



Home Office

# Identity Standards: Applications for entry clearance, permission to stay and settlement

Version 1.0

Identity standards for applications made in the UK and outside the UK.

# Contents

|                                                                     |    |
|---------------------------------------------------------------------|----|
| Contents.....                                                       | 2  |
| About this guidance .....                                           | 3  |
| Contacts .....                                                      | 3  |
| Publication.....                                                    | 3  |
| Changes from last version of this guidance .....                    | 4  |
| Introduction .....                                                  | 5  |
| Entry clearance applications (outside of the UK) .....              | 6  |
| Entry clearance – satisfactory explanation .....                    | 7  |
| Entry clearance – alternative acceptable documents .....            | 7  |
| Permission to remain applications (in the UK).....                  | 9  |
| Access UK1 (AUK1) .....                                             | 9  |
| Biometric Enrolment Centres (VAC / SSC) .....                       | 9  |
| Resolve Identity Service (RIS).....                                 | 9  |
| ID Operations (ID Ops) .....                                        | 9  |
| Decision maker (Atlas).....                                         | 10 |
| PEGA (EU Settlement Scheme (EUSS)) .....                            | 10 |
| Access UK2 (AUK2) .....                                             | 10 |
| Identity reuse via customer account.....                            | 10 |
| Person Resolution Service (PRS) .....                               | 11 |
| Visa Application Centre (VAC) (for VAC Integration flow only) ..... | 11 |
| Decision maker (Atlas casework).....                                | 11 |
| Satisfactory explanation (In-country).....                          | 11 |
| Alternative acceptable documents (In-country) .....                 | 12 |

# About this guidance

This guidance explains the identity standards that must be applied when considering in-country and out-of-country UKVI applications. It sets out who is responsible for establishing, fixing and assuring identity, and what decision makers must do where identity cannot be confirmed through a passport, travel document, biometrics or existing Home Office records.

This guidance is primarily for:

- Immigration, nationality and asylum decision makers and caseworkers
- 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

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

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. The guidance also applies to other types of British nationals who are subject to control.

**Decision maker** means immigration, nationality, asylum decision maker, Entry Clearance decision maker, or another official making a decision on behalf of the Secretary of State.

**People / person** means applicants, claimants, individuals, and dependants.

## Contacts

If you have any questions about the guidance and your line manager or senior caseworker 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 **1.0**
- published for Home Office staff on **22 October 2026**

## Changes from last version of this guidance

This is new guidance.

### Related content

[Contents](#)

# Introduction

The identity standard is the same whether the person is applying from overseas or within the UK.

What changes is:

- the systems used
- what happens if identity cannot be accepted (for example, rejection or refusal)

In most in-country applications, the person's identity will have been established through earlier Home Office processes (for example, a previous grant of entry clearance / permission and biometric enrolment) and the case will normally reach the decision maker with an accepted identity record. In these cases, the decision maker only needs to take further action if something is flagged or missing. Where identity has not previously been established (for example, asylum claims, including those from clandestine arrivals, or other routes where the person has no prior record), the decision maker must take the steps needed to establish, fix and assure identity before deciding the application. In entry clearance applications the responsibility of fixing and assuring the person's identity lies with the decision maker.

## **Related content**

[Contents](#)

# Entry clearance applications (outside of the UK)

All people applying for entry clearance are required to submit a visa application form online. Once this has been completed, most people are required to attend a Visa Application Centre (VAC) where they will provide their biometrics (fingerprints and a facial image). If the person holds a passport or travel document, the biometric data page will be scanned by the supplier before being returned to the person.

---

## **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**

If the person does not possess a valid passport or travel document, you must consider alternative documents and consider whether the evidence provided satisfactorily establishes their nationality and identity.

If biometrics were captured, you must then review the results to establish whether they reveal any concerns about the person's identity. Concerns may arise where the person has previously provided biometrics in a different identity, particularly when this identity has not been disclosed. However, you must be mindful of instances where a person's identity has changed for legitimate reasons (for example, name changes due to marriage). When considering the application, you must also refer to this guidance if you have other concerns about the person's identity.

## Entry clearance – satisfactory explanation

A satisfactory explanation is needed if the person cannot provide a valid passport or travel document. A valid passport or travel document remains the normal expectation for entry clearance applications across all routes. Where a passport has been lost or stolen, people would normally be expected to obtain a replacement from the issuing authority. Unlike in in-country cases for further immigration permission, where the Home Office will have previously fixed a person's identity, people applying from overseas may not have a previously established Home Office identity record.

People on some routes may be less likely to hold one due to their circumstances. Examples may include:

- there is no functioning or accessible issuing authority, or it is not safe or reasonable to contact one
- the application is made under a route where access to documents is limited, such as:
  - crisis or resettlement routes

You must assess whether the explanation is reasonable for the route and circumstances and record your decision on the system.

## Entry clearance – alternative acceptable documents

Alternative documents can be considered only where valid passport or travel document is not available, and a satisfactory explanation has been provided.

Possible alternatives (not exhaustive) include:

- a recently expired passport or travel document (with supporting evidence)
- a national identity card (where applicable)
- civil registration documents (for example, birth certificate) as supporting evidence only
- other government-issued documents that can be independently checked

---

### 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

You must refer cases where you intend to accept alternative documents to an Entry Clearance Manager or a Technical Specialist for approval.

At present, the only route that routinely accepts expired passports is the British Nationals (Overseas) (BN(O)) indefinite leave to remain route. This applies to only BN(O) and Hong Kong Special Administrative Region (HKSAR) passport holders,

and only where the passport expired no more than 5 years before the date of application.

**Related content**

[Contents](#)

# Permission to remain applications (in the UK)

Most immigration applications made within the UK are processed through one of the following digital platforms: Access UK 1 (AUK 1) and Access UK 2 (AUK2). The operational processes described below relate primarily to those platforms. Some routes, including asylum and other protection-based processes, use different systems and workflows. However, the same identity principles apply; decision makers must establish, fix and assure identity using all available evidence before making a decision. For further information see the Identity Standards glossary.

## Access UK1 (AUK1)

The applicant submits their application through AUK1 for routes such as further leave to remain, settlement, fee waivers, or Changes of Circumstances. When required under the validity rules, they attend a biometric enrolment appointment at either a Service and Support Centre (SSC) (for Family & Human Rights applications) or a VAC for all other eligible AUK1 routes. However, some routes using the AUK1 form, such as the EU Settlement Scheme (EUSS), do not always require applicants to attend a VAC as, in some circumstances, identity verification is completed by UKVI caseworkers. The applicant will also provide identity and supporting documents.

Once biometrics have been enrolled, the following have varying responsibilities for the person's identity.

## Biometric Enrolment Centres (VAC / SSC)

Biometric Enrolment Centres (VAC / SSC) capture people's biometric data (facial images and fingerprints) and transmit it into IABS. The information is then used in downstream biometric and case working checks including Atlas and HOPS. They do not verify identity; their role is limited to collecting and transmitting enrolment data.

## Resolve Identity Service (RIS)

The Resolve Identity Service (RIS) is an automation process that carries out identity resolution after biometric enrolment, checking all identity 'islands' to consolidate available information and flag potential issues such as mismatched data or possible mis-merges. It also runs PNC and Home Office database checks, routing any hits to ID Operations for action. RIS feeds identity information into the Consider Task and the Person Summary View but cannot confirm identity. It can only resolve data based on what it receives.

## ID Operations (ID Ops)

ID Operations (ID Ops) step in whenever system checks flag a potential identity concern, enriching the case and assessing whether the hit genuinely relates to the

person. They update records, confirm or clear matches, and ensure any identity concerns are fully resolved. Once their checks are complete, the case returns to standard casework.

## Decision maker (Atlas)

The decision maker in Atlas is the primary owner of identity requirement for AUK1 and begins by reviewing the validity screen when the application is received. They compare the uploaded passport in HOPS with the biographic details in Atlas, alongside historic and enrolment images in the Person Summary View. Through these checks, they detect issues such as mis enrolments or inconsistencies in age, gender, or images. Rather than explicitly 'approving' identity, they confirm it by deciding they meet the requirement to establish, fix, and assure identity because no verification occurs earlier in the AUK1 flow.

## PEGA (EU Settlement Scheme (EUSS))

The PEGA caseworker is responsible for assessing whether identity has been satisfactorily established for EUSS applications made using the AUK1 form. Identity may be verified through documents submitted to UKVI, existing Home Office records and biometric information. Where identity has already been established and there are no concerns, the caseworker may rely on those records. If identity cannot be verified, or concerns remain, the caseworker must take further steps to establish, fix and assure identity before making a decision. Identity assurance remains the responsibility of the decision maker and is based on all available evidence.

## Access UK2 (AUK2)

The person uses AUK2 through one of several routes, such as digital chip checks, biometric reuse, or integration with a visa application centre depending on their circumstances. As part of the process, they upload an identity document, usually a passport or biometric residence permit (BRP), which are no longer issued, and provide a liveness selfie. These steps allow the system to capture and link their identity information for assessment. EUSS applications may be made from within or outside the UK, so caseworkers must follow the relevant route-specific process when considering how identity has been evidenced and verified.

## Identity reuse via customer account

Identity reuse via customer account is when a person's previously assured identity is utilised for subsequent in-country immigration applications, removing the need for repeated verification through physical documents such as an in-date passport or attendance at a VAC or an SSC. This method relies on matching the person's facial image against an assured facial image held on the Immigration and Asylum Biometric System (IABS). Fingerprint biometric information, stored on IABS, will be rechecked against law enforcement fingerprint databases, including the police series of fingerprint databases, IDENT1, in line with the UKVI Operating Mandate (OM). This is to enable decision makers to conduct suitability checks on the person.

## Person Resolution Service (PRS)

The Person Resolution Service (PRS) is the core owner of Operating Mandate (OM) compliance in AUK2, ensuring identity is established, fixed, and assured. For all AUK2 variations, it receives uploaded identity documents and liveness images, carrying out automated and manual verification, including comparisons with historic images in Atlas. If verification fails, PRS requests a new liveness image and, if the identity remains unverifiable, rejects it and routes the case to casework for a decision. By confirming identity before the case reaches a decision maker, PRS removes the need for traditional biographic or document checks in chip-check, biometric-reuse, and identity-reuse flows.

## Visa Application Centre (VAC) (for VAC Integration flow only)

VACs support the VAC Integration flow by enrolling biometrics for people who are not eligible for identity reuse via customer account, including those allowed to enrol without a passport under discretion rules. They capture and provide the biometric data needed for RIS and PRS to continue identity resolution and verification.

## Decision maker (Atlas casework)

In most AUK2 flows, Atlas decision makers do not carry out identity verification because PRS has already completed this step. Their responsibilities vary by flow:

- **Chip Check:** no identity checks required - [PRS](#) already verified
- **Biometric Reuse:** decision makers must check BRP biographics against Atlas records to ensure the person has not changed their personal details
- **VAC Integration:** identity is assured via biometrics and PRS' liveness checking

**Identity Reuse via customer account:** Decision makers do not conduct document-based identity checks unless the details have changed as identity reuse relies on [PRS](#) output and system-presented information. Decision makers must, however, ensure that the identity relates to the same person where there has been a change of name.

## Satisfactory explanation (In-country)

A satisfactory explanation is required where the person cannot provide a valid passport or travel document, and identity cannot be confirmed through existing Home Office records. A valid passport or travel document remains the normal expectation for in-country applications across all routes. Where a passport has been lost or stolen, people would normally be expected to obtain a replacement from the issuing authority.

A satisfactory explanation may include:

- there is no functioning or accessible issuing authority, or it is not safe or reasonable to contact one
- the passport, national identity card, BRP or travel document is held by the Home Office in connection with an existing immigration application or process
- the passport, national identity card or travel document has been lost or stolen and cannot reasonably be replaced
- the person is vulnerable due to age, disability, or long-term residence without travel
- the person has changed their gender and cannot obtain updated identity documents because their country does not recognise the change
- the application is made under a route where access to documents is limited, such as:
  - crisis or resettlement routes
  - stateless persons, trafficking victims, or children in care

## Alternative acceptable documents (In-country)

You can only accept alternative documents where identity cannot be confirmed through reuse or existing records, and the person has provided a satisfactory explanation for not having a valid passport.

These may include:

- previously accepted identity documents
- expired documents (in limited circumstances)
- Home Office records and biometric matches
- supporting documents that link the person to their identity over time

For further information on alternative documents see the Identity document assurance framework.

You must:

- take account of previous identity decisions
- only reassess a previously assured identity where there is good reason to do so, such as where there is new evidence that undermines the asserted identity
- escalate if identity cannot be assured to the required standard

You must refer cases where you intend to accept alternative documents to a Technical Specialist for approval.

### Related content

[Contents](#)

### Related external links

[PRADO](#)

[Edison](#)

[DISCS](#)