



Home Office

UKVI Identity Standards

Version 5.0

Contents

Contents.....	2
About this guidance	4
In this guidance.....	4
Contacts	4
Publication.....	5
Changes from last version of this guidance	5
Introduction	6
What is an identity.....	6
Why confidence about an identity matters	6
Quick guide: Identity Standards guidance	7
What you must be satisfied about	7
The core identity standards process	7
Best evidence of identity.....	7
If a valid passport is not available	8
Entry clearance and in-country applications	8
Decision making.....	8
The identity standard	9
The process for establishing, fixing and assuring an identity.....	9
Required standard	9
How a person establishes their identity	11
Fixing an identity.....	12
Biometrics	12
Original documents.....	12
Generic Identity Document Verification (GIDV) app	12
Other information.....	13
Results from biometric checks	13
Using information from background checks.....	13
Other supporting evidence	14
Assuring an identity	15
Assess the evidence obtained.....	15
Validate documents and evidence.....	15
Match the person to the document.....	16
Consider background and intelligence checks.....	16
DNA and biological relationships.....	17
Evidence from sponsors and other parties.....	17

Weighing up the evidence	17
Determining an identity.....	19
Satisfied.....	19
Not satisfied	19
Insufficient evidence	19
Deception	19

About this guidance

This guidance tells you about the identity requirements which must be met by a person during their immigration and citizenship journey.

This guidance is primarily for:

- Immigration, nationality and asylum decision makers, and enrichment officers
- Entry Clearance Decision Makers (ECDM), also referred to as Entry Clearance Officers (ECO)
- any official making a decision on behalf of the Secretary of State

This guidance also applies to any official responsible for establishing, fixing, verifying or assuring a person's identity, including administrative and enrichment staff where those functions form part of their role.

Border Force and Immigration Enforcement officers must be aware of this guidance to understand the basis of a person's identity.

There is specific identity guidance for nationality decision makers who are considering applications for registration or naturalisation as a British citizen, however the standards set out in this document will otherwise also apply to such cases.

The identity requirements described in this guidance do not apply to British citizens or holders of a certificate of entitlement to the right of abode, who are not subject to immigration control. It does apply to British nationals who are subject to control.

In this guidance

'Decision maker' means:

- immigration, nationality and asylum decision makers; other officers responsible for registering and processing asylum claims; and enrichment officers

'People / person' means:

- applicants, claimants, individuals, and dependants

Contacts

If you have any questions about the guidance and your line manager or senior decision maker cannot help you, or you think that the guidance has factual errors, then email the Identity Security Team.

If you notice any formatting errors in this guidance (broken links, spelling mistakes and so on) or have any comments about the layout or navigability of the guidance then you can email the Guidance Rules and Forms team.

Publication

Below is information on when this version of the guidance was published:

- version **5.0**
- published for Home Office staff on **xx October 2026**

Changes from last version of this guidance

There are significant changes from the previous guidance, including:

- new definition for identity standards
- new sections on how an identity is established, fixed and assured and determined

Related content

[Contents](#)

Introduction

The Home Office must be satisfied about a person's identity before granting permission to come to, enter or stay in the UK. Identity assurance underpins effective immigration control, safeguarding, and national security checks. This guidance explains what an identity is, the identity standard that must be met, and the process for establishing, fixing and assuring an identity. It recognises there are legitimate reasons why some people may not have official identity documents and supports a proportionate, evidence-based approach. Definitions of different forms of identity documents (including passports, travel documents, expired documents and unrecognised passports) are set out in the [Identity Standards glossary](#).

What is an identity

An identity is the combination of biographic information and biometric information that uniquely identifies a person. Biographic information includes name, date of birth, place of birth, nationality and other life events such as marriage. Biometric information, for the purposes of this guidance, is facial image and fingerprints.

The Government Digital Service [Good Practice Guide 45 \(GPG45\)](#) provides the overarching framework for building confidence that a person is who they claim to be. In an immigration context, this includes securely linking a person's claimed identity to them through biometrics collected during the application or enrolment process. Decision makers should use GPG45 alongside this guidance to understand how identity is established, fixed and assured.

Why confidence about an identity matters

Being confident about a person's identity is essential to support accurate background, security and suitability checks, protect the integrity of the immigration system, and ensure lawful and defensible decision making. This also supports the secure link between the person, their Home Office record and any identity product issued (for example, an eVisa), which underpins access to services and entitlements where applicable.

This is distinct from biometric enrolment or application stage verification alone, as biometrics do not, by themselves, confirm an identity. Decision makers must be satisfied that the claimed biographic identity can be credibly and reliably linked to the biometrics of the person presenting it. Without this confidence, harmful people may avoid detection, vulnerable people may not receive protection, and Home Office records and decisions risk becoming unreliable.

Related content

[Contents](#)

Related external links

Identity Standards glossary

[Good Practice Guide 45 \(GPG45\)](#)

Quick guide: Identity Standards guidance

This quick guide outlines the identity assessment requirements for immigration applications. This is intended as high-level reference for decision makers and **must** be read with the relevant sections in the full guidance.

What you must be satisfied about

In non-protection cases, before a person can be granted permission, you must be satisfied on a balance of probabilities the claimed identity exists, belongs to the person, and has been reliably linked to them. This means considering the evidence and not relying on one document in isolation. Just because a decision maker does not suspect deception, this does not automatically mean that the claimed identity is true. The less evidence provided, or the weaker the evidence provided is, the lower the assurance rating of that identity.

In protection, including asylum and humanitarian protection claims, a person may not have documents. For asylum claims, you must decide whether the claimed identity is more likely than not to be true, taking into account all the evidence. For humanitarian protection claims, relevant aspects of identity (in particular nationality) may be assessed to the lower standard of a reasonable degree of likelihood, where appropriate.

The core identity standards process

Identity is normally assessed in 3 connected stages:

- the person **establishes** their identity by providing information and evidence
- the claimed identity is **fixed** through biometrics and document scans and checks carried out under controlled conditions
- the decision maker **assures** the identity by weighing all the evidence, checks, and any inconsistencies

Best evidence of identity

A valid national passport will usually provide the strongest evidence, especially where it is issued by a recognised authority and can be checked reliably, for example through a readable chip and document integrity checks. Some documents provide lower assurance, either because their security features cannot be fully checked or because they do not securely link the identity to the holder. See Identity Document Assurance Framework. EEA or Swiss citizens applying under the EU Settlement Scheme (EUSS), or under Family and Private Life entry clearance, permission to stay and settlement routes, may use a valid national identity card instead of a passport.

If a valid passport is not available

Where a person cannot reasonably provide a valid passport, an explanation must be provided. You must consider whether they have given a satisfactory explanation and whether alternative or corroborative evidence, together with biometric checks, Home Office records, and other controlled checks, is enough to establish identity to the required standard. Where the explanation is accepted, you must record that the Secretary of State's discretion has been exercised and briefly explain the reasons for doing so.

Entry clearance and in-country applications

Entry clearance and in-country applications may be made through several different immigration routes, but the identity standards remain the same. Be alert to impostors, age discrepancy cases, and false, altered or fraudulently obtained documents. If significant doubts remain, you cannot be satisfied as to the identity.

Decision making

To make a full assessment and come to a decision you must use the full guidance. You must record clear reasons for your decision with reference to the evidence. If significant doubts remain and cannot be resolved, you cannot be satisfied as to the identity. For decision letter wording, see Identity standards decision letter example wording. For asylum cases, requests for further information must follow established asylum processes.

Related content

[Contents](#)

Identity Standards glossary

Identity Document Assurance Framework

Identity Standards In-country and out of country applications

Identity Standards Impostor and Age Discrepancy Cases

Identity standards decision letter example wording

The identity standard

You must be satisfied about a person's identity before that person can be granted permission to come to, enter or stay in the UK. This section explains what being satisfied about a person's identity means.

The process for establishing, fixing and assuring an identity

An identity needs to be established by the person, fixed by providing their biometrics and original identity documents under controlled conditions, and then assured by a decision maker. The diagram below sets out the stages that enable an identity to be established and assured. These stages are supported by core Home Office casework systems (including Proviso, Atlas and PEGA) that capture, verify and assess identity information. Responsibilities for checks and recording outcomes vary by flow where AUK1 is completed by the decision maker, and AUK2 uses PRS (for key words used in this guidance see the Identity Standards glossary).

Required standard

A decision maker must check all the information provided by a person and consider any other available information (making reasonable requests for further information if required) of a person's identity before their application or claim can be decided. The person is responsible for substantiating who they are and for showing their claimed identity is genuine. In most cases, this will happen when a person provides a valid national passport and enrolls their biometrics under supervised conditions, enabling secure checks to be made.

When considering the person's identity, the decision maker must consider the totality of the evidence provided by the person. In particular, the decision maker must be satisfied that:

- the identity belongs to the person, who is a living person
- any identification documents, such as passports, relate to the person and are capable of authentication
- documentary evidence provided in support of the application contains reliable biographic information
- they can link the person to those documents, including any facial image or other biometric link
- any other supporting evidence, including family, community or institutional corroboration, is reliable

No single piece of evidence is determinative, and the weight given to any item depends on its source, integrity, resistance to alteration, and consistency with the evidence as a whole. Where a person lacks strong documentary evidence, they must demonstrate their identity through alternative means, including responding to any reasonable requests from the decision maker. The decision maker must be satisfied that the claimed identity is more likely than not to be true. **A decision maker might**

not suspect deception, however, that does not automatically imply that the claimed identity is true.

In applying the required standard, decision makers must be satisfied that the evidence belongs to, and reasonably matches, the person's appearance (including through biographic details and biometric links where available), and consider whether alternative evidence provides sufficient assurance where no valid identity documents are available. Just because a person produces identification documentation does not automatically mean they will have satisfied a decision maker about their claimed identity, especially where the evidence is self-certified or cannot be assured. Any material that appears to be contradictory or presents adverse information must be identified, assessed and weighed, and the overall judgment must be based on the totality of the evidence, giving appropriate weight to higher assurance, verifiable information. For the method and detailed checks to apply these principles, see [Assuring an identity](#).

Related content

[Contents](#)

Related external links

Identity Standards glossary

How a person establishes their identity

This section explains what a person needs to do to establish their identity.

People are responsible for establishing their identity and must provide reliable information and evidence to support their claimed identity and nationality. People are normally expected to provide a valid passport or identity card. What counts as valid and the assurance strength of different documents is set out in Identity Document Assurance Framework. High assurance documents, such as ePassports that contain a readable chip, can be reliably verified and authenticated which will usually (but not necessarily) evidence identity satisfactorily. Other documents may provide lower assurance where security features cannot be easily checked (such as unrecognised passports) or lack any reliable biometric link to the holder (such as birth certificates).

Decision makers must consider the assurance of all available evidence, including both documentary evidence (for example, identity documents and supporting or corroborative documents) and the outcomes of controlled checks. They must also consider consistency with the person's account and whether further checks are needed. Where a person lacks a sufficiently assured document, identity may be strengthened through alternative or corroborative evidence and controlled checks such as tri-scan images (see Identity Standards glossary) and biometric enrolment. Where a person is reasonably unable to obtain a valid passport, this must be explained and assessed in line with the UKVI Identity Standards Policy.

Related content

[Contents](#)

Identity Standards glossary

Identity Document Assurance Framework

Fixing an identity

Fixing an identity means securely linking the claimed identity to the person, so the information cannot be manipulated or changed without notifying the decision maker. This is primarily achieved through the enrolment of biometrics and the controlled capture of original documents which are linked to an identity in Home Office systems via the relevant caseworking system. Where biometrics have not been enrolled, decision makers must take steps to identify and, where appropriate, merge linked records across relevant systems.

Biometrics

People must enrol their biometrics in line with the relevant application process, unless exempt or excused as set out in the Biometric information: enrolment guidance (see that guidance for where it does and does not apply). Enrolling biometrics acts as a critical safeguard because it ensures that a person is uniquely identifiable, prevents identities from being reused or duplicated, and enables the identity to be reliably checked across systems.

Original documents

Where original identity documents are provided, they must be scanned or checked under controlled conditions to ensure that security features can be properly examined, including for passports, tri-scanning where available. This reduces the risk of tampering or substitution, protects personal data, and preserves the evidential integrity of identity evidence relied upon in decision making. Documents that are self-uploaded under uncontrolled conditions or poor-quality copies are not sufficient to fix an identity and their authenticity and integrity cannot be reliably verified. Such documents may prevent security features from being examined properly and do not provide the same assurance that the document can be securely linked to the person presenting it and their biometrics.

Generic Identity Document Verification (GIDV) app

The use of digital identity verification tools, including the GIDV app where applicable, supports biometric enrolment and document capture but does not remove the need for decision makers to assess all the information available and therefore be satisfied with the identity on a balance of probabilities. Although, in most cases where a person has successfully used the GIDV app, including completing any 'liveness' checks, that will usually provide satisfactory evidence of their identity. Detailed biometric and document handling processes (including where they differ for applications made from outside or inside the UK) are set out in Identity Standards In-country and out of country applications.

Related content

[Contents](#)

Biometric information: enrolment

Identity Standards In-country and out of country applications

Other information

This section sets out how to use other information available to the Home Office to support identity assessment. This includes results from biometric checks, information from background checks, and other supporting evidence that may corroborate or contradict the identity being claimed. You must consider this information alongside the person's documents and account, and give it appropriate weight based on its source, accuracy and relevance. You must also consider whether there is evidence the claimed identity has previously been present in the UK (for example, a previous grant of permission).

Results from biometric checks

Checks against Immigration and Asylum Biometric System (IABS) and IDENT1, the police series of fingerprint databases, and matches under international biometric data sharing processes may reveal previous applications, identities, or encounters recorded within Home Office systems. Information obtained can support identity assessment and highlight inconsistencies. Decision makers must use this information to check whether the results are relevant to the application they are considering. For example, if fingerprint checks show a previous application made under a different name or date of birth, this may raise questions about the person's identity that must be explored and resolved before a decision is made.

Using information from background checks

Background checks can provide information relevant to identity and credibility, including results from watch-listing systems, intelligence and forgery reports, and country information on passport and identity document issuing processes. This information may corroborate, contradict or undermine other evidence and assist in assessing plausibility, document integrity, and known risks. Watchlist checks may identify matches against domestic or international systems, intelligence and forgery reports may highlight concerns about document integrity or known risks, and country information can explain how passports and identity documents are issued, managed, and secured. Appropriate weight must be given to this information based on its accuracy, source, relevance, and context. It must not be treated as determinative on its own. For example, information about insecure passport issuing processes may undermine the value of the information contained in the passport.

Official – sensitive: start of section

The information on this page has been removed as it is restricted for internal Home Office use.

The information on this page has been removed as it is restricted for internal Home Office use.

Official – sensitive: end of section

Other supporting evidence

The application or claim is a primary source of information about identity and personal history. Consistency within the account, and with other evidence, is relevant to assessment. Any discrepancies must be examined carefully.

DNA evidence may support a claimed biological relationship where relevant, but it does not establish identity on its own. See [DNA and biological relationships](#) in Assuring an identity section.

An interview may be one of the options to clarify information and explore inconsistencies. Responses must be assessed for detail, consistency, and plausibility. When an interview is conducted any evidence must be considered alongside all other material.

Information from sponsors or other corroborative sources may support aspects of an application or claim. The reliability and relevance of such information must be assessed carefully and must be weighed alongside all other available evidence.

Related content

[Contents](#)

Assuring an identity

This section sets out the practical method for applying the principles in [Required standard](#). How identity information is captured, verified and assessed will depend on where and how an application or claim is made, for example at a Visa Application Centre (VAC) or at a Service and Support Centre, or on arrival at the border or when claiming asylum in any other circumstances). The core systems where decision makers may view, verify and assess identity information across Home Office operations are Proviso, Atlas and PEGA, each providing specific tools and functionality that contribute to establishing, fixing and assuring identity in line with this guidance. Different officials are responsible for different aspects of identity assessment, and their involvement will vary at different stages of a person's immigration journey. Assuring an identity involves assessing, validating and weighing all available evidence to decide whether you are satisfied that the claimed identity is the identity of the person.

In the case of an asylum claim, the person's identity will be established as far as practicable at the earliest opportunity, usually at registration; however, a decision is not made on the application at that point, and so it will be at a later time when an asylum decision-maker finally assures the identity to the appropriate standard.

Assess the evidence obtained

The decision maker must consider all evidence obtained during the application or claim process, including documentary, biometric, biographical, background, and intelligence information.

Validate documents and evidence

Where identity documents are provided, the decision maker must take reasonable steps to validate them using available systems and checks. The decision maker does not need to check every system in every case. However, checks on internal systems that fall within the Operating Mandate must be completed in every case. Additional checks using other tools, such as [EdisonTD](#) and [PRADO](#), (See Identity Standard glossary for further information), may be appropriate where there are concerns about a document or other indicators of risk. For example:

- the document looks unusual, damaged, or low quality
- details do not match other information (for example name, date of birth, nationality, or travel history)
- there is a known risk or fraud trend for that document type or route
- the decision maker thinks the document could be lost, stolen, or used by someone else

If the decision maker cannot access a tool, they must follow the local process to ask for the check. Checking documents against these databases can help decision makers to determine whether documents appear genuine, valid, and consistent with the claimed identity.

Official – sensitive: start of section

The information on this page has been removed as it is restricted for internal Home Office use.

Official – sensitive: end of section

Match the person to the document

The decision maker must assess whether the person presenting the identity appears to match the document provided. This includes considering:

- whether the person resembles the photograph in the document
- whether the biographic details recorded on the document, including age and appearance are consistent with the person presenting it

If the person does not reasonably match the document, this may indicate that the document is not genuine, or has been tampered with, or that a genuine document is being presented by an impostor (someone using another person's identity). Apparent age discrepancies must be explored and may require further checks or explanation. They do not, on their own, prove that the claimed identity is false. In the assessment of age discrepancy cases, the decision maker must consider the suggestions set out in Identity Standards Impostor and Age Discrepancy Cases.

Biometric checks confirm that a person is physically present. On their own, they do not prove the person's claimed identity. In some cases, such as where biometrics or identities have been reused, they may only show that it is the same person, and not that the identity they claim is correct. Biometric results must therefore be considered alongside other evidence.

Consider background and intelligence checks

The decision maker must consider whether background, security, or intelligence checks provide information that supports or contradicts the claimed identity. This includes:

- whether checks reveal contra-indicators, such as previous identities, aliases, or inconsistent biographical details
- whether there is information suggesting the person may be using a different identity or misrepresenting their circumstances
- whether any document they have used was reported lost, stolen or whether they could have obtained fraudulently obtained documents

Any adverse or conflicting information must be considered as part of the overall assessment.

Decision makers who are reviewing supporting documents as part of their consideration of suitability and eligibility may encounter evidence that contradicts the claimed identity.

DNA and biological relationships

Where a person has chosen to provide DNA evidence, the decision maker must consider whether the results support the claimed biological relationship or undermines the credibility of the claimed identity or family relationship. DNA evidence should be assessed alongside all other evidence and does not automatically determine the outcome. For example, while the evidence may prove a biological relationship it does not mean the claimed biographical information is accurate. More information about the DNA policy can be found in the DNA policy guidance.

Evidence from sponsors and other parties

The decision maker must consider whether sponsors or other people have provided evidence that supports the claimed identity, or contradicts the person's account, or other evidence on file. Any information that conflicts with the application must be looked at carefully and assessed to decide how reliable and relevant it is.

The decision maker must check whether the application or claim matches the identity being claimed. This includes checking whether family relationships and ages seem reasonable, and whether the account, documents, and background information fit together. This may include records from any application or claim made by the sponsor. Differences or gaps in the information do not automatically mean the identity is false, but they can reduce confidence in the identity if they are not clearly explained.

Weighing up the evidence

To weigh the evidence, decision makers must consider all identity evidence together and decide how much confidence it gives that the person is who they claim to be. When weighing the evidence, decision makers must consider how reliable and secure each piece of evidence is, whether it is consistent with the person's account and other information held, and whether it can be clearly linked to the person, for example through biographic or biometric details. If some evidence is weak or missing, this does not automatically mean that identity cannot be assured. Decision makers must consider whether the identity can be strengthened using other evidence or checks, in line with this guidance.

However, just because a person provides numerous pieces of evidence does not automatically mean that the claimed identity is assured. Documentary evidence must be assessed alongside the wider evidence for the identity and must satisfy the decision-maker that on the balance of probabilities that the claimed identity is genuine.

Related content

[Contents](#)

Related external links

[EdisonTD](#)

[PRADO](#)

[DISCS](#)

[Interpol i24/7](#)

Identity Standards glossary

Identity Standards Impostor and Age Discrepancy Cases

DNA policy guidance

Determining an identity

This section explains what a decision maker must do when they have decided whether they are satisfied with the claimed identity of the person.

Satisfied

If you are satisfied with the claimed identity, you must proceed to conduct all relevant suitability and eligibility checks in line with the Immigration Rules and guidance (see Operating Mandate UK Visas and Immigration). However, be aware that further information may come to light that could undermine the claimed identity, which may require the decision maker to review the application.

Not satisfied

If you are not satisfied with the claimed identity, you must consider the reason why and take the appropriate next steps, as set out below.

Insufficient evidence

If there is insufficient evidence to satisfy you about the claimed identity, but there are no indicators of deception, you must consider whether it is appropriate to write and request further evidence or clarification before making a decision. Where appropriate, you must also consider whether an interview is needed to clarify gaps, test consistency, or resolve discrepancies in the evidence. This is to allow the person to satisfy you about their identity before a decision is made. Example decision letter wording (including requesting further evidence and 'not satisfied' outcomes) is provided in Identity standards decision letter example wording. Just because a person is not seeking to use deception, there may be situations where the person simply lacks sufficient evidence to satisfy you about their identity. In protection claims, a lack of identity documentation evidence does not automatically make a claim invalid or result in refusal; a risk-based assessment is required in all cases. See the asylum guidance in Considering and deciding a claim, in particular, Assessing Credibility and Refugee Status.

Deception

Where an identity discrepancy cannot be resolved through the checks in this guidance, you must consider whether the person has used deception to obtain, or attempt to obtain, an immigration status. This includes providing false or misleading identity information such as inconsistent biographical details, conflicting dates of birth (including significant unexplained age discrepancies), incorrect or unverifiable documents, the use of an impostor identity (presenting a genuine document that belongs to someone else), use of false documents including counterfeit, forged or fraudulently obtained genuine documents, or the omission of relevant identity information.

You must assess whether the evidence shows deliberate dishonesty before applying the relevant suitability provisions of the Immigration Rules (where those provisions are applicable). For the EU Settlement Scheme (EUSS), identity deception or fraud is a validity issue as the identity requirement is not met. Whether the application is rejected or refused depends on the route under which the person has applied.

Where it is considered that deception may have occurred, you must follow the relevant guidance on document verification and Suitability: false representations, deception, false documents, non-disclosure of relevant facts (not applicable to the EUSS).

Related content

[Contents](#)

Related external links

Identity Standards decision letter example wording

Document verification

Suitability: false representations, deception, false documents, non-disclosure of relevant facts