Proof of Age
Standards Scheme

PASS

PASS 2:2020

Requirements for e-ID Validation Technology

Introduction

The Proof of Age Standards Scheme ("PASS") is the United Kingdom's national Proof of Age Accreditation Scheme, endorsed by the Home Office, the National Police Chiefs' Council (NPCC), the Security Industry Authority (SIA) and law enforcement officers, such as Trading Standards.

The PASS Scheme is operated by a Community Interest Company providing accreditation to suppliers of Proof of Age Cards in the UK.

The Accredited Providers are assessed against the standards set out in:

- PASS 0 – General Principles and Definitions
- PASS 1 – Requirements for Identity and Age Verification
- PASS 2 – Requirements for e-ID Validation Technology
- PASS 3 – Requirements for Data Protection, Privacy and Security
- PASS 4 – Requirements for Proof of Age Card Design and Construction

The PASS Scheme may decide to add further standards for specific types of proof of age services, which shall result in extensions to this list.

All Accredited Providers are required to comply with PASS 0:2020 and any relevant PASS Standards applicable to their business operations. The relevant PASS Standards will be shown on the individual licence agreement between PASSCo CIC and the Accredited Provider.

All Accredited Providers are required to comply with the latest version of the PASS Standards (indicated by the year of issue), subject to any transitional arrangements agreed by the PASS Standards Committee.

The PASS Standards are assessed by qualified, competent auditors appointed by PASS to ensure that Accredited Providers reach and continue to operate to the requirements of the PASS Standards. This means that providers of age restricted goods, content and services can be confident in accepting cards with a PASS hologram, safe in the knowledge that the scheme is supported by the police, Trading Standards and a wide range of trade bodies.

Contents

1. Scope

The Proof of Age Standards Scheme (PASS) Standards are applicable to any Proof of Age Card provider that wishes to operate under the PASS Scheme and have access to use of the PASS registered Trade mark.

This part of the PASS Standards:

- establishes the requirements for electronic identification document validation technology utilised during the PASS card, token or device application process;
- determines how e-IDVT are to be audited and assessed;
- sets the process for document checking using e-IDVT;
- establishes the requirements for extracting data from documents presented to e-IDVT and for sharing these with Accredited Providers;
- sets requirements for training of staff involved in the e-IDVT process;
- addresses tackling fraud and attempted fraud;
- specifies requirements for reporting the results of e-IDVT to Accredited Providers.

The suite of PASS Standards are applied as applicable to the activities of Accredited Providers or Applicant Providers. This will be dependent on the scope of operations of the providers and the services that they provide for citizens.

2. Normative References

Legal Provisions

National and International Standards

ISO/IEC 14443 Identification cards – Contactless integrated circuit cards – Proximity cards

ISO/IEC 7810 Identification cards – Physical characteristics

ISO/IEC 30107 – Information technology – Biometric presentation attack detection

PAS 1296 – Online age check – Code of Practice

Other Documents

Home Office Guidance on Identification Document Validation Technology (March 2018)

3. Terms and definitions

In this document:

"shall" indicates a requirement

"should" indicates a recommendation

"may" indicates a permission

"can" indicates a possibility or a capability

GUIDANCE NOTES *are shown in italic text and are intended to assist the reader with understanding provisions.*

When referring to the PASS Standards, refer to the PASS Standard, followed by the year of issue, followed by the provision – such as **PASS 0, 4.3.2**.

The terms and definitions established in PASS 0 apply to this standard and all PASS Standards.

4. Identity Document Validation Technology

Use of e-IDVT

4.1 An Accredited Provider may use e-IDVT to assist with establishing the authenticity of documents presented for identity verification as part of an application for a PASS Card.

4.2 An e-IDVT may be used in relation to:

(a) a photographic identification document listed in PASS 1 - Requirements for Identity and Age Verification, s 4.1;
(b) a non-photographic identification document listed in PASS 1 - Requirements for Identity and Age Verification, s 5.1;
(c) ascertaining that a referee is from a recognised profession listed in PASS 1 - Requirements for Identity and Age Verification, s 5.10;
(d) the capture of a photograph provided it is a full-frontal image captured in accordance with ISO/IEC 19794-5:2011 + A2:2015 Information Technology – Biometric data interchange formats – Part 5: Face image data.

4.3 An Accredited Provider shall not require the use of e-IDVT in the application process without also providing another means for applicants to provide their identification documents in accordance with PASS 1 – Requirements for Identity and Age Verification.

4.4 An Accredited Provider shall assess the validity of the electronic identification submitted in support of the application in order to comply with the requirements in PASS 0, 4.4 (confident so they are sure) including, where applicable, assessing that the photograph to be assigned to the PASS Card is a true likeness of the photograph on the supporting document. An e-IDVT may only be used to assist with this process, not as a replacement for it.

Audit of e-IDVT

4.5 An e-IDVT system or provider shall be audited by an auditor appointed by PASSCo, in accordance with this standard, before being utilised as e-IDVT for the purpose of being used as part of the application process for a PASS Card.

4.6 An Audit shall determine:

(a) the permitted capture devices that the e-IDVT is designed to work with and any parameters that may be associated with that;
(b) the software and template library utilised by the e-IDVT and any limitations, including jurisdictional limitations, that may be associated with that;
(c) the certification and testing of liveness detection, facial recognition and near field communications analysis utilised by the e-IDVT;
(d) the application interface with the Accredited Provider (if any), including any requirements, settings or policies necessary to ensure the interoperability of the systems;
(e) the minimum authentication requirements applicable to the use of the e-IDVT.

4.7 The Auditors may agree with an individual e-IDVT an application interface protocol applicable to the use of the e-IDVT by Accredited Providers.

5. Process of Document Checking

Checking that an e-IDVT Document is genuine

5.1 An e-IDVT shall undertake checks to establish if the document is genuine.

This requirement is about identifying if the document is false, counterfeit, altered, forged, inconsistent or there is the presence of contra-indicators.

5.2 An e-IDVT shall establish that a document is genuine to a Level of Assurance – Rank 3 – assurance based on beyond reasonable doubt.

The Level of Assurance – Rank 3 is set out in the Home Office Guidance on Identification Document Validation Technology. An image of a photocopy of a document (a second generation image) presents reasonable doubt regarding the validity of the original image and shall not be used for Level of Assurance – Rank 3. The image taken of the presented document shall be of the original document.

5.3 An e-IDVT shall identify at least five security features in the document and compare these against an identity document template.

5.4 If assessing a document with a contactless integrated circuit card, the e-IDVT may utilise near field communication (NFC) analysis of the document instead of examining five security features in the document and comparing it against an identity document template.

5.5 An e-IDVT shall perform a check on any UK or EU issued identity document by reference to the PRADO Database (PRADO - Public Register of Authentic travel and identity Documents Online).

5.6 An e-IDVT shall perform a check on any non-UK or non-EU issued identity documents against a suitable and reliable document template database for that document.

5.7 A document check shall not damage the document under check.

E-IDVT checks are not intended to be destructive. They should be able to perform checks repeatedly without damaging the document. This means that the check should not involve physical testing of the document.

Checking that an e-IDVT Document is valid

5.8 An e-IDVT shall undertake checks to establish if the document is valid.

This requirement is about assessing whether or not the document is current, issued by an appropriate authority authorised to issue such documents, not lost or stolen and whether there is the presence of contra-indicators.

5.9 An e-IDVT shall establish that a document is valid to a Level of Assurance – Rank 3 – assurance based on beyond reasonable doubt.

The Level of Assurance – Rank 3 is set out in the Home Office Guidance on Identification Document Validation Technology.

5.10 An e-IDVT shall identify:

(a) the identity of the issuing authority for the document;
(b) the date, if any, that the document was issued by that issuing authority;
(c) the date, if any, that the document is due to expire.

5.11 An e-IDVT shall identify the authoritativeness category of the issuing authority, which may be:

(a) a PASS Accredited Provider;
(b) a public authority;
(c) a financial institution;
(d) a utility provider;
(e) a recognised professional body.

5.12 An e-IDVT shall not accept an asserted validity by the document holder without conducting independent validity checks.

5.13 An e-IDVT shall notify the Accredited Provider of any contra-indicators concerning the validity of the identification document presented.

Checking the holder of an e-IDVT Document

5.14 An e-IDVT shall undertake checks to link the holder of the document to the presented identification document, where that document is a photographic identification document.

This requirement is about assessing whether or not the person presenting the document is a real person, is the person to whom the document was issued and whether there is the presence of contra-indicators.

5.15 An e-IDVT shall establish that the holder of the document is the person to whom the document was issued to a Level of Assurance – Rank 3 – assurance based on beyond reasonable doubt.

The Level of Assurance – Rank 3 is set out in the Home Office Guidance on Identification Document Validation Technology. An image of a copy of a photograph (a second generation image) presents reasonable doubt regarding the validity of the original image and shall not be used for Level of Assurance – Rank 3. The image taken of the person shall be a directly captured photograph.

5.16 An e-IDVT shall establish that the person presenting the document is alive.

This means that the e-IDVT must undertake liveness detection in accordance with ISO/IEC 30107 – Information technology – Biometric presentation attack detection.

5.17 An e-IDVT shall be capable of detecting a presentation attack of either a false instrument, an artificial or human presentation attack instrument or an artificially generated presentation attack.

A presentation attack occurs when a false instrument or a person or artefact not relating to the claimed identity is presented to the e-IDVT system. The assessment, measurement, reliability and characteristics of a presentation attack are set out in ISO/IEC 30107 – Information technology – Biometric presentation attack detection.

Facial Recognition

5.18 An e-IDVT assessing a photographic identification document may undertake automated or semi-automated facial recognition.

5.19 An e-IDVT automated facial recognition process shall undertake a minimum of twenty-six (26) landmark point analysis of any landmark point types. These can include MPEG4 Features, Anthropometric 2D or 3D landmarks.

Landmark point analysis is described in ISO/IEC 19794-5:2011 + A2:2015 – Information technology – Biometric data interchange formats – Part 5: Face image data.

5.20 An e-IDVT facial recognition process that cannot establish and verify 26 landmark points to analyse the image of the card holder, is semi-automatic and requires a suitably trained individual to perform secondary facial matching checks.

5.21 The landmark points utilised to perform the check shall be recorded.

This PASS Standard does not require the point metric to be recorded (that is personally identifiable information), but does require the point identifier as set out in Table 15 – Definitions of anthropometric landmarks of ISO/IEC 19794-5:2011 + A2:2015 – Information technology – Biometric data interchange formats – Part 5: Face image data to be recorded.

5.22 If assessing a document with a contactless integrated circuit card, the e-IDVT may utilise near field communication (NFC) analysis of the document to extract landmark points instead of examining the photograph in the document.

Non-Photographic Identification Documents

5.23 Where e-IDVT is being used to assess whether a non-photographic identification document is genuine and valid, it shall be the responsibility of the Accredited Provider to complete checks to link the document to the holder in accordance with PASS 1 – Requirements for Identity and Age Verification, Section 5.

6. Data Extraction

Checking that an e-IDVT Document is genuine

6.1 An e-IDVT may undertake a process of data extraction from the presented document in order to provide information about claimed identity to the Accredited Provider.

6.2 When extracting data from a document, the e-IDVT shall:

(a) identify the data contained in any machine readable zone (MRZ), including identifying and verifying check digits through the applicable algorithm for that document;
(b) identify at least three items of data printed on the document that can be validated against the MRZ or claimed attributes from the applicant during the application process;
(c) establish the extracted data in accordance with the requirements in PASS 1 – Requirements for Identity and Age Verification (naming and photo standards).

6.3 An e-IDVT shall report contra-indicators in a data extraction process to the Accredited Provider.

A contra-indicator could be where the optical character recognition process for the MRZ has extracted data that does not match the check digits. This could be a failed capture or it could be where the applicant has attempted to alter the data contained in the MRZ.

6.4 If assessing a document with a contactless integrated circuit card, the e-IDVT may utilise near field communication (NFC) analysis of the document to extract data instead of undertaking a comparison of MRZ data with data printed on the document.

7. Dealing with Fraud or Attempted Fraud

7.1 An e-IDVT shall have a documented process for dealing with fraud or attempted fraud.

7.2 An Accredited Provider shall deal with e-IDVT fraud or attempted fraud as a contra-indicator.

7.3 An e-IDVT shall:

(a) participate, as far as permitted and practicable, with the Amberhill Database;
(b) provide information about fraud to Action Fraud;
(c) otherwise cooperate with law enforcement agencies to counter fraud or attempted fraud.

The Amberhill Database is operated by the Metropolitan Police. E-IDVT's can share reports automatically or semi-automatically with amberhill@met.pnn.police.uk. Action Fraud is a means for reporting fraudulent activity to local police.

7.4 An e-IDVT provider, Accredited Provider or any other party in the process shall, in partnership with police and specialist agencies, take action to assist persons with hijacked identities to manage the impact on the genuine owner of that identity.

This includes ensuring that an attempted hijacking of an existing PASS Card holder, does not prevent the genuine owner of that identity from continuing to use their genuine PASS Card.

7.5 An e-IDVT provider may:

(a) allow a submitted document assessed as not being genuine to be resubmitted up to 5 times, but the number of attempts must be recorded and provided to the Accredited Provider;
(b) allow a facial recognition data capture to be retaken up to 5 times, but the number of attempts must be recorded and provided to the Accredited Provider;
(c) treat a failed validation as a contra-indicator and report this to the Accredited Provider.

8. Training and Data Protection

8.1 An e-IDVT shall provide Accredited Providers with suitable training on the use of the e-IDVT system, analysis of results and understanding of fraud and contra-indicators.

8.2 An e-IDVT utilising human document and facial matching recognisers shall provide them with suitable training to undertake that activity.

8.3 An e-IDVT and the Accredited Provider shall comply with the requirements of PASS 3 – Requirements for Data Protection, Privacy and Security.

8.4 In particular, the e-IDVT shall:

(a) limit the use of the e-IDVT to the intended purposes;
(b) limit the amount of data collected to the minimum necessary to discharge the intended purposes;
(c) ensure that restrictions are in place limiting access to e-IDVT records to those whose duties require it;
(d) ensure that there is an audit and access logging function;
(e) establish suitable data sharing agreements;
(f) monitor the level of false positive or false negative results generated by the e-IDVT.

9. Reports to Accredited Providers

9.1 An e-IDVT provider shall provide a means for Accredited Providers to access the outcome of e-IDVT checks.

This can be an electronic dashboard, written report or any other effective and recorded means of disseminating the results of the e-IDVT checks in a secure way. Where dissemination is by way of a data interchange, the Biometric data, Face Image data, identity attributes, authoritativeness category and level of assurance shall be exchanged by use of recognised interchange formats (such as ISO/IEC 19794-5:2011 + A2:2015 – Information technology – Biometric data interchange formats – Part 5: Face image data as an example).

9.2 If an Accredited Provider is supplied with a dashboard through which the Accredited Provider can carry out the document validity checks themselves, the staff of the Accredited Provider shall be given suitable training to perform that task.

9.3 If an e-IDVT permits the sharing of unverified attributes with an Accredited Provider, the Accredited Provider shall not be entitled to rely upon:

(a) an unverified name;
(b) an unverified date of birth;
(c) an unverified photograph.

Accredited Providers may treat these unverified attributes as contra-indicators or may determine to utilise an alternative means of verification.

9.4 If an e-IDVT permits the sharing of a verified, but not determined, age with an Accredited Provider, the Accredited Provider shall not be entitled to rely upon that without also establishing the date of birth of the applicant.

9.5 An Accredited Provider can rely on an attribute data string provided by the e-IDVT system, established, audited and certified in accordance with this PASS Standard as effective evidence of claimed identity for the purposes of PASS 1 – Requirements for Identity and Age Verification, without having to see an image of the document used for the e-IDVT purpose.

Subject to having a suitable data sharing agreement in place, an Accredited Provider may put into place a system whereby an image of the document used for the e-IDVT process is shared with the Accredited Provider.

About PASS

The PASS Scheme is operated by a Community Interest Company providing accreditation to suppliers of Proof of Age Cards in the United Kingdom. The Accredited Providers are assessed against strict standards by qualified auditors to ensure that they operate to the highest standards. Sellers of age restricted products can be confident in accepting cards with a PASS hologram, safe in the knowledge that the Scheme is supported by the police, Trading Standards and a wide range of trade bodies.

Assurance

Every card that carries a PASS hologram will have been issued by a provider who has been through a stringent application and accreditation process.

Confidence

Production of a PASS hologrammed card at the point of sale affords retailers and their staff the confidence of knowing that the card is a trusted and secure form of identification.

Reliability

The unique PASS hologram is a registered Trade mark, making it a criminal offence to manufacture cards that have a mark similar to the PASS one.

Support

Possession of a PASS accredited card demonstrates that your age and personal details have been verified by your Accredited Provider and you are who you say you are!

PASS

PASSCo C.I.C.

www.pass-scheme.org.uk

A community interest company registered in England at 37 Stoney Street, Nottingham, England, NG1 1LS with the registered number 04570623.