CPNI
Centre for the Protection of National Infrastructure

PRE-EMPLOYMENT SCREENING

DOCUMENT VERIFICATION

Edition three: October 2015

Contents

Appendices

Introduction

The aim of this guidance

This document provides guidance to staff within organisations who undertake document verification as part of the Pre-Employment Screening process, in particular those confirming identity or checking supporting documentation as part of Pre-Employment Screening checks. It highlights the main security features present in a number of documents and the main methods used to forge such documents. It should assist staff in the detection of basic forgeries.

However, this guidance will not provide staff with the skills to detect all forgeries, particularly those which have been produced using highly professional and sophisticated techniques. Nor is it intended to replace an organisation's existing document verification process, but rather to provide information on good practice.

Most of the examples in this guidance relate to passports, driving licences and identity cards (including the Biometric Residence Permit). The forgery techniques outlined are relevant to all types of documents e.g. university certificates.

We are grateful for the support and help provided by the National Document Fraud Unit and the Driver and Vehicle Licensing Agency (DVLA) in putting together this guidance. All images are owned and supplied by them.

This document should be read in conjunction with CPNI's *Pre-Employment Screening: a good practice guide*, which can be downloaded from www.cpni.gov.uk.

Document verification

Document verification is the process of ensuring that documents presented by prospective employees are genuine and that the holder is the rightful owner. It is an integral part of the Pre-Employment Screening process. Staff responsible for checking documents should have the knowledge and tools to be able to confirm the authenticity of documents, and identify basic forgeries.

It is important that your document verification processes are integrated within your wider Pre-Employment Screening policies.

Recruitment process

The document verification process should be explained to all applicants as part of the recruitment process (in the application pack or online). It should highlight which documents are requested and why e.g. to guard against identity fraud and forgery. You should stress how important document verification is to your organisation and that you may seek to confirm the authenticity of relevant documentation. This may deter applicants who might apply using forged documentation.

You should also make it clear that applicants who cannot provide the required documentation will not be employed (except for cases where a reasonable explanation can be provided), particularly where their right to work in the UK must be verified.

Training

You should consider the training needs of staff who check documents, i.e.:

- how much knowledge/experience do they already have?
- what sort of training might they require?
- how frequently should this training be refreshed?

You may wish to designate a particular member of staff as the internal 'expert' on document verification. They could be responsible for ensuring all training needs are met, and for monitoring developments in documents and detection techniques. They could also act as the first point of contact for colleagues who raise concerns about any documentation.

You may decide to seek training, either from CPNI or the police (see the chapter on where to get help) or from a private sector supplier. You may also wish to develop your own internal training programme. This may include the opportunity for staff to practise examining documents – such as their own passports or driving licences – to ensure your processes are practicable and understood. You could discuss previous examples of document concern, and how you dealt with the situation.

Take Another Look: ID Verification[1]

This short film highlights the importance of verifying a person's identity and the authenticity of their documents as part of the recruitment process. It also serves as a refresher for those who have undertaken identity and document verification training. If you would like a copy of the film and an accompanying desk-top checklist, please email IDENTITY@cpni.gsi.gov.uk.

Equipment

You should consider whether your processes require the use of verification tools. Both magnifiers and ultraviolet (UV) light sources are easy to obtain and can enhance your ability to detect fraudulent documentation. However, the use of this equipment will only be effective if users have a sound understanding of the document and its safeguards.

Magnifiers – standard handheld magnifying glasses (strength of x8 or greater) can be useful when examining documents for photo substitution (i.e. dirt around the photo or misalignment of safeguards which overlap from the page to the photo), miniprint and microprint (see the next chapter).

UV light sources – hand-held UV lights and desk-top UV lamps are useful tools for determining whether documents and their UV safeguards are genuine.

Document checking

It is essential that all documents are examined thoroughly. Documents must initially be checked in the presence of the individual presenting them; a more detailed check can then be undertaken away from the individual. It may be helpful to design a checklist (see the example at Appendix 2) to ensure all aspects of the document are examined. You may decide that each document will not be 'signed off' until each section of the checklist has been completed.

Light sources

Documents and their security features can be viewed using the following:

- **Oblique light** – light from the side, falling at a shallow angle, which reveals the surface structure of an object through contrasts of light and shade. Can be used to inspect embossing stamps, intaglio printing and latent images (see the next chapter).
- **Transmitted light** – light shining through the object being viewed. The object viewed is placed between the eye and the light source.
- **UV light** – used in document verification to analyse substrate brightness, fluorescence and other features, as well as document tampering.

[1] EVCOM (Event and Visual Communication Association) Screen Awards 2015 – Best Documentary

Concerns

If you have concerns about a document, you should first ensure all other aspects of the document are checked before you take the matter further. You should then seek professional advice on travel documents (see the chapter on where to get help). For other documents, you should contact the originating organisation.

Ideally, you should seek further advice before you return the document to the individual. The advice you receive may be able to resolve the issue. If it is not possible to seek a second opinion, proceed with caution and raise your concerns with the applicant asking them whether they can provide an explanation. You should inform them that you are following standard procedures for the verification of documents. You should not place yourself or any colleagues in any danger.

Scanning or photocopying the relevant documents may be sufficient to conduct further investigations (e.g. concerns with the type face on the biodata page of a passport). However, you may need to ask the applicant to return with the original document which can then be examined by an expert or someone more experienced.

If you are unable to resolve your suspicions, you should not continue with the applicant's recruitment. You should document all your dealings with the applicant (i.e. telephone calls, emails, letters etc.) and other relevant parties.

Security features

The examples of the security features in this section can be found in many passports, identity cards and driving licences issued internationally, but designs will vary.

Substrate security features

A substrate is the material from which the documents are made. Traditionally, the substrate in passports and identity cards has been paper, into which many features have been incorporated to protect the document against counterfeiting and forgery. However, a polycarbonate (hard plastic) substrate can also be used for the biodata page and photocard driving licences and identity cards. Security features contained within the substrate can include:

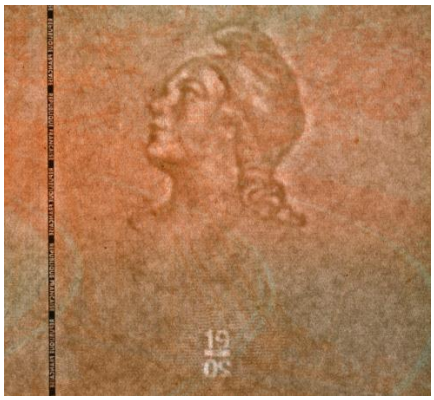
Base fluorescence

Passports and identity cards are made from high quality security paper. This is designed to have a low-base fluorescence (i.e. not react brightly) when exposed to UV light. Lower quality paper (used frequently by forgers and counterfeiters) tends to fluoresce to a greater extent under UV light.

Examples of a genuine (left) and counterfeit (right) Slovakian identity card to show fluorescing of counterfeit substrate

Watermarks

A watermark is created during the manufacture by variations in the thickness of the paper, and can be viewed using transmitted light. A genuine watermark should consist of subtle changes in tone and both lighter and darker areas. It should never react under UV light.



Watermark through transmitted light

Security fibres

Security fibres appear in random patterns across the paper. They can be visible to the naked eye, or fluorescent when exposed to UV light.

Security fibres under normal and UV light source in the UK passport first issued in 2010

Security printing techniques

The printing methods used in a number of documents can also contain a number of security features. These include:

Rainbow printing

Colours are merged subtly into each other, resulting in a gradual colour change.

Miniprint and microprint

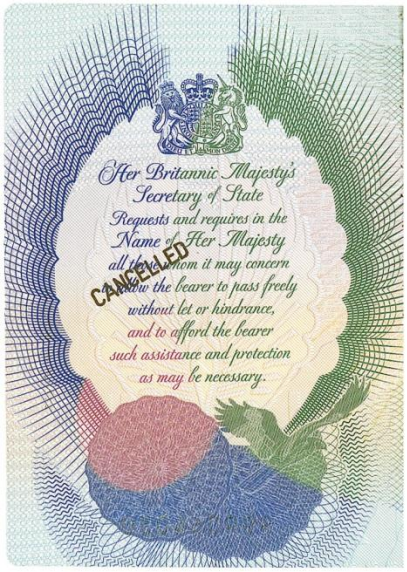
These are lines or motifs consisting of very small letters or numbers that are barely perceptible to the eye. Miniprint may be discerned with the naked eye, but can be viewed more clearly with magnification. Microprint will often require the use of magnification.

Intaglio printing

Intaglio is a printing process which results in the ink having a raised and rough feel which can be felt by running a finger over the paper. Intaglio printing can be found on the inside cover of many passports. It will often include a number of intricate designs and miniprint or microprint.

Latent image

This technique is applied using an intaglio process. The printing technique used means that the pattern can only revealed by viewing the page using oblique light.



Intaglio printing viewed face on (UK passport first issued in 2006)

Latent image (2006 UK passport)

Optically variable ink (OVI)

This is a printing ink containing microscopic pigments which result in strong variations in colour when the document is manoeuvred. OVI can be used in intaglio printing or in images in documents.

See-through registers

These are images printed to create an accurate front-to-back register. Designs or partial motifs are seemingly printed at random on the front and back of the substrate, but they match up perfectly to form a complete motif when light is shown through the substrate.

See-through register featured in the 2010 UK passport

Secondary (ghosted) images

Found in some passports and driving licences, these can be applied using the same printing process for primary facial images or by different processes, for example:

- **Laser perforation** – viewed under transmitted light.
- **Fluorescent overprint** – invisible under normal light but can be viewed under UV light.
- **LetterScreen** – the image is made up of a microprint such as the owner's name, date of birth or document number.

Example of LetterScreen on the observations page of the 2010 UK passport

Gold blocking

Gold blocking consists of a real gold leaf stamped hard into the cover of the passport. Genuine gold blocking will be of high quality and fine detail. When assessing gold blocking it is important to proceed with caution as the gold blocking in older passports can fade due to wear and tear. In general, gold blocking in recently issued passports should be less faded. Potentially suspicious gold blocking is not conclusive. However, it should prompt closer inspection of the rest of the document.

Laser perforated designs

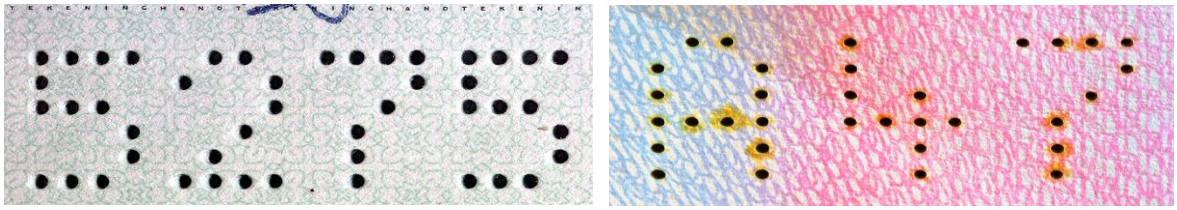
On some passports, there are very fine laser perforated designs which can be seen by holding the biodata page up to the light. This feature, known as DestriPerf®, can be seen on the editions of the UK passport first issued in 1998 and 2006, for example.

Two photos of DestriPerf® on the biodata page of the UK passport first issued in 2006 – the one on the left is face on, the one the right is using transmitted light

Needle and laser perforation

In many passports, the serial number is perforated through the substrate. This is achieved by one of the following methods:

- **Needle perforation** – a regular, matrix-type arrangement of circular, equal sized holes. Ridges can be felt on the reverse of the substrate.
- **Laser perforation** – where a laser is fired through the substrate. Typical features of laser perforation include:
  - traces of burning around the holes;
  - the size of the holes decreases when the passport is viewed from the front to the back;
  - the designs of the holes can include different shapes.



Examples of needle perforation (left) and laser perforation (right)

Optical variable devices (OVDs)

OVDs are iridescent images that exhibit various optical effects such as movement or colour changes. They cannot be copied or scanned, nor can they be replicated or reproduced to a high standard. Two common types of OVDs are holograms and Kinegrams®.

Kinegrams® are rich in colour and contain fine definition, including extra small print. They must be manoeuvred to be viewed in their entirety.

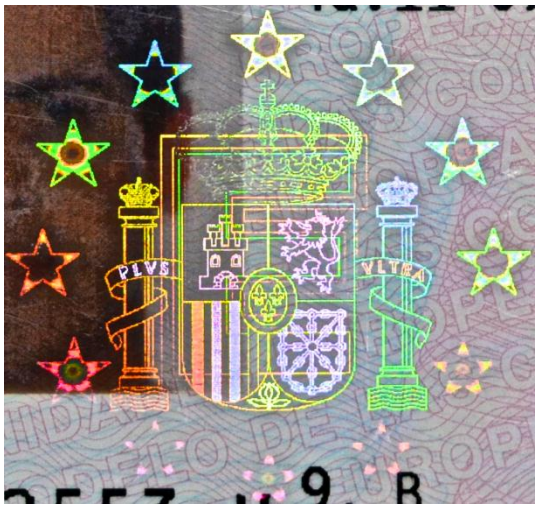


Image of hologram featured on the Spanish driving licence photocard

Lamination

Standard laminate – this is a sheet of clear plastic which can incorporate visible and invisible safeguards.

Laminates with OVDs – examples are all current editions of the UK passport where a clear plastic laminate featuring a transparent OVD protects the holder's digital image and biographical data.

Image of laminate with OVD from the 2010 UK passport

Some laminates include a rip-cut effect – these are weak points incorporated into the laminate. The laminate will rip if it is manipulated.

Basic photograph authentication

This refers to any feature added at the time of issue, usually as a means of deterring the removal of the photograph of the holder. An example of this is an embossed stamp (dry seal).

Image of embossed stamp

UV light

Most passports and identity documents contain safeguards which can only be seen with a UV light. UV features have become more sophisticated with each new issue of passport, travel document, driving licence etc., and random fibres will often fluoresce under UV light. Care should be taken as these safeguards can be simulated. However, if they are missing altogether it is likely that something is wrong with the document.

Fluorescent features visible under UV light include:

- **Security fibres** – see above;
- **Ink** – used to print both text and motifs;
- **Overprint** – seen on many laminates in passports on the biographical data page and on identity cards and driving licences, typically covering the holder's photograph and personal information to protect against manipulation. Not to be confused with fluorescent ink;
- **Planchettes** – small coloured discs mixed into the substrate during manufacture. Can also be viewed under normal light;
- **Security thread** – a thin strip of plastic, metallic or other material embedded or partially embedded in the substrate during manufacture;
- **Stitching thread** – used to hold the pages of a passport together.

UV overprint on the laminate covering the biodata page in the 2010 UK passport

Page numbering

When inspecting a passport, you should check that none of the pages is missing, and the page numbers run in sequence. In passports, the page numbers can be viewed in background print, watermarks and under UV light.

Optical character recognition (OCR)

Many passports internationally contain a series of machine readable characters on two rows along the length of the biodata page of the passport. The font used for these characters is defined by the International Civil Aviation Organisation (ICAO). This font has a number of distinct attributes. For example, the number 'three' has a flat, as opposed to a curved, top line and the number 'four' has a broken vertical line. A check of these two digits on any passport should help to identify any potential concerns.

0123456789
ABCDEFGHI
JKLMNOPQR
STUVWXYZ <

OCR character set

Biometrics

Biometric details enable an individual's unique identity to be recorded. There are a number of physiological features which are unique to an individual and can be used to provide a person's identity. Biometric identifiers include facial image, fingerprints or iris recognition. Although biometrics cannot completely protect documents against fraud, they help make passports harder to forge or counterfeit.

The UK has issued biometric passports (also known as ePassports) since 2006. These measure 125mm by 88mm, and comply with ICAO standards and EU common format requirements. The standard issue passport contains 32 pages and the business passport 48 pages, and will normally be valid for ten years. Passports issued to children under 16 are valid for five years.

The ICAO specified symbol on the front cover of the passport signifies that the passport contains a biometric chip. In UK passports the chip contains the personal details and an image of the passport holder. The chip may contain biometric details (i.e. image of the iris or fingerprints) of the holder in other passports.

Images of the UK biometric passport (also known as ePassport) first issued in 2006 – visa pages under UV light and normal light (left), and biodata page under transmitted light (right). The biometric chip can be seen on the reverse of the page.

Visas

Visas are secure documents in themselves and should have a similar standard of security as passports. They contain many of the features found in passports e.g. rainbow printing, holograms and Kinegrams®, latent and UV images. Printing designs and security features on visas issued in the EU are broadly similar.

Example of a UK visa (vignette) under normal light (left) and UV light (right)

Biometric residence permits (BRP)

BRPs are issued to all migrants from outside the European Economic Area and Switzerland who have been granted permission to stay in the UK for more than six months. All holders aged six and above are required to provide their biometrics. These will be a digital photograph and scans of all ten fingerprints (applicants under six are not required to provide fingerprints).

The features of the BRP are uniform across all EU member states. These include: rainbow printing, microprint, laser-engraved personalisation, OVI, Kinegram®, UV light and a lenticular device (where alternate images can be viewed from different angles).

Front of the BRP under normal (left) and UV light (right)

OVI on the front of the BRP

Lenticular device on the rear of the BRP

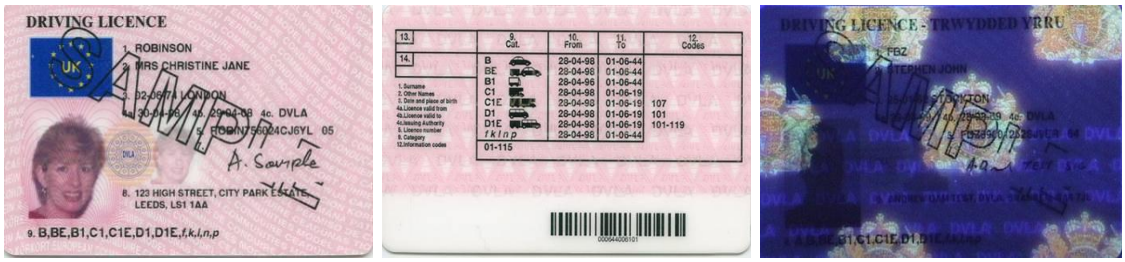
Other forms of identification

Identity cards and driving licences often contain some of the security features found in passports.

The Cypriot identity card below, introduced in February 2015, contains security features including: high quality rainbow printing, a digital image, an OVD, OVIs, a lenticular device and tactile (raised) features. Further security features can be viewed under UV examination.

Cypriot identity card (first issued 2015) under normal (left) and UV light (right)

The various issues of the UK photocard driving licence feature similar security features including: high quality background printing, extra small print, digital images, holograms, tactile features and OVIs. Again, further security features can be viewed under UV examination.



UK driving licence photocard first issued in 1998

UK driving licence photocard first issued in 2007

UK driving licence photocard first issued in 2014

Document fraud

Document fraud can be conducted in a number of ways. This section shows how fraud takes place and how it can be detected. The majority of examples of fraudulent documents relate to passport fraud.

The main types of fraud are:

- **Imposters** – where the holder of the document may look like the rightful owner.
- **Counterfeit** – a document made from scratch.
- **Forgery** – a genuine document which has been altered.

Imposters

This is the simplest type of document fraud, where the 'holder' is simply a look-a-like, and the document is often not altered at all. To guard against imposters you should:

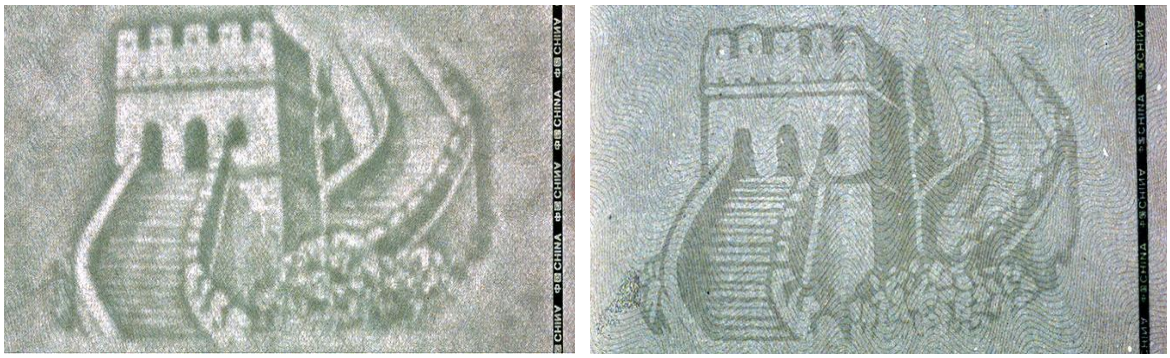
- ascertain the age of the person (using the date of birth in the document, if provided), and compare that with the person presenting the document. It can be difficult to gauge a person's age from their appearance; it is important to consider that people may have aged as much as ten years since their photo was taken. You should therefore proceed with caution;
- compare the photograph in the document with the applicant – pay particular attention to the eyes, nose, lips, chin, ears, and any visible scars, marks etc. This must be done in the presence of the applicant;
- compare as much of the data contained in the document with other information you have on the applicant;
- compare the signature in the document with one provided elsewhere by the applicant e.g. on their application form.

Counterfeits

A counterfeit document is one that has been made from scratch to resemble an officially issued document. The quality of counterfeits can vary greatly. High quality counterfeits can be difficult to identify, however the information below may help to identify counterfeits of lesser quality.

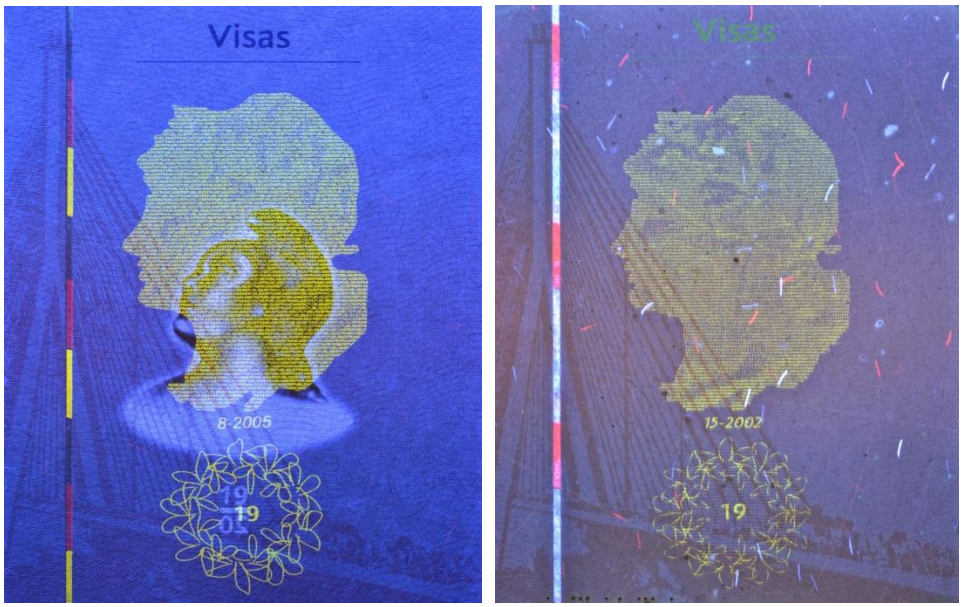
Watermarks

By holding the document up to the light you should be able to identify the watermark. A genuine watermark has subtle variations in the light and dark areas, unlike many counterfeit watermarks.



Example of a genuine (left) and counterfeit (right) watermark

A genuine watermark should **never** react under UV light. However, chemically simulated watermarks are likely to fluoresce.



Counterfeit watermark (left), viewed with UV light. A genuine watermark should not fluoresce (right) – see also the image on page 7

Intaglio and latent image

A relatively easy detection point for a counterfeit document may be the absence of intaglio print and a latent image which are often found on the inside cover of genuine travel documents. In a counterfeit document, attempts to replicate the intaglio may create a waxy feel unlike the rough surface of the genuine document. It may also lack detail.

In a counterfeit document there may be no attempt to simulate any latent image (see page 9). You can check this by holding the page where the latent image should be at an angle.

Printing

Genuine travel documents are manufactured on large scale security printing presses using high quality, solid colour print processes and are deliberately complex to make copying difficult. Counterfeits are often produced using colour copies or other scanning devices - this is likely to

produce jagged edges compared to the solid lines of background print in a genuine document. Ink-jet printers cannot replicate the smooth transition between colours created by rainbow background print.

The quality of printing can be assessed using magnification – for instance the printing in a counterfeit document may lack intricate designs, without solid and clearly defined lines and shapes.

Examples of background printing on a genuine (left) and counterfeit (right) German identity card

Gold blocking

Compare the quality and fine detail of the genuine gold blocking with the counterfeit below.

Examples of genuine (left) and counterfeit (right) gold blocking on a Portuguese passport

Forged documents

A forged document is a genuine document which has been altered in some way. Photos and personal details are common examples but pages, visas and stamps may also be forged. The main types of forgery are covered below.

Page substitution

A document will often be dismantled in order to substitute a page used to:

- remove an incriminating endorsement;
- benefit from a visa, stamp or residence permit;
- change a photograph, image or personal details.

Genuine pages from another passport or counterfeit pages may be inserted into a document. The biographical data page is substituted in many forged passports.

Covers and endpapers

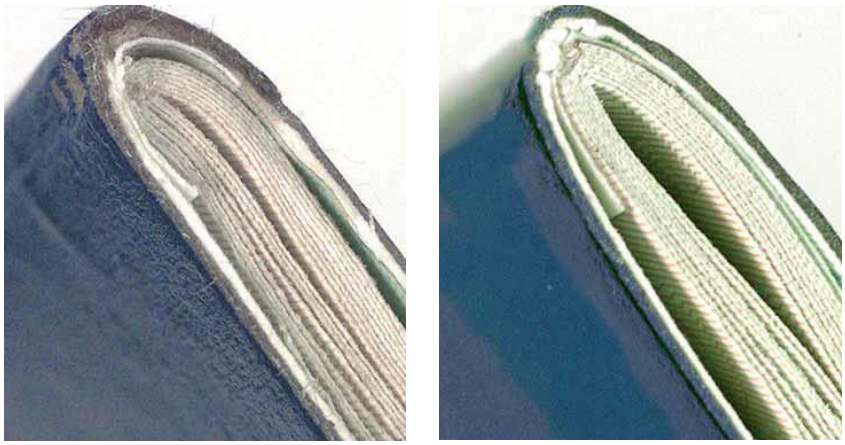
To dismantle a passport one or both of the endpapers must be removed to access the reverse of the stitching. Allowances should be made for wear and tear, but any localised damage or wrinkling to the endpapers or covers should be treated with suspicion.

Example of wrinkled endpaper

Alignment

Pages are trimmed to a standard size and should therefore align exactly. In a forgery the pages may be misaligned due to the poor reassembly of the document. The pages may not align with the spine and the endpaper may have separated from the cover. The document may not close cleanly.

Photo shows poor alignment of pages when passport is closed

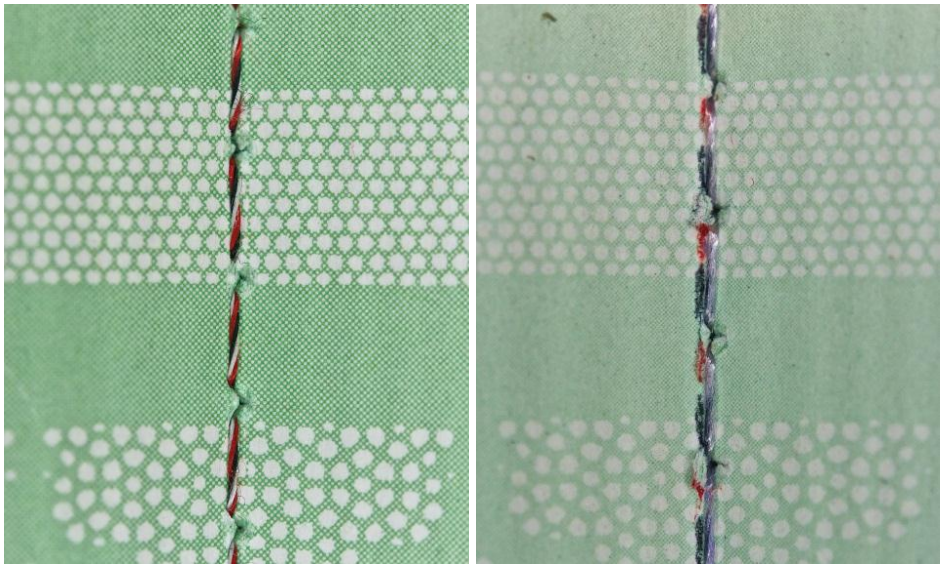


Photos showing misaligned pages indicating poor assembly (left) and a genuine document (right)

Stitching

Stitching should appear evenly in passports. The thread will be stitched tightly, and should not be loose or broken. Passports which have been dismantled to remove pages may contain empty stitch holes where the original thread used to be.

In many passports, the stitching will fluoresce under UV light. Again, the colours should be continuous and not appear broken. If the original thread is replaced, it is unlikely to fluoresce in the same colour scheme.



Photos of original stitching (left) and tampered stitching (right) from a Pakistan passport

Photograph substitution

Forgers involved in photo-substitution may decide to leave biographical details unchanged, resulting in a possible mismatch between the holder and the profile in the document. They may also alter the biographical details to match the profile of the holder.

The main methods of substituting a photograph are outlined below:

Lifted laminate method – where the laminate is lifted from the biographical data page and the photograph is substituted. Few signs of damage to the document may be visible, but the main detection points are:

- damage or degradation to the laminate safeguards, including holograms and UV;
- creases or air bubbles in the laminate;
- extraneous material beneath the laminate;
- disturbed paper fibres or damage to the paper fibres beneath the laminate;
- misalignment of the substitute photograph.

Damage to the laminate from the lifted laminate method seen under oblique light

Window method – where a window is cut in the laminate on the photograph page and the original photograph is replaced. A new laminate is fixed over the page to conceal the damage. Main detection points include:

- damage to, or lack or, safeguards such as holograms or ink stamps over the photograph area;
- UV features stop where the laminate covering the photograph has been cut away;
- misalignment or damage to any stamps and embosses covering the photograph. Counterfeit stamps and embosses may lack fine detail.

Window method showing damage to safeguards

Photos showing misalignment (left) and spelling errors in embossed stamps (right)

Split page method – where the page containing the photograph is split along its edge or the photo page is split away from the cover. Once split the photograph can be accessed from behind. The main detection points are:

- the cover may not be firmly affixed to its endpaper;
- damage to the paper may be visible around the edge of the page or photograph;
- damage to safeguards covering the photograph.

Whichever photo substitution method is used, an unusually large photograph may be used to conceal damage to the area where the original photograph was positioned.

Digital image substitution

Modern passports, identity cards and driving licences are usually printed with the holder's personal details digitally printed directly onto the substrate, and use digital images rather than photographs. The main ways to substitute a digital image include:

Partial digital image substitution – where the actual face has been removed and the new holder's face is inserted; however the original hair and shoulders remain. The new image often lacks the clarity of the shoulders and hair which are likely to be of a higher resolution.

When cutting takes place to remove the image, cut marks in the page may become apparent when the page is viewed with the use of indirect (reflected) light.

Whole digital image substitution – this involves the separation of substrate and laminate. A substrate containing the new image is grafted onto the original substrate and the laminate is re-applied. Main detection points include:

- damage to the biographical data page and laminate;
- the additional paper adds thickness to the page;
- the area has a high base fluorescence when exposed to UV light;
- extraneous material beneath the laminate;
- inaccurate, broken or missing laminate pattern and/or safeguard.

Alterations

The following methods might be used to alter details within a document:

Mechanical (abrasion, rubbing, scraping of the substrate) – if a document has been altered mechanically you may see:

- under oblique light – raised fibres in the altered area;
- under transmitted light – paper thinning or thicker areas of paper in the altered area (the forger may have added paper to conceal alteration or paper damage).

Chemical (liquids such as water, solvents or bleach) – if a document has been altered chemically, shrinkage, wrinkling, or damage to the substrate can often be viewed. New details can be typed or hand-written over the area where the original information has been removed. Biographical data should be checked carefully, and you should look for smudging around the written details, or traces of original information which has not been removed fully.

Information which has been altered

Stolen blanks

Genuine documents may be stolen before they are issued and subsequently used by fraudsters. To detect such documents it is important to check the authenticating stamps and the type-written personal details carefully. The black print in-fill on the biodata page is different in a stolen blank to one issued officially (see below).

Genuine (left) and stolen blank (right) print in UK passports

Visas

Substituted visas (those taken out of one document and, after alteration, inserted into another) may display signs of alteration to the passport number or personal and issue details. You should compare the biographical data in the visa with the same information in the passport and application form.

Image or typeface substitution may also occur. The use of transmitted light may reveal paper thinning caused by abrasion when the original image was removed (e.g. by chemical treatment or scraping). Further examination using UV light may show damage to the UV print safeguards.

Spelling mistakes are common as in the stamps below. The red squares highlight the mistakes – 'CHANNEL TRAVEL' should read 'CHANNEL TUNNEL' and 'PUBLIC PONDS' should read 'PUBLIC FUNDS'.

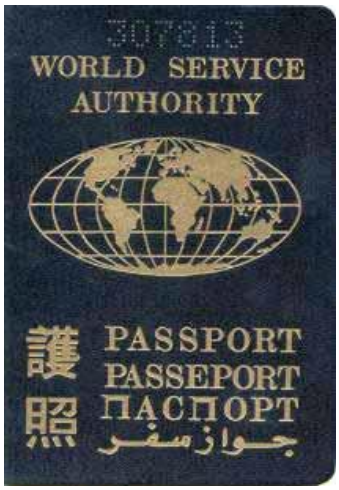
Examples of stamps with spelling mistakes

Alternative passports

Other documents exist purporting to be issued for international travel but which are issued outside the accepted rules and procedures of international practice. Individuals may use these documents when they wish to avoid using a genuine passport using their true identity and nationality. The main types of these documents are:

Camouflage passports – these are unofficial travel documents in the name of non-existent countries which are offered for sale by commercial organisations. A person may purchase a complete kit which can include birth certificates, driving licences etc. Documents can also be issued for countries which are no longer known by their former name e.g. British Honduras (Belize), Ceylon (Sri Lanka) or New Granada (Grenada).

Fantasy passports – these are documents with no authority and which are not officially recognised. They may have the physical appearance of a passport, identity card or driving licence, but are not an acceptable statement of either identity or nationality.



Examples of fantasy documents

Supporting documents

These are documents which support an individual's identity or proof of address, and include utility bills or mortgage statements, for example. Supporting documents are not documents of identity.

Unlike identity documents, supporting documents do not have many security features. Despite the relative ease with which supporting documents can be altered (for example, by the use of modern office equipment), close examination may identify anomalies or inconsistencies which warrant further investigation.

Old style British Gas bill – removal of correct address and new details added

Features which can be examined on supporting documentation include:

- company logos – these can lose their quality when photocopied or scanned as opposed to those printed on original company paper;
- spelling and grammatical errors. Also mathematical errors on bank statements/utility bills;
- changes in font sizes/styles during sentences or paragraphs;
- watermarks, security fibres, embossing, crests, and high quality paper (the latter three are common features of exam and degree certificates);
- many bills and statements are machine folded before being sent to customers.

Top shows an original old style British Gas logo – middle laser printing and bottom bubble jet printing show decrease in print quality

If you have any concerns about supporting documentation, you should contact the applicant. If you need to contact a utility or other company to confirm they provide a service to the given address, you should obtain permission from the applicant first.

Internet banking and bills

Many people use the internet to bank and pay their bills. As a consequence they no longer receive hard copy bills. An applicant may inform you that they are unable to provide a hard copy bill. They might offer, instead, to print a copy from their internet account. However, such approaches are open to abuse and forgery. You should ask the applicant whether they are able to provide a hard copy bill/statement. Alternatively, you can accept an internet bill or statement in conjunction with a separate, independently issued hard copy bill or statement from another organisation.

Documents you should not accept

You should not accept:

- duplicate or photocopied identity documents (modern photocopiers often produce excellent results);
- driving licence paper counterpart – this was abolished on 8 June 2015 and is no longer a legal document. Paper driving licences issued prior to the introduction of the photocard licence in 1998 are still valid;
- an international driving licence – these are easily and frequently forged. However, an international driving permit is an internationally –recognised additional document to support driving licences from any country. In the UK, they can be purchased from a Post Office;
- a copy of a birth certificate issued more than six weeks after birth – these can be purchased on request by any individual without proof of identity;
- mobile telephone bills (as these can be sent to different addresses).

Where to get help

CPNI offers free training to organisations in the critical national infrastructure on identity and document verification. For further details, please contact your CPNI adviser.

If you have any concerns about the validity of documents presented to you, you should contact the UK Visas and Immigration (UKVI) Sponsorship, Employer and Education Helpline on 0300 123 4699. They will treat any information you provide in confidence and pass this on to the relevant UK Local Enforcement Office for further investigation. Often there may be criminal offences other than the production of a forged document involved. If you suspect this is the case, you should contact your local police.

If it is a foreign document, then the relevant embassy or consulate may be able to help you. You may also find useful information in government owned or sponsored websites.

The Public Register of Authentic Identity and Travel Documents Online (PRADO) provides information on the security features of passports, visas, identity cards, driving licences and other documents of identity issued in EU member states, and an increasing number of non-EU member states. For further details, please visit www.consilium.europa.eu/prado/en/prado-start-page.html.

Commercial companies provide systems which can check the authenticity and validity of documents. Services include the checking of many of the security features described in this guidance, checking of the machine readable zone in passports and document expiry dates, and access to databases of security features.

Operation Fairway

The purpose of Operation Fairway is to detect, deter and disrupt terrorist attack planning in the UK. It is managed and coordinated by the National Counter Terrorism Security Office (NaCTSO).

Operation Trammel (a strand of Operation Fairway) was launched in 2003. Its aims include: to identify individuals who use fraudulent or fraudulently obtained genuine travel and identity documentation to support international terrorist activities.

Of current concern is the misuse of forged or stolen passports or other identity documents to gain employment in vulnerable premises.

Do you know who you are employing?

The Fairway Team offers free Document Awareness workshops to HR and recruitment departments of companies vulnerable to terrorist attack, and aims to increase their knowledge of identity documents and the potential for their abuse.

For Operation Trammel enquiries or to find out more about Fairway document awareness, please contact nactso@cpni.gsi.gov.uk or telephone 020 7084 8433.

Appendix 1: Basic document examination summary

The application of a few simple, non-destructive tests can identify the more obvious forgeries and counterfeits. Wherever possible, when examining documents compare them with known originals, or refer to websites such as PRADO (see previous chapter). If unsure, seek a second opinion.

Check for impersonation

- compare the photograph/image to the document holder;
- check the age, visible marks and signature of the document holder. If practicable, ask the candidate to sign something in the presence of an authorised individual who can then compare the signature with that on the documentation provided;
- check the chin, lips, ear shape (if possible), eyes and nose and their relation to the face as a whole;
- Check that the details provided correspond with what is already known about the candidate.

Check for evidence of counterfeiting

- check the cover and overall construction of the document. Is the gold blocking well-defined and well-aligned? Do all the pages line up?
- inspect the condition of the document in relation to issue dates and look for signs of wear and tear to the document. If unsure, inspect other security features on the document;
- check for incorrect issue and expiry dates (e.g. the 31st of 30 day months);
- check the watermark using transmitted light;
- use UV light. Do the paper and watermark react? (they shouldn't)
- check the print quality. Is it misaligned? Does the font change unexpectedly on the page?
- are there any spelling or grammatical errors?
- is there any intaglio printing? Is it raised or rough when you touch it?
- is it a camouflage/fantasy document? Can you verify that the country or issuing authority exists?

Once you are satisfied that the document is not counterfeit, you should check for signs that the document may have been tampered with.

Check for evidence of page substitution

- do all of the pages align?
- is the stitching correct? Does it react when exposed to UV light? (it should in a genuine document)
- do all pages react the same way when exposed to UV light? (they should in a genuine document)
- are all of the pages present? Are they in numerical order?

Check for photograph/image substitution

- check the authentication and for any damage to embossed stamps (if present);
- check that safeguards in the laminate are present and undamaged (e.g. holograms and UV features);
- look for unusual UV reaction in the photograph/image area;
- check for creases, tears or air bubbles in the laminate, and for any extraneous material beneath the laminate. This could include dirt or the original laminate, for example;
- look for any cut marks around or behind the photograph/image.

Check the visas and stamps in the document

- visas are secure documents in themselves and should have security features to the same standards as passports;
- check for spelling mistakes in the visas and stamps.

Appendix 2: Document verification checklist

You should only use this checklist after having read and gained an understanding of this document.

	Cause for concern	
	Yes	**No**
Condition How does the age of the document compare with the issue date?		
Do all the pages align when the document is closed?		
Is each page numbered?		
Do the pages run in numerical order?		
Does the stitching appear loose or broken?		
Are any of the stitching holes enlarged or empty?		
Photographs Compare the document's photo with the applicant		
Are there any safeguards such as embossed stamps over the photo? Do they match up between the photo and the page?		
Is there a holographic image covering the photo and biodata page?		
Is there an edge, cut marks or ridge between the photo and page? (run your finger across the page)		
Is the photo area noticeably thicker than the rest of the page?		
Is there any dirt or other extraneous substances around the edge of the photo?		
Is there only one laminate? (view at the edge of the page)		
Biographical data Compare the biodata (date of birth, signature etc.) with the same information provided elsewhere by the applicant.		
Check for spelling mistakes including visas and stamps.		
Examination under transmitted light Can you see a watermark?		
Are there laser-perforated designs on the biographical data page?		
Examination under ultra-violet light Does the watermark react under UV light? Watermarks should never react under UV light.		
Does the page react under UV light? Genuine pages should only have a low base-fluorescence (i.e. should not react brightly).		
Is there a UV safeguard that runs over the photo and biodata page? If not, this could indicate photo or biodata page substitution.		
Does the stitching react under UV light? (it should)		
Printing Is the printing on the inside front cover raised and rough? (run your finger across the page)		
Is there rainbow printing throughout the document?		
Is there miniprint or microprint throughout the document?		