practice Guide (GPG) 45, version 4.1

Contents

1.0 Purpose of this document

1.0.1 You should read this guidance to help you decide how you or your service will check someone's identity.

1.0.2 You can use this guidance to work out which process you could use to check the identity of a customer, employee, or someone acting on behalf of a business. You could check someone's identity:

- digitally
- over the phone
- by post
- by email
- face to face

1.0.3 This guidance can also be used by people who:

- want to understand how another individual or organisation checks someone's identity (this includes auditing and certification of identity services)
- are comparing different identity checking processes, for example comparing schemes with the electronic identity and trust services (eIDAS) regulation

1.0.4 This guidance will not:

- tell you how to use accounts and passwords to give users access to something (also known as 'authentication')
- tell you how to assess your risk of identity fraud
- be relevant if you ask users for information about their identity but do not check it (also known as 'self-assertion')

2.0 What is identity

2.0.1 An identity is a combination of characteristics that identifies a person.

2.0.2 A single characteristic is not usually enough to tell one person apart from another, but a combination of characteristics might be.

2.1 When to check an identity

2.1.1 You should check someone's identity if you or your service:

- shows a user personal information about themselves, such as their driving licence or passport details
- gives the user something valuable, such as money or benefits

2.1.2 Users will not need to prove their identity to access some services. For example, if your service just needs to recognise that someone has used it before, you can authenticate them (by asking for a username and password) without checking their identity.

2.2 Why you should check an identity

2.2.1 By successfully checking someone's identity, you or your service can be confident that you'll give the right people access to the right things. If you do not do this, you or your service could be affected by identity fraud. This is when someone uses a 'synthetic' (made up) or stolen identity to pretend to be someone they're not.

2.2.2 The number of synthetic and stolen identities being used to commit identity fraud in the UK is growing every year. Some of the most common reasons people or criminal groups commit identity fraud are to:

- access services they're not entitled to
- get benefits they're not entitled to
- steal personal, medical or financial information from other identities
- enable organised crime, like human trafficking
- avoid being detected by the police and other authorities

2.2.3 If you follow this guidance, you or your service will check identities in a way that's consistent with other people or services that also follow this guidance. This does not mean you have to check an identity in the exact same way as someone else. You can do different types of checks to another person or organisation, but achieve the same levels of overall trust in someone's identity.

2.2.4 Checking identities in a consistent way will reduce the chance that one person or service does less effective identity checks than others. This helps protect against identity fraud. It also means that there will be fewer people or services with less effective identity checks that could be targeted by identity fraud.

2.2.5 Consistent identity checks also make it easier for you to trust an identity that's been checked by someone else. This means you can be comfortable reusing identities from someone else, so that:

- people only have to prove their identity once
- organisations and services can share the cost of checking someone's identity

3.0 How to check someone's identity

3.0.1 You'll need to know the 'claimed identity' of the person you're checking. A claimed identity is a combination of information (often someone's name, date of birth and address) that represents the characteristics of whoever a person is claiming to be.

3.0.2 When you have this, you can find out if the person is who they say they are. This process is known as 'identity checking' and is made up of 5 parts:

- get evidence of the claimed identity ('strength')
- check the evidence is genuine or valid ('validity')
- check the claimed identity has existed over time ('activity')
- check if the claimed identity is at high risk of identity fraud ('identity fraud')
- check that the identity belongs to the person who's claiming it ('verification')

3.0.3 Doing different parts of the identity checking process will help you build up confidence in an identity so that you can be sure someone is who they say they are.

3.0.4 You do not have to do all parts of the identity checking process at once. You can do them over any period of time and gradually build up your confidence in an identity.

3.0.5 You'll get a score for each part of the identity checking process you do. The highest score you can get for each part is 4.

3.0.6 How much confidence you'll have in an identity depends on:

- how many pieces of evidence you collect
- which parts of the identity checking process you do
- what scores you get for each part of the identity checking process

The different combinations of the identity checking process are known as 'identity profiles'.

3.0.7 Each identity profile relates to one of the following levels of confidence:

- low confidence (previously known as 'identity level 1')
- medium confidence (previously known as 'identity level 2')
- high confidence (previously known as 'identity level 3')
- very high confidence (previously known as 'identity level 4')

3.0.8 You should aim to get a higher level of confidence in someone's identity if you or your service are at high risk of identity-related crime.

3.0.9 How confident you are in a person's identity can increase over time if you do extra checks or collect more evidence.

3.0.10 Your confidence can also decrease over time, for example if you later find out that a piece of evidence you used might have been lost or stolen at the time you checked that person's identity.

3.0.11 You can also reuse identity checks done by another organisation if they do some or all parts of the identity checking process explained in this guidance.

3.1 Authoritative sources

3.1.1 You might need to check things with an 'authoritative' source. To be authoritative for a particular piece of information, the source must make sure:

- the integrity of the information is protected
- the information is up to date

The source must also do one of the following:

- issue evidence, for example the Driver and Vehicle Licensing Agency (DVLA) issues evidence such as driving licences
- get information from an organisation that issues evidence, for example credit reference agencies can have authoritative information about bank accounts
- get information from another authoritative source, for example from another identity scheme

4.0 Get evidence of the claimed identity ('strength')

4.0.1 This part of the identity checking process was previously known as 'Element A'.

4.0.2 Some pieces of evidence are 'stronger' than others, which means they will be harder to:

- forge (when an existing piece of evidence is changed to make it look like it belongs to someone else)
- counterfeit (when a piece of evidence is created from scratch)

4.0.3 How strong the evidence is depends on:

- what security features are on it (for example a hologram or an electronic chip)
- what information it has
- how the person proved their identity to get the evidence

4.0.4 The stronger the evidence is, the higher its score will be. You must check and score one piece of evidence at a time.

4.0.5 To get evidence of a claimed identity, you can either:

- ask the person to provide evidence themselves, like a document (such as a passport) or account details (which they can show by giving you something like a bill or an account number)
- find some evidence of their identity yourself, for example by checking databases

4.0.6 The evidence can be physical or digital.

4.0.7 The identity is sometimes shown as a synonym on different pieces of evidence. For example, it might say the person's name is Samantha on their passport, but Sam on their bank card. You can usually accept a synonym, unless you need to know the claimed identity's 'official' name (this is the name on any official documents they have, such as their passport).

4.0.8 The names might be different on different pieces of evidence. For example, someone's surname might have changed because they got married. If the names are different, you might need to collect other pieces of evidence or do other checks to make sure all the evidence belongs to the same person.

4.1 Score 1

4.1.1 The evidence will have a score of 1 if it contains at least 2 of the following pieces of information:

- the claimed identity's name
- the claimed identity's date of birth
- the claimed identity's place of birth
- the claimed identity's address
- the claimed identity's biometric information (these are measurements of biological or behavioural characteristics, like an iris or fingerprint)
- a photo of the claimed identity
- a reference number

4.1.2 The evidence should come from an organisation that you know will:

- check the person's identity when they issue the evidence
- make sure its process for issuing the evidence is not misused by people associated with the organisation

4.1.3 Some examples of evidence that will have a score of 1 include an email, PDF or letter from a local authority.

4.1.4 You may not be able to thoroughly check the validity of evidence that has a score of 1.

4.2 Score 2

4.2.1 The evidence will have a score of 2 if it has everything it needs to get a score of 1 and it includes information that's unique to either:

- the identity
- that piece of evidence

4.2.2 It must also:

- show the person's name instead of any pseudonyms, aliases or nicknames (if the evidence includes a name)
- be protected by physical security features that stop it from being reproduced without specialist knowledge or information (if the evidence is a physical document)
- be protected by cryptographic security features that can correctly identify the organisation that issued it (if the evidence includes digital information)

4.2.3 Some examples of evidence that have a score of 2 include:

- a firearm certificate
- a Home Office travel document (convention travel document, stateless person's document, one-way document or certificate of travel)
- a birth or adoption certificate
- an older person's bus pass
- an education certificate from a regulated and recognised educational institution (such as an NVQ, SQA, GCSE, A level or degree certificate)
- a rental or purchase agreement for a residential property
- a proof of age card recognised under the Proof of Age Standards Scheme (PASS)
- a Freedom Pass
- a marriage certificate
- a building, contents or vehicle insurance policy
- a gas or electric account

- a ‘substantial’ electronic identity from a notified eIDAS scheme

4.3 Score 3

4.3.1 The evidence will have a score of 3 if it has everything it needs to get a score of 2 and:

- it includes information that's unique to both the identity and that piece of evidence
- the organisation that issued the evidence made sure it was received by the same person who applied for it
- the organisation that issued the evidence checked the person’s identity in a way that follows the Money Laundering Regulations 2017

4.3.2 It must also:

- show the person’s 'official' name instead of their initials or synonyms, for example 'Julian' instead of 'Jules' (if the evidence includes a name)
- be protected by physical security features that stop it from being reproduced without specialist equipment (if the evidence is a physical document)

4.3.3 The evidence must also include one of the following:

- a photo of the person
- biometric information that uses cryptographic security features to protect its integrity
- cryptographic security features that can be used to identify the person who owns the evidence (this includes evidence with cryptographic chips and digital accounts that are protected by cryptographic methods)

4.3.4 Some examples of evidence that will have a score of 3 include:

- passports that meet the International Civil Aviation Organisation (ICAO) specifications for machine-readable travel documents
- identity cards from an EU or European Economic Area (EEA) country that follow the Council Regulation (EC) No 2252/2004 standards
- UK photocard driving licences
- EU or EEA driving licences that follow the European Directive 2006/126/EC
- a Northern Ireland electoral identity card
- a US passport card
- a bank, building society or credit union current account (which the claimed identity can show by giving you a bank card)
- a student loan account
- a credit account
- a mortgage account (including buy to let mortgage accounts)

- a digital tachograph driver smart card
- an armed forces identity card
- a proof of age card recognised under PASS with a unique reference number
- a loan account (including hire purchase accounts)
- a 'high' electronic identity from a notified eIDAS scheme

4.4 Score 4

4.4.1 The evidence will have a score of 4 if it has everything it needs to get a score of 3 and:

- it includes biometric information
- all digital information (including biometric information) is protected by cryptographic security features
- the cryptographic security features can prove which organisation issued the evidence
- the organisation that issued the evidence proved the person's identity by comparing and matching the person to an image of the claimed identity from an authoritative source

4.4.2 Some examples of evidence that will have a score of 4 include:

- biometric passports that meet the ICAO specifications for e-passports
- identity cards from an EU or EEA country that follow the Council Regulation (EC) No 2252/2004 standards and contain biometric information
- a UK biometric residence permit

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

5.0.1 This part of the identity checking process was previously known as 'Element B'.

5.0.2 To make sure you only accept a piece of evidence that's real, you should check if it's:

- genuine (not forged or counterfeit)
- valid (it's been issued and has not expired, been cancelled, or reported as lost or stolen)

5.0.3 You can check the evidence in person or remotely.

5.1 Score 1

5.1.1 The evidence will have a score of 1 if the physical features of the evidence appear to be genuine.

5.1.2 They'll appear to be genuine if the person checking the evidence can confirm:

- they're checking an original, certified copy or scan of the evidence
- there are no errors on the evidence, like wrong paper type, spelling mistakes, irregular use of fonts or missing pages
- the details, layout or alignment of the evidence look the way they should
- any logos look the way they should
- any references to information are the same across the evidence (for example if the body text of a letter references an address, this should match the address shown at the top of the letter)

5.2 Score 2

5.2.0.1 The evidence will have a score of 2 if you do one of the following:

- confirm the evidence is valid
- confirm the visible security features are genuine (these are security features that can be seen without using specialist light sources)
- confirm the ultraviolet (UV) or infrared (IR) security features are genuine

5.2.1 Confirm the evidence is valid

5.2.1.1 The person or system doing the check can confirm the evidence is valid by making sure the details on it match those held by an authoritative source.

5.2.2 Confirm the visible security features are genuine

5.2.2.1 The person or system doing the check will need to make sure:

- the original evidence has been shown (this could be in person or remotely, for example by using an app)
- they do not accept scans, photos uploaded by a user, or photocopies of the evidence (this is because it can be difficult to tell if these are forgeries or counterfeits)
- the evidence has not expired

- the evidence was shared with the person or system in a way that protects it from being tampered with (for example it could be sent by secure delivery)
- the evidence (or the image or video of the evidence) is clear enough to be able to examine its security features

5.2.2.2 They should check this using non-specialist light sources such as natural sunlight, indoor lights or desk lamps.

5.2.2.3 The person or system will need to use official templates to check any of the following features on the evidence look the way they should:

- background printing
- fonts and alignment
- holograms and positioning
- the way it's been laminated
- designs printed with optical variable ink (and check they look the way they should at certain angles)
- the format of any 'compound identifiers', such as a Driver and Vehicle Licensing Agency (DVLA) driver number or a machine-readable zone (MRZ)
- the position of any photographs on the evidence (they should not have been replaced or edited)

5.2.2.4 Some places where you can find official templates are:

- the Public Register of Authentic travel and identity Documents Online (PRADO)
- the EU and EEA driving licence handbook
- EdisonTD

5.2.2.5 If the evidence is being checked by a person, they must:

- be trained in how to detect false documents by a specialist trainer, such as the Home Office, National Document Fraud Unit or Centre for the Protection of National Infrastructure (CPNI)
- refresh their training at least every 3 years

5.2.2.6 If the evidence is being checked by a system, it must:

- have been built following good practice, such as the Home Office's guidance on identification document validation technology
- update the templates it checks the evidence against at least every 3 years

5.2.3 Confirm the UV or IR security features are genuine

5.2.3.1 The person or system doing the check will need to use a UV or IR light to make sure:

- the evidence has not expired
- the paper the evidence is printed on looks the way it should
- the alignment of the evidence looks the way it should
- any fluorescent features (such as fluorescent inks or fibres) look the way they should
- the evidence has not been tampered with (for example a UV light will show where UV features have been covered by glue if something has been stuck on the evidence)

5.2.3.2 The person or system will need to use official templates to check any of the following features on the evidence look the way they should:

- background printing
- fonts and alignment
- holograms and positioning
- the way it's been laminated
- designs printed with optical variable ink (and check they look the way they should at certain angles)
- the format of any 'compound identifiers', such as a DVLA driver number or an MRZ
- the position of any photographs on the evidence (they should not have been replaced or edited)

5.2.3.3 Some places where you can find official templates are:

- PRADO
- the EU and EEA driving licence handbook
- EdisonTD

5.2.3.4 If the evidence is being checked by a person, they must:

- be trained in how to detect false documents by a specialist trainer, such as the Home Office, National Document Fraud Unit or CPNI
- refresh their training at least every 3 years

5.2.3.5 If the evidence is being checked by a system, it must:

- have been built following good practice, such as the Home Office's guidance on identification document validation technology
- update the templates it checks the evidence against at least every 3 years

5.3 Score 3

5.3.0.1 The evidence will have a score of 3 if you check it's both genuine and valid. You can do this by doing all of the following:

- confirm the evidence is valid
- confirm the visible security features are genuine
- confirm the UV or IR security features are genuine

Alternatively, you can check the cryptographic security features are genuine.

5.3.1 Confirm the evidence is valid

5.3.1.1 The person or system will need to do the same checks to confirm the evidence is valid that are needed at score 2.

5.3.2 Confirm the visible security features are genuine

5.3.2.1 The person or system must do the same things needed at score 2 to confirm the visible security features are genuine.

5.3.2.2 They'll also need to:

- use evidence that has not been intercepted and reused (known as a 'replay attack')
- make sure any shadows or glare do not stop the security features on the evidence from being examined
- update any official templates that are used (such as those from PRADO) every year
- refresh their training in how to detect false documents every year (if the checks are being done by a person)

5.3.2.3 They must also confirm:

- designs printed using intaglio (raised) ink look the way they should
- designs that have been laser etched look the way they should
- features are consistent and correct across sections of the evidence

Example
In a UK passport, there should be a passport number on the page with the person's details on it. You should check if this number is the same as the number punched on the other pages in the passport.

To check this, they must use one of the following:

- a magnification tool (such as a magnifier)
- other inspection equipment used to identify forged or counterfeit documents

5.3.3 Confirm the UV or IR security features are genuine

5.3.3.1 The person or system must do the same things needed at score 2 to confirm any UV or IR security features are genuine.

5.3.3.2 They'll also need to:

- use evidence that's been shared in a way that prevents it from being replayed (intercepted or reused)
- make sure any shadows or glare do not stop the security features on the evidence from being examined
- update any official templates that are used every year
- refresh their training in how to detect false documents every year (if the checks are being done by a person)

5.3.4 Confirm the cryptographic security features are genuine

5.3.4.1 To make sure the cryptographic security features are genuine, the system that checks the evidence will need to:

- make sure the evidence has not expired
- read the cryptographically protected information
- provide any required cryptographic keys
- check the digital signature is correct
- check the signing key belongs to the organisation that issued the evidence
- check the signing key is the correct type for that evidence
- check the signing key has not been revoked

Example
Most debit or credit cards will have a cryptographic chip on them. You can check the chip is genuine by asking a user to make a zero balance payment using a card reader. If the transaction is successful you'll know the cryptographic chip and the bank account linked to it are genuine.

5.4 Score 4

5.4.0.1 The evidence will have a score of 4 if you do all of the following:

- confirm the visible security features are genuine
- confirm the UV or IR security features are genuine
- confirm the cryptographic security features are genuine
- check the evidence has not been cancelled by the organisation that issued it

5.4.1 Confirm the visible security features are genuine

5.4.1.1 The person or system must do the same things needed at score 3 to confirm the UV or IR security features are genuine.

5.4.1.2 They'll also need to:

- be supervised when they capture and examine the evidence by someone who's also been trained by a specialist trainer, such as the Home Office, National Document Fraud Unit or CPNI
- examine the evidence under 'controlled' light conditions (which means the lighting in the room creates the best possible environment for examining the security features on the evidence)
- examine the evidence under 'controlled' security conditions (which means there are ways to prevent systems from being fooled or people from being manipulated)

5.4.1.3 They'll need to check the following features of the evidence look correct:

- watermarks
- security fibres
- consistency throughout the piece of evidence
- secondary background ('ghost') images

Example
In the latest UK passport, there should be a ghost image of the person on the 'observations' page. You should check if the surname and date of birth in the image are the same as the person’s details.

To check this, they must use one of the following:

- a magnification tool (such as a magnifier)
- a low angle ('oblique') light
- other inspection equipment to identify forged or counterfeit documents

5.4.2 Confirm the UV or IR security features are genuine

5.4.2.1 The person or system must do the same things needed at score 3 to confirm any UV or IR security features are genuine.

5.4.3 Confirm the cryptographic security features are genuine

5.4.3.1 The person or system must do the same things needed at score 3 to confirm the cryptographic security features are genuine.

5.4.4 Check the evidence has not been cancelled

5.4.4.1 The person or system doing the check will need to make sure the evidence has not been cancelled by the organisation that issued it. They can do this by checking an authoritative database of cancelled evidence, for example Interpol for passports or a mobile phone operator for mobile phone contracts.

6.0 Check the claimed identity has existed over time ('activity')

6.0.1 This part of the identity checking process was previously known as ‘Element E’.

6.0.2 To lower the risk of you accepting a synthetic identity or an identity that belongs to someone who's died, you can check the claimed identity has existed over time.

6.0.3 You will not need to do this part of the identity checking process to meet all the identity profiles.

6.0.4 You should check if the claimed identity has interacted with other organisations. Some examples of interactions are:

- credit card transactions
- student loan repayments
- mortgage payments
- gas or electricity account payments
- when someone signs in to an online bank or retail account

6.0.5 You can also check if the claimed identity has records that show it's been known by organisations over time. Some examples of these records are:

- health records
- employment records
- school records

6.0.6 How confident you can be that the claimed identity was involved in an interaction depends on if:

- the organisation the claimed identity interacted with checked their identity
- the claimed identity's interactions are what you'd expect them to be

6.0.7 You should expect some people's interactions to appear differently to others. What interactions you expect the claimed identity to have usually depends on the type of interaction they're doing and the type of person they are (like their age or financial situation).

Example
You can expect someone who's been working for 20 years to have things like frequent financial transactions, but someone who's recently left school might not.

6.0.8 If you can't find interactions that happen in a way you'd expect for the claimed identity, you might be less sure that they were actually involved in the interactions. If this happens, you should find more interactions over a longer period of time. This lowers the risk that the claimed identity was not involved in the interactions because it would've taken a lot of effort for someone else to create so many false interactions.

6.1 Score 1

6.1.1 You'll get a score of 1 if you:

- have evidence of interactions between the claimed identity and an organisation
- know the organisation checked the claimed identity is who they say they are

6.1.2 These interactions need to have happened:

- over the last year
- in a way that you'd expect the claimed identity to behave

Example
Over the last year you've seen posts on a social media website that you'd expect the owner of the account to make. This account appears to be linked to the claimed identity, but you cannot be sure they actually created it. This is because this social media website does not check users' identities when they sign up. However, you've used an authoritative source to

make sure the email address or phone number associated with the account is linked to the claimed identity.

6.1.3 If the interactions do not happen in a way you'd expect the claimed identity to behave, you'll need to find interactions from over the last 3 years instead.

6.2 Score 2

6.2.1 You'll get a score of 2 if you:

- have evidence of interactions between the claimed identity and an organisation
- know the organisation used an authoritative source to check the claimed identity was who they said they were

6.2.2 These interactions need to have happened:

- over the last 6 months
- in a way that you'd expect the claimed identity to behave

Example
Over the last 6 months you've seen payments to a post-pay electricity account that you'd expect the owner of the account to make. This electricity supplier checked the account owner's identity using a credit check. This means you know the claimed identity is linked to this account.

You've found evidence of these payments by looking at printed or online statements that you know belong to the claimed identity.

6.2.3 If the interactions do not happen in a way you'd expect the claimed identity to behave, you'll need to find interactions from over the last year instead.

6.3 Score 3

6.3.1 You'll get a score of 3 if you:

- have evidence of interactions between the claimed identity and an organisation
- know the organisation checked the claimed identity was who they said they were in a way that at least met the requirements of the Money Laundering Regulations 2017.

6.3.2 These interactions need to have happened:

- over the last 3 months
- in a way that you'd expect the claimed identity to behave

Example
Over the last 3 months you've seen mortgage payments that you'd expect the mortgage owner to make. The mortgage provider checked the mortgage owner's identity when they applied for it in a way that follows the Money Laundering Regulations 2017.

You've found evidence of these payments by looking at printed or online statements that you know belong to the claimed identity.

6.3.3 If the interactions do not happen in a way you'd expect the claimed identity to behave, you'll need to find interactions from over the last 6 months instead.

6.4 Score 4

6.4.1 You'll get a score of 4 if you:

- have evidence of interactions between the claimed identity and an organisation
- know the organisation checked the claimed identity was who they said they were in a way that at least met the requirements of the Money Laundering Regulations 2017
- know the organisation compared the claimed identity to an image from an authoritative source

6.4.2 You'll need to find at least one interaction from the last 3 months.

Example
You've seen that the claimed identity has been on an international flight in the last 3 months. You know their identity was checked when they crossed the border. They would've shown their passport to a border officer, who would've checked it was genuine. The border officer would also have checked the person matched the photo on their passport.

7.0 Check if the claimed identity is at high risk of identity fraud ('identity fraud')

7.0.1 This part of the identity checking process was previously known as 'Element D'.

7.0.2 You should make sure the claimed identity is not at a higher than usual risk of identity fraud or likely to be synthetic.

7.0.3 You can do this by checking the details of the claimed identity with authoritative counter-fraud data sources, such as a national fraud database.

7.1 Score 1

7.1.1 You'll get a score of 1 if you use an authoritative source to check if the claimed identity has either:

- had its details stolen (even if those details have not been used fraudulently yet)
- been reported as stolen

7.1.2 If either of these things have happened, you must do extra verification checks. For example, you could ask the person to complete more or higher quality knowledge-based verification (KBV) challenges.

7.1.3 You must also use an authoritative source to check if the claimed identity is a known synthetic identity.

7.1.4 If it is, you must reduce these risks by:

- doing additional verification checks
- collecting more evidence of the claimed identity

7.2 Score 2

7.2.1 To get a score of 2 you must do all the checks needed to get a score of 1. You must also use an authoritative source to check that the claimed identity:

- belongs to someone who's still alive
- is known by an organisation that should have a record of that person (for example an Electoral Registration Office in a local authority)
- is at a usual risk of being impersonated (for example a 'politically exposed person' like a politician or judge is at a higher than usual risk of being impersonated)

7.2.3 You must do extra verification checks if any of these things do not apply.

7.3 Score 3

7.3.1 You'll get a score of 3 if you use more than one authoritative source to do all the checks needed to get a score of 2.

7.3.2 The sources must also be ‘independent’, which means they’re either:

- separate from the part of your organisation that checks the person’s identity
- part of a different organisation

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

8.0.1 This part of the identity checking process was previously known as 'Element C'.

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

8.0.3 If you do not do this, you will not know if someone is using evidence that belongs to someone else.

8.1 Score 1

8.1.0.1 The person will get a score of 1 if they can prove they know information that does not change over time ('static' information) that only the claimed identity should know.

8.1.0.2 You should check this by asking the person to answer questions or complete tasks. These are known as 'knowledge-based verification' (KBV) challenges.

Example
You can ask the person to give you a customer reference number that was issued to them when they bought something from your organisation. You can make sure the number was issued to their claimed identity by checking it against your records. This reference number is static because it does not change over time.

8.1.0.3 How many KBV challenges you ask the person to do depends on if they're low, medium or high quality.

8.1.0.4 You should ask the person to complete one of the following:

- 2 low quality KBV challenges
- 4 low quality multiple choice KBV challenges
- 1 medium quality KBV challenge
- 2 medium quality multiple choice KBV challenges
- 1 high quality KBV challenge

8.1.1 Quality rules for KBV challenges

8.1.1.1 KBV challenges should be specific enough to be able to prove that that person is who they say they are.

8.1.1.2 Someone who has stolen a claimed identity's wallet, purse or phone should not be able to complete all of the KBV challenges you ask them to.

8.1.1.3 Low quality KBV challenges must be:

- about the claimed identity
- clear and simple so the person knows exactly what you're asking them
- about something the claimed identity can reasonably be expected to know
- from a source that maintains the integrity of the information the question is based on
- from a source that makes sure the information cannot be misused by the claimed identity (for example the claimed identity should not be able to create false records)

8.1.1.4 Low quality KBV challenges must not:

- be able to be answered with information that's available in the public domain (for example in an open dataset or on a website that anyone can access)
- be able to be answered using information the person has submitted at another point in the identity checking process
- be predictable (the questions and answers should change each time someone goes through your identity checking process)
- have answers that can be easily guessed if you're asking multiple choice questions
- include information that will give the person the answer to another question
- show personal information (unless the person has already submitted it at another point during the identity checking process)

8.1.1.5 Medium quality KBV challenges must meet all the requirements for low quality challenges, as well as:

- come from a source that did its own identity checks on the claimed identity
- share codes, like a one-time password sent to the claimed identity's phone, in a way that means you can be sure they were given to the claimed identity (if you use them)

8.1.1.6 High quality KBV challenges must meet all the requirements for low and medium quality challenges, as well as:

- come from a source that checked the claimed identity was who they said they were in a way that follows the Money Laundering Regulations 2017
- come from a source that makes sure the information cannot be accessed, modified or created by its employees
- come from a source that's separate from your organisation
- come from a source that's regulated by a statutory or independent body
- be based on information that cannot be known or accessed by anyone apart from the claimed identity and their immediate family without breaking the law (for example information that could be found on the dark web should not be used)

8.2 Score 2

8.2.0.1 The person will get a score of 2 if you do one of the following:

- make sure the person physically matches the photo on or associated with the strongest piece of genuine evidence you have of the claimed identity (you can do this in person or remotely)
- make sure the person's biometric information (such as their face or fingerprints) matches biometric information from or associated with the strongest piece of genuine evidence you have of the claimed identity
- ask the person to complete multiple 'dynamic' KBV challenges that only the claimed identity should be able to do

8.2.1 Make sure someone matches the photo in person

8.2.1.1 The person doing the match must:

- have been trained in how to detect impostors by a specialist trainer, such as the Home Office, National Document Fraud Unit or CPNI
- refresh their training at least every 3 years
- have good enough eyesight (with or without prescription lenses) to effectively compare the person to the image

8.2.1.2 When doing the match, you must make sure:

- the person whose identity is being checked is present
- the light conditions are good enough to clearly see the person and the image on the evidence (for example there should be no glare or shadows)
- you are comparing the person to a photo from a genuine piece of evidence
- the photo has not been tampered with

8.2.1.3 The person whose identity is being checked must not:

- be wearing a head covering (unless it's for religious or medical reasons)
- have their eyes closed
- have anything covering their face or eyes (such as shadows or their hair)

8.2.2 Make sure someone matches the photo remotely

8.2.2.1 When doing the match, you must make sure:

- the person whose identity is being checked is present when their image or video is captured (you should not use a scan or an upload from a photo or video feed)
- the image or video has not been intercepted and reused ('replayed')
- you are comparing an image or video of the person to an image or video of a genuine piece of evidence
- the image or video has been shared in a way that prevents it from being tampered with (for example by using a 'man-in-the-middle' attack)

8.2.2.2 If a person is doing the match, they must:

- have been trained in how to detect impostors by a specialist trainer, such as the Home Office, National Document Fraud Unit or CPNI
- refresh their training at least every 3 years
- have good enough eyesight (with or without prescription lenses) to effectively compare the person to the image

8.2.2.3 The image or video of the person must be:

- clear and in focus
- in colour

8.2.2.4 In the image or video, the person must:

- be in clear contrast to the background
- not have 'red eye'
- not wear a head covering (unless it’s for religious or medical reasons)
- not have their eyes closed
- not have anything covering their face or eyes (such as shadows or their hair)

8.2.3 Make sure someone matches biometric information

8.2.3.1 When doing the biometric comparison, you must make sure:

- the number of ‘false matches' and ‘false non-matches' in your system are appropriate for your security and usability needs
- your system matches the person to biometric information that's known to belong the claimed identity (this is known as 'one-to-one verification')

- the biometric information has not been tampered with (if it was taken from a piece of evidence)
- your system can identify if the person's biometric information has been intercepted and reused ('replayed')
- the biometric information has been shared in a way that prevents it from being tampered with
- your system can tell if someone's using an artefact to convince the system they're someone else (known as 'spoofing') - this could mean making sure they're not holding up a photo or playing a recording of someone's else's voice if you're checking a facial or vocal type ('modality') of biometric
- your system confirms that the person is real (known as a 'liveness' test)

Example
If you're checking a fingerprint biometric modality, you can use heart rate sensors to make sure that the person who is providing their fingerprint is alive.

8.2.4 Asking the person to complete dynamic KBV challenges

8.2.4.1 To be 'dynamic', the answers to a KBV challenge must change over time. This will make it harder for impostors using information from things like data breaches to successfully complete the challenge.

8.2.4.2 The KBV challenges must follow the same quality rules that need to be followed to get a score of 1.

8.2.4.3 The KBV challenges must also not be based on information from a single source. An account and a mortgage from the same bank count as different sources if the claimed identity went through a different application process to get each one.

Example
You can make a zero balance transaction into the claimed identity's bank account and attach a reference number (which is valid for a short period of time) to it. This will show up as a code on the claimed identity's bank statement.

The person will need to sign in to the claimed identity's account within the allowed time to get the code. If they give you the correct code, it will prove the person you're dealing with has control of and access to that account. Only the claimed identity should be able to do this.

8.2.4.4 How many KBV challenges you ask the person to complete depends on the quality of the questions. You should ask them to complete one of the following:

- 4 low quality KBV challenges
- 8 low quality multiple choice KBV challenges
- 2 medium quality KBV challenges

- 3 medium quality multiple choice KBV challenges
- 2 high quality KBV challenges
- 2 high quality multiple choice KBV challenges

8.3 Score 3

8.3.0.1 The person will get a score of 3 if you do either of the following in person or remotely:

- make sure they physically match the photo on (or associated with) the strongest piece of genuine evidence you have of the claimed identity
- make sure their biometric information matches biometric information from (or associated with) the strongest piece of genuine evidence you have of the claimed identity

8.3.1 Make sure someone matches a photo in person or remotely

8.3.1.1 The person doing the match must have all the skills and training needed to get a score of 2. They must refresh their training in how to detect impostors every year.

8.3.1.2 The person or system doing the match must do everything needed to check someone matches a photo (in person or remotely) at score 2. You must also make sure:

- your process has a way to identify if someone is wearing a mask, makeup or prosthetics to look like someone else
- their eyes are visible without any glare or reflections (if the person is wearing glasses)

8.3.2 Make sure someone matches biometric information

8.3.2.1 You must do everything needed to check someone matches biometric information at score 2. You must also make sure:

- the number of 'false matches' and 'false non-matches' in your system are appropriate for your security and usability needs and are based on industry best practice (for example ISO/IEC TR 29156:2015)
- your system uses a biometric algorithm that's been proven to be effective against a recognised benchmark, like the National Institute of Standards and Technology's (NIST's) face recognition vendor test guidance

- the person’s biometric information is captured under conditions that do not reduce the accuracy of the type of biometric check being used (things like light, noise, and humidity impact the success rates for different biometric modalities and should be adjusted if needed)
- your system can tell when someone's spoofing the system using an artefact that's taken time, money and effort to create, for example detecting if someone is changing the pitch and adding background noise to a recording of a vocal biometric
- your system uses multiple processes or measures to confirm that the person is real (known as an ‘enhanced liveness' test)

Example
If you’re checking a facial biometric modality, you can ask the person to take a short video of themselves, during which they repeat a random sequence of words back to you. This helps you make sure there's a real person involved. You can also continually assess small movements of the person’s head while the biometric measurement is taking place.

8.4 Score 4

8.4.1 The person will get a score of 4 if you make sure their biometric information matches biometric information from (or associated with) the strongest piece of genuine evidence you have.

8.4.2 The system doing the match must do everything needed to check someone matches biometric information at score 3.

8.4.3 It must also be able to tell when someone's spoofing the system using a sophisticated artefact that's taken a lot of time, money, effort or criminal activity to create. If you're checking a facial biometric modality, this could mean making sure the person is not showing a 3D animated avatar on a hijacked computer or device.

8.4.4 The biometric information on the evidence and the biometric information of the person must also be captured under 'controlled conditions'. This means:

- any equipment has been designed in a way that makes it difficult to be tampered with
- someone who was trained in how to compare people to their identity evidence by a specialist trainer (such as the Home Office, National Document Fraud Unit or CPNI) supervises how the biometric information is captured
- the supervisor refreshes their training every year
- the supervisor monitors the behaviour of the person who's biometric information is being captured to make sure it's not suspicious

- the area and equipment used to capture the biometric information has been designed in a way that reduces the likelihood of incorrect matches for the type of biometric information being used

Example
Some facial recognition software will be less accurate in different light conditions. A facial biometric comparison should take place under the best light conditions for the biometric algorithm that's being used. This will reduce incorrect matches and false rejections.

The area where the check is being done should also be monitored by trained personnel who make sure people are not trying to fool the system.

9.0 Identity profiles

9.0.1 Each part of the identity checking process will protect you or your service against different identity risks.

9.0.2 There are a number of ways to combine parts of the identity checking process to meet a level of confidence in an identity. These combinations are known as identity profiles.

9.0.3 Each identity profile will give you one of the following levels of confidence:

- low confidence
- medium confidence
- high confidence
- very high confidence

9.0.4 You can only meet a level of confidence if you meet an identity profile. The higher the level of confidence an identity profile meets, the more protection you or your service will have.

9.0.5 An identity profile is made up of scores for each part of the identity checking process. To meet an identity profile, you must have all these required scores. You can use a score that's the same or higher than the score needed.

Example
You need a validity score of 1 to meet an identity profile. The evidence from the person whose identity you're checking has a validity score of 2. You can use this score of 2 to meet the lower score requirements of the identity profile.

9.0.6 You can choose to meet any identity profile. The identity profile you choose might depend on:

- how confident you need to be in someone's identity
- what evidence your users are likely to have
- which parts of the identity checking process you can do
- how thoroughly you do each part of the identity checking process
- how many pieces of evidence you need

9.0.7 Meeting an identity profile and reaching a level of confidence will mean:

- you know how well your service is protected against identity risks
- your identity checking process can be understood and reused by other organisations or services

9.0.8 If you collect evidence from a user that does not include all the personal information you need, you will need to collect other evidence that does. You'll also need to link these pieces of evidence together to make sure they all relate to the claimed identity.

Example
You need evidence of a person’s name and address. A person gives you a bus pass that shows their photo and address but not their name. They also give you a genuine passport that shows their photo and their name. You check these photos match, so you know both pieces of evidence relate to the same claimed identity.

9.0.9 If you collect more than one piece of evidence, you must make sure the evidence has been issued by either:

- different organisations
- an organisation that used a different identity checking process to issue each piece of evidence you're using

Example
You collect 3 pieces of evidence of a claimed identity from different organisations. One is a letter from a local authority, one is from a solicitor and one is from a gas company. They were all issued to the same claimed identity.

9.1 Low confidence in the person’s identity

9.1.0.1 Compared to not doing any identity checks, having low confidence in the person's identity will lower the risk of you accepting either:

- synthetic identities
- impostors who are not close friends or family of the identity they’re pretending to be

9.1.1 If you have 1 piece of evidence

9.1.1.0.1 There are 3 identity profiles you can meet if you collect 1 piece of evidence.

9.1.1.1 Low confidence, 1 piece of evidence, profile A (L1A)

Check	Score
Strength	2
Validity	2
Activity	Not needed
Identity fraud	2
Verification	1

9.1.1.1.1 By meeting this identity profile, you will:

- know that evidence of the claimed identity exists
- know if the evidence is genuine or valid
- have made sure you or your service have reduced the risks of any known identity fraud associated with the claimed identity
- be confident the person going through the identity checking process knows things that only the claimed identity should know

9.1.1.1.2 You do not need to do an activity check because you know the organisation that issued the evidence already did basic checks to make sure the claimed identity exists in the real world.

9.1.1.2 Low confidence, 1 piece of evidence, profile B (L1B)

Check	Score
Strength	3
Validity	2
Activity	Not needed
Identity fraud	Not needed

Verification	3

9.1.1.2.1 By meeting this identity profile, you will:

- know that strong evidence of the claimed identity exists
- know if the evidence is genuine or valid
- be confident the person matches either the photo or biometric information that's shown on the evidence

9.1.1.2.2 You do not need to do:

- an activity check because the organisation that issued the evidence did multiple checks to make sure the claimed identity exists in the real world
- an identity fraud check because the person going through the identity checking process has been matched to the claimed identity through a physical or biometric comparison

9.1.1.3 Low confidence, 1 piece of evidence, profile C (L1C)

Check	**Score**
Strength	3
Validity	3
Activity	Not needed
Identity fraud	1
Verification	2

9.1.1.3.1 By meeting this identity profile, you will:

- know that strong evidence of the claimed identity exists
- know the evidence is genuine and valid
- have made sure you or your service have reduced the risks of any known identity fraud associated with the claimed identity
- have checked the person going through the identity checking process matches the photo or biometric information that's shown on the evidence, or know they can complete challenges that only the claimed identity should be able to do

9.1.1.3.2 You do not need to do an activity check because you know the organisation that issued the evidence already did multiple checks to make sure the claimed identity exists in the real world.

9.1.2 If you have 3 pieces of evidence

9.1.2.0.1 There's only one identity profile you can meet if you collect 3 pieces of evidence.

9.1.2.1 Low confidence, 3 pieces of evidence, profile A (L3A)

Check	Score (first piece of evidence)	Score (second piece of evidence)	Score (third piece of evidence)
Strength	1	1	1
Validity	1	1	1

Check	Score
Activity	3
Identity fraud	2
Verification	2

9.1.2.1.1 By meeting this identity profile, you will:

- know each piece of evidence appears to be genuine
- be confident that the claimed identity exists in the real world
- have made sure you or your service have reduced the risks of any known identity fraud associated with the claimed identity
- have checked the person going through the identity checking process matches the photo or biometric information that's shown on the evidence, or know they can complete challenges that only the claimed identity should be able to do

9.1.2.1.2 You'll need to collect multiple pieces of evidence because the evidence you have does not have many security features that stop it being forged or counterfeit.

9.2 Medium confidence in the person’s identity

9.2.0.1 Compared to low confidence, having medium confidence in the person's identity will lower the risk of you:

- accepting synthetic identities
- accepting impostors who are not close friends or family of the identity they're pretending to be
- accepting impostors who do not look like the identity they're pretending to be

9.2.0.2 Medium confidence also provides some protection against accepting impostors who are close friends or family of the identity they're pretending to be.

9.2.1 If you have 1 piece of evidence

9.2.1.0.1 There are 2 identity profiles you can meet if you collect 1 piece of evidence.

9.2.1.1 Medium confidence, 1 piece of evidence, profile A (M1A)

Check	Score
Strength	4
Validity	3
Activity	Not needed
Identity fraud	1
Verification	3

9.2.1.1.1 By meeting this identity profile, you will:

- know that very strong evidence of the claimed identity exists
- know the evidence is genuine and valid
- have checked the claimed identity exists in the real world
- have made sure you or your service have reduced the risks of any known identity fraud associated with the claimed identity
- be confident the person going through the identity checking process matches either the photo or biometric information that's shown on the evidence

9.2.1.1.2 You do not need to do an activity check because you know the organisation that issued the evidence already did multiple checks to make sure the claimed identity exists in the real world.

9.2.1.2 Medium confidence, 1 piece of evidence, profile B (M1B)

Check	Score
Strength	3
Validity	3
Activity	2
Identity fraud	1
Verification	3

9.2.1.2.1 By meeting this identity profile, you will:

- have strong evidence that shows the claimed identity exists
- know the evidence is genuine and valid
- have records that the claimed identity exists in the real world
- have made sure you or your service have reduced the risks of any known identity fraud associated with the claimed identity
- be confident the person going through the identity checking process matches either the photo or biometric information that's shown on the evidence

9.2.2 If you have 2 pieces of evidence

9.2.2.0.1 There are 4 identity profiles you can meet if you collect 2 pieces of evidence.

9.2.2.1 Medium confidence, 2 pieces of evidence, profile A (M2A)

Check	Score (first piece of evidence)	Score (second piece of evidence)
Strength	2	2
Validity	2	2

Check	Score
Activity	3

Identity fraud	1
Verification	3

9.2.2.1.1 By meeting this identity profile, you will:

- have more than one piece of evidence that shows the claimed identity exists
- know the evidence is genuine or valid
- be confident that the claimed identity exists in the real world
- have made sure you or your service have reduced the risks of any known identity fraud associated with the claimed identity
- be confident the person going through the identity checking process matches either the photo or biometric information on the evidence

9.2.2.2 Medium confidence, 2 pieces of evidence, profile B (M2B)

Check	**Score (first piece of evidence)**	**Score (second piece of evidence)**
Strength	3	2
Validity	3	2

Check	**Score**
Activity	2
Identity fraud	2
Verification	2

9.2.2.2.1 By meeting this identity profile, you will:

- have strong evidence that shows the claimed identity exists
- have another piece of evidence that shows the claimed identity exists
- know the evidence is genuine, valid or both
- have records that the claimed identity exists in the real world
- have made sure you or your service have reduced the risks of any known identity fraud associated with the claimed identity

- have checked the person going through the identity checking process matches the photo or biometric information that's shown on the evidence, or know they can complete challenges that only the claimed identity should be able to do

9.2.2.3 Medium confidence, 2 pieces of evidence, profile C (M2C)

Check	Score (first piece of evidence)	Score (second piece of evidence)
Strength	3	2
Validity	3	2

Check	Score
Activity	2
Identity fraud	1
Verification	3

9.2.2.3.1 By meeting this identity profile, you will:

- have strong evidence that shows the claimed identity exists
- have another piece of evidence that shows the claimed identity exists
- know the evidence is genuine, valid or both
- have checked the claimed identity exists in the real world
- have made sure you or your service have reduced the risks of any known identity fraud associated with the claimed identity
- be confident the person going through the identity checking process matches either the photo or biometric information that's shown on the evidence

9.2.2.4 Medium confidence, 2 pieces of evidence, profile D (M2D)

Check	Score (first piece of evidence)	Score (second piece of evidence)
Strength	4	2
Validity	3	2

Check	Score
Activity	Not needed
Identity fraud	2
Verification	2

9.2.2.4.1 By meeting this identity profile, you will:

- have very strong evidence that shows the claimed identity exists
- have another piece of evidence that shows the claimed identity exists
- know the evidence is genuine, valid or both
- have checked the claimed identity exists in the real world
- have made sure you or your service have reduced the risks of any known identity fraud associated with the claimed identity
- have checked the person going through the identity checking process matches the photo or biometric information that's shown on the evidence, or know they can complete challenges that only the claimed identity should be able to do

9.2.2.4.2 You do not need to do an activity check because you know the organisation that issued the evidence already did multiple checks to make sure the claimed identity exists in the real world.

9.2.3 If you have 3 pieces of evidence

9.2.3.0.1 There's only one identity profile you can meet if you collect 3 pieces of evidence.

9.2.3.1 Medium confidence, 3 pieces of evidence, profile A (M3A)

Check	Score (first piece of evidence)	Score (second piece of evidence)	Score (third piece of evidence)
Strength	2	2	2
Validity	2	2	2

Check	Score

Activity	2
Identity fraud	2
Verification	2

9.2.3.1.1 By meeting this identity profile, you will:

- have multiple pieces of evidence that show the claimed identity exists
- know each piece of evidence is genuine or valid
- have records that the claimed identity exists in the real world
- have made sure you or your service have reduced the risks of any known identity fraud associated with the claimed identity
- have checked the person going through the identity checking process matches the photo or biometric information that's shown on the evidence, or know they can complete challenges that only the claimed identity should be able to do

9.3 High confidence in the person's identity

9.3.0.1 Compared to medium confidence, having high confidence in the person's identity will lower the risk of you:

- accepting synthetic identities
- accepting impostors who know the identity (including close friends or family)
- accepting impostors who do not know the identity
- being targeted by people who do not look like the identity

9.3.1 If you have 1 piece of evidence

9.3.0.1 There are 2 identity profiles you can meet if the person gives you 1 piece of evidence.

9.3.1.1 High confidence, 1 piece of evidence, profile A (H1A)

Check	**Score**
Strength	4

Validity	3
Activity	Not needed
Identity fraud	3
Verification	3

9.3.1.1.1 By meeting this identity profile, you will:

- have very strong evidence that shows the claimed identity exists
- know the evidence is genuine and valid
- have made sure you or your service have reduced the risks of any known identity fraud associated with the claimed identity
- be confident the person matches either the photo or biometric information that's shown on the evidence

9.3.1.1.2 You do not need to do an activity check because you know the organisation that issued the evidence did multiple thorough checks to make sure the claimed identity exists in the real world.

9.3.1.2 High confidence, 1 piece of evidence, profile B (H1B)

Check	**Score**
Strength	4
Validity	4
Activity	Not needed
Identity fraud	Not needed
Verification	3

9.3.1.2.1 By meeting this identity profile, you will:

- have very strong evidence that shows the claimed identity exists
- know the evidence is genuine and valid
- be confident the person matches either the photo or biometric information that's shown on the evidence

9.3.1.2.2 You do not need to do:

- an identity fraud check as the person going through the identity checking process is unlikely to be someone else (you'll know this because they've been matched to the claimed identity through a physical or biometric comparison)
- an activity check because the organisation that issued the evidence did multiple thorough checks to make sure the claimed identity exists in the real world

9.3.2 If you have 2 pieces of evidence

9.3.2.0.1 There are 3 identity profiles you can meet if you collect 2 pieces of evidence.

9.3.2.1 High confidence, 2 pieces of evidence, profile A (H2A)

Check	**Score (first piece of evidence)**	**Score (second piece of evidence)**
Strength	3	3
Validity	3	3

Check	**Score**
Activity	3
Identity fraud	2
Verification	3

9.3.2.1.1 By meeting this identity profile, you will:

- have more than one piece of strong evidence that shows the claimed identity exists
- know both pieces of evidence are genuine and valid
- be confident that the claimed identity exists in the real world
- have made sure you or your service have reduced the risks of any known identity fraud associated with the claimed identity
- be confident the person matches either the photo or biometric information that's shown on the evidence

9.3.2.2 High confidence, 2 pieces of evidence, profile B (H2B)

Check	Score (first piece of evidence)	Score (second piece of evidence)
Strength	4	3
Validity	3	3

Check	Score
Activity	Not needed
Identity fraud	2
Verification	3

9.3.2.2.1 By meeting this identity profile, you will:

- have very strong evidence that shows the claimed identity exists
- have another piece of strong evidence that shows the claimed identity exists
- know both pieces of evidence are genuine and valid
- have made sure you or your service have reduced the risks of any known identity fraud associated with the claimed identity
- be confident the person matches either the photo or biometric information that's shown on the evidence

9.3.2.2.2 You will not need to do an activity check because the organisation that issued the evidence did multiple thorough checks to make sure the claimed identity exists in the real world.

9.3.2.3 High confidence, 2 pieces of evidence, profile C (H2C)

Check	Score (first piece of evidence)	Score (second piece of evidence)
Strength	4	2
Validity	3	2

Check	Score
Activity	2
Identity fraud	2
Verification	3

9.3.2.3.1 By meeting this identity profile, you will:

- have very strong evidence that shows the claimed identity exists
- have another piece of evidence that shows the claimed identity exists
- know the evidence is genuine, valid or both
- be confident that the claimed identity exists in the real world
- have made sure you or your service have reduced the risks of any known identity fraud associated with the claimed identity
- be confident the person matches either the photo or biometric information that's shown on the evidence

9.3.3 If you have 3 pieces of evidence

9.3.3.0.1 There's only one identity profile you can meet if you collect 3 pieces of evidence.

9.3.3.1 High confidence, 3 pieces of evidence, profile A (H3A)

Check	Score (first piece of evidence)	Score (second piece of evidence)	Score (third piece of evidence)
Strength	3	2	2
Validity	3	2	2

Check	Score
Activity	3
Identity fraud	3
Verification	3

9.3.3.1.1 By meeting this identity profile, you will:

- have strong evidence that shows the claimed identity exists
- have more than one other piece of evidence that shows the claimed identity exists
- know the evidence is genuine, valid or both
- be confident that the claimed identity exists in the real world
- have made sure you or your service have reduced the risks of any known identity fraud associated with the claimed identity
- be confident the person matches either the photo or biometric information that's shown on the evidence

9.4 Very high confidence in the person's identity

9.4.0.1 Very high confidence makes it very difficult for someone to:

- use a synthetic identity
- impersonate someone without breaking the law

9.4.1 If you have 1 piece of evidence

9.4.1.0.1 There's only one identity profile you can meet if you collect 1 piece of evidence.

9.4.1.1 Very high confidence, 1 piece of evidence, profile A (V1A)

Check	Score
Strength	4
Validity	4
Activity	4
Identity fraud	3
Verification	4

9.4.1.1.1 By meeting this identity profile, you will:

- have very strong evidence that shows the claimed identity exists

- know the evidence is genuine and valid
- be very confident that the claimed identity exists in the real world
- have made sure you or your service have reduced the risks of any known identity fraud associated with the claimed identity
- be confident the person's biometric information matches what's shown on the evidence

9.4.1.1.2 You'll have been as thorough as possible with all parts of the identity checking process so you only need one piece of evidence.

9.4.2 If you have 2 pieces of evidence

9.4.2.0.1 There are 2 identity profiles you can meet if you collect 2 pieces of evidence.

9.4.2.1 Very high confidence, 2 pieces of evidence, profile A (V2A)

Check	Score (first piece of evidence)	Score (second piece of evidence)
Strength	4	4
Validity	4	4

Check	Score
Activity	N/A
Identity fraud	2
Verification	4

9.4.2.1.1 By meeting this identity profile, you will:

- have more than one piece of very strong evidence that shows the claimed identity exists
- know the evidence is genuine and valid
- have made sure you or your service have reduced the risks of any known identity fraud associated with the claimed identity
- be confident the person's biometric information matches what's shown on the evidence

9.4.2.1.2 This means the organisation that issued the evidence did multiple thorough checks to make sure the claimed identity exists in the real world (so you do not need to do an activity check).

9.4.2.2 Very high confidence, 2 pieces of evidence, profile B (V2B)

Check	Score (first piece of evidence)	Score (second piece of evidence)
Strength	4	3
Validity	4	3

Check	Score
Activity	2
Identity fraud	3
Verification	4

9.4.2.2.1 By meeting this identity profile, you will:

- have very strong evidence that shows the claimed identity exists
- have another piece of strong evidence that shows the claimed identity exists
- know the evidence is genuine and valid
- have records that the claimed identity exists in the real world
- have made sure you or your service have reduced the risks of any known identity fraud associated with the claimed identity
- be confident the person's biometric information matches what's shown on the evidence

9.4.3 If you have 3 pieces of evidence

9.4.3.0.1 There's only one identity profile you can meet if you have 3 pieces of evidence.

9.4.3.1 Very high confidence, 3 pieces of evidence, profile A (V3A)

Check	Score (first piece of evidence)	Score (second piece of evidence)	Score (third piece of evidence)
Strength	4	3	3
Validity	4	3	3

Check	Score
Activity	1
Identity fraud	2
Verification	4

9.4.3.1.1 By meeting this identity profile, you will:

- have very strong evidence that shows the claimed identity exists
- have more than one other piece of strong evidence that shows the claimed identity exists
- know the evidence is genuine and valid
- have checked the claimed identity exists in the real world
- have made sure you or your service have reduced the risks of any known identity fraud associated with the claimed identity
- be confident the person's biometric information matches what's shown on the evidence

9.4.3.1.2 You can do weaker activity and identity fraud checks because you have multiple pieces of evidence that were issued by organisations that checked the claimed identity exists in the real world.