[ANNEX 4]

Proof of Age
Standards Scheme

PASS

PASS 5:2023

Requirements for Digital Presentation of Proof of Age

PASS 5:2023
Requirements for Digital Presentation of Proof of Age

PASS

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 services 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
- PASS 5 – Requirements for Digital Presentation of Proof of Age

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

Introduction 2

Contents 3

1. Scope 5

2. Normative References 6

3. Terms and definitions 7

4. Creation of a PASS Digital Presentation of Proof of Age Service 11

Operating a PASS DPoA Service 11

Use of the PASS Dynamic Graphic by the Accredited Provider 12

Use of the PASS Trade Mark by Providers of DPoA Interoperability Services 13

5. Digital Proof of Age Elements and Positioning 14

The DPoA Elements 14

PASS Dynamic Graphic 16

PASS Digital Proof of Age Insignia 17

Supporting Organisation Logos 17

Photograph of the User 18

Name of the User 19

Date of Birth of the User 20

Accredited Provider's Identification Number assigned to the User 20

Age Identifier 21

Guilloche 22

DPoA Issuers Zone 23

Validation Symbol 23

Indicative Examples of DPoA Screen Layout 24

6. Reveal Process for Digital Presentation of Proof of Age 25

Pre-Reveal Stage 25

Reveal Activation 26

DPoA-Reveal Stage 27
Biometric User Authentication 28
One Time Code 29
DPoA Usage Logs 30
7. Security Features and Presentation Controls 32
Security Controls 32
Cryptography 33
Session Handling 33
Stack Protection 34
Attack Detection 34
Screen Recording 35
Contra Indicators 35
Penetration Testing 35
8. Customer Care and Support 36
Supporting DPoA Users 36
Account Suspension or Closure 36
App Support Tools 37
About PASS 38

1. Scope

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

These technical requirements are intended to facilitate the digital presentation of proof of age (DPoA) using a smart device, such as a mobile telephone. They are open standards that do not prescribe the technology or solution provided, but set standards of consistency of display (to ease recognition, interpretation and training for the staff of relying parties) and implement requirements for security and presentation controls.

This part of the PASS Standards:

- establishes the requirements for technical implementation of a digital proof of age application and linkage to a PASS Accredited Provider's database with verified identification and age;
- establishes that Digital Proof of Age (DPoA) does not seek to emulate a Digital ID but does contain high standards of verification to establish that the bearer seeking to prove their age attribute is the person they purport to be;
- determines the security and anti-spoofing control features associated with the digital presentation of proof of age on a device;
- sets the design and look of the user interface for when a visual display of the DPoA is utilised (including key features, minimum sizing and aspect ratio locks);
- establishes requirements addressing the methods of activation of the digital proof of age including signal activation or code activation;
- sets the protocols for the digital sharing of DPoA, once activated, through connected devices and interoperability protocols;
- sets requirements in relation to presentation attack detection, dealing with spoofing and system level attacks;
- determines the requirements for the control and use of any PASS Dynamic Graphic, including effective controls over technical features of that file (the .GIF PASS image);
- addresses the requirements for dealing with customer care, loss of utility of the App, account recovery and addressing misuse of the App or system;
- establishes the requirements for technical implementation of interoperability between Accredited Providers including by sub-contractors and providers of DPoA Interoperability Services.

PASS 0 establishes the general principles applicable to all PASS Accredited Providers, including common terms and definitions used throughout this PASS Standard.

2. Normative References

The normative references in PASS 0 are relevant to this standard and, in addition, the following are also relevant:

BS 8626:2020 - Design and operation of online user identification systems – Code of practice

ISO 8601-1:2019 – Date and time – Representations for information interchange – Part 1: Basic rules

ISO/IEC 18092 / ECMA-340—Near Field Communication Interface and Protocol-1 (NFCIP-1)

ISO/IEC 19794-2:2011 - Information technology — Biometric data interchange formats — Part 2: Finger minutiae data

ISO/IEC 19794-5:2011 + A2:2015 Information Technology – Biometric data interchange formats – Part 5: Face image data

ISO/IEC 21481 / ECMA-352—Near Field Communication Interface and Protocol-2 (NFCIP-2)

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

PAS 1296:2018 – Code of Practice for Age Check Services

UK Government Good Practice Guide 45 – Identity Proofing Guidance

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 0:2020 4.3.2**.

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

3.1
Adult Means an individual who has attained the age of 18.

3.2
Attack Detection Means:

(a) In the context of systems attack detection, the collection of information and taking appropriate response measures by monitoring the DPoA network, system status, behaviour, and the usage of system, which should automatically detect unauthorized usage of system users and attacks of external attackers on the system; and
(b) In the context of presentation attack detection, the identification of an artefact or human characteristic presented to the biometric capture subsystem in a fashion

that could interfere with the correct biometric user authentication.

3.3
Biometric User Authentication

Means the process described in s.6.16 – 6.19 of these technical requirements.

3.4
Brute Force Attack

Means an attack on a cryptosystem that employs an exhaustive search of a set of keys, passwords or other data, such as encryption keys.

3.5
Child

Means an individual that has not attained the age of 18.

3.6
Code Activation

Means activation of the DPoA elements in accordance with s.6.8 of these technical requirements.

3.7
Cryptography

Means the discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification, and/or prevent its unauthorized use.

3.8
DPoA

Means Digital Proof of Age

3.9
DPoA app

Means an application for download and use within an operating system of a mobile device that can be used to manage and reveal a DPoA.

3.10
Encryption

Means the function of transforming data by the discipline of cryptography so as to make the data undecipherable to anyone other than the legitimate sender and receiver.

3.11
Jailbreaking

Means the process of exploiting the flaws of a locked-down electronic device to install software other than what the manufacturer has made available for that device. Jailbreaking allows the device owner to gain full access to the root of the operating system and access all the features.

3.12
Man-in-the-Middle Attack

Means a systems attack in which an attacker is able to read, insert, and modify messages between two parties without their knowledge.

3.13
Matrix Barcode

Means a two-dimensional code consisting of black and white "cells" or dots arranged in either a square or rectangular pattern. One example of a matrix barcode is a Quick Response (QR) Code.

3.14
Near Field Communication (NFC)

Means a set of communication protocols for communication between two electronic devices over a distance of 4 cm or less as set out in ISO/IEC 18092 / ECMA-340—Near Field Communication Interface and Protocol-1 (NFCIP-1) or ISO/IEC 21481 / ECMA-352—Near Field Communication Interface and Protocol-2 (NFCIP-2).

3.15
PASS Dynamic Graphic

Means a Graphic Interchange Format file (or other protected and encrypted file format) issued to the Accredited Provider by PASSCo for use within a DPoA.

3.16
Primary DPoA Elements

Means the DPoA elements described in s.5.1.

3.17
Providers of DPoA Interoperability Services

Means the sub-contractors of PASSCo, Accredited Providers or Relying Parties that are established to provide the interoperability functionality of DPoA services.

3.18
Relying Party

Means an entity that relies upon the DPoA.

3.19
Rooted Device

Means a process of unlocking devices to attain higher administrative privileged controls. This can include gaining the ability to install unapproved apps, update operating systems, delete unwanted apps, underclock or overclock the processor, replace firmware and customize anything else.

3.20
Secondary DPoA elements

Means the DPoA elements described in s.5.2.

3.21
Signal Activation

Means activation of the DPoA elements in accordance with s.6.5 of these technical requirements.

3.22
SSL Pinning

Means the processing of incorporating the expected secure socket layer certificate for a server into the application interface with that server.

3.23
Stack

Means a technology stack, also called a solutions stack, technology infrastructure, or a data ecosystem, as a list of all the technology services used to build and run the DPoA application.

3.24
Stack Canaries

Means a process used to detect a stack buffer overflow before execution of malicious code in an application can occur.

4. Creation of a PASS Digital Presentation of Proof of Age Service

Operating a PASS DPoA Service

4.1 An Accredited Provider may establish a technical user interface to provide the facility for the user to display their proof-of-age status through a digital device (such as through a mobile telephone). The display may be onscreen or through a digital sharing of their proof of age status through an interoperability mechanism. This is called a DPoA throughout these technical requirements.

Note: The creation of a DPoA is optional for Accredited Providers. It is also not a requirement that an Accredited Provider issuing a DPoA also has to issue physical cards as well. The relevant provisions of the PASS Standards will apply to the type of business operation of the Accredited Provider.

4.2 The DPoA shall be established in accordance with the requirements of these technical requirements.

4.3 An Accredited Provider shall establish the identity and age verification of the user in accordance with PASS 1 – Requirements for Identity and Age Verification and, if paragraph 4.6 of those requirements applies, in accordance with PASS 2 – Requirements for e-ID Validation Technology.

4.4 The Accredited Provider shall provide a facility for user account set up on the DPoA which shall secure:

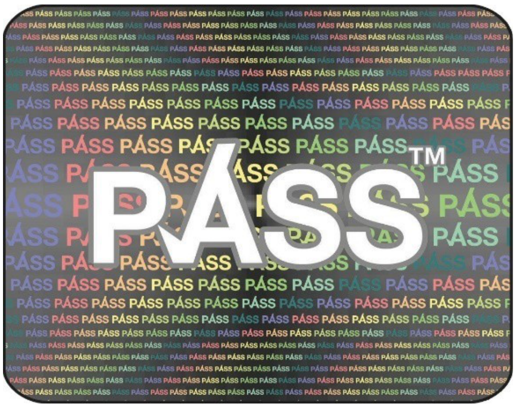
(a) Enrolment of the user;
(b) Binding of the user to the identity and age verification established by paragraph 4.3.

Note: Recommendations on the implementation of these processes are provided in BS 8626:2020 - Design and operation of online user identification systems – Code of practice.

4.5 The user account shall be bound to the device by establishing a record of the device identification number.

Use of the PASS Dynamic Graphic by the Accredited Provider

4.6 The PASS Dynamic Graphic shall consist of a moving image of the PASS Hologram Logo provided in Graphic Interchange Format (.GIF) (or other protected and encrypted file format) designed to display on a repeating five second loop for the duration of the DPoA display in accordance with s.5.6 to 5.8.



4.7 Accredited Providers or their sub-contractors shall handle and use the PASS Dynamic Graphic in accordance with this section.

4.8 The PASS Dynamic Graphic shall be treated as a controlled asset. This means that, from the receipt of the PASS Dynamic Graphic (.GIF) file for or on behalf of the Accredited Provider through to the incorporation of it in a DPoA app and the deletion or removal of it, the PASS Dynamic Graphic shall be actively tracked and monitored.

4.9 Accredited Providers or their sub-contracts shall not place the PASS Dynamic Graphic in the public domain other than embedded within a DPoA app.

4.10 The transmission of the PASS Dynamic Graphic shall always be encrypted.

4.11 The Accredited Provider shall record, and be subject to audit on the number of DPoA user accounts created by the Accredited Provider.

4.12 Each creation of an active account by an Accredited Provider shall be a licensed use of the PASS Dynamic Graphic.

Use of the PASS Trade Mark by Providers of DPoA Interoperability Services

4.13 A DPoA Interoperability Service shall not use the PASS Trade Mark to indicate that their DPoA is compatible with these PASS Technical Requirements unless:

(a) They have submitted an interoperability statement to PASSCo;
(b) They have produced an integration protocol for their system in accordance with the Interoperability Guidelines issued by PASSCo;
(c) They have provided a copy of their interoperability statement and integration protocol to all Accredited Providers of DPoA;
(d) They have not established or attempted to establish any exclusivity arrangements with any individual relying parties;
(e) Their approach to interoperability has been audited by the PASSCo auditors to ensure that it is compatible with these PASS Technical Requirements.

Note: These Technical Requirements recognise that interoperability with the electronic systems of relying parties is critical to success. It is intended that these requirements are enabling, to provide for multiple potential opportunities for digital interoperability, but it is also clear from relying parties that they want a uniform approach. As the market for DPoA develops, PASS expects solutions to emerge for this and the purpose of this section is for there to be some future oversight of those solutions to ensure that they remain appropriate for the PASS ecosystem.

5. Digital Proof of Age Elements and Positioning

The DPoA Elements

5.1 The primary DPoA elements shall consist of:

(a) The PASS Dynamic Graphic
(b) The PASS Digital Proof of Age Insignia
(c) The Supporting Organisation Logos
(d) The Age Identifier
(e) The Guilloche (a complex patterned emblem)
(f) The DPoA Issuers Zone
(g) The Validation Symbol

5.2 The secondary DPoA elements shall consist of:

(a) The Name of the User
(b) The Date of Birth of the User
(c) The Accredited Provider's Identification Number assigned to the User

5.3 The DPoA shall only be operable on a device that is capable of displaying all of the primary DPoA elements in the required sizes in a single field of vision on the device (i.e. without screen scrolling). The DPoA may also display the secondary DPoA elements in the required sizes in the same field of vision on the device.

Note: This requirement would indicate that the DPoA would not be operable on a small smart device (such as a watch) and Accredited Providers may need to describe minimum screen sizes for devices in their marketing and communications to enable compliance with this requirement.

Note: The display of DPoA elements in a specified format is intended to aid the recognition by staff of the relying party of a PASS accredited proof of age. This is particularly important for staff training and ubiquitous acceptance of PASS proof of age.

5.4 The DPoA shall be capable of functioning on devices operating:

(a) in portrait or landscape;
(b) with screen rotation or lock enabled;
(c) with dark, light or automatic background appearance;
(d) with adaptive ambient lighting adjustment (for brightness and contrast);
(e) with dynamic type display;
(f) with standard or zoomed features provided paragraph 5.2 can be complied with;
(g) with spoken content or audio descriptions enabled;
(h) with hearing commands, sound recognition or adaptive displays;
(i) with subtitles or captioning;
(j) on devices and equipment that supports users with additional needs, such as braille activated devices (provided that the interface display to the relying party is in a manner that enables them to view the DPoA elements).

The layout of pages of the DPoA other than the DPoA reveal page, such as those required for account management, transparency information, customer service or advice are at the discretion of the DPoA provider.

5.5 The DPoA elements may be held in an encrypted file on the device for serving to the DPoA reveal for a maximum period of seven days before re-authentication with the Accredited Provider's server and re-encryption on the local device.

Note: This permits the DPoA to serve elements from a local folder where there is no device connection to the Accredited Provider's server for a maximum period of one week.

PASS Dynamic Graphic

5.6 The PASS Dynamic Graphic shall display on screen (when permitted by these technical requirements) in a manner that secures that it is:
(a) at least 20mm wide;
(b) at least 15mm high;
(c) with square edges (i.e. that the left and right sides of the PASS Dynamic Graphic are at right angles (± 1°) to the top and bottom of the graphic);
(d) with square or cornered edges with ingress to the hologram not exceeding 2mm;
(e) with a locked aspect ratio if the user reorientates the display; and
(f) orientated such that the PASS Dynamic Graphic is parallel (± 1°) to the bottom of

the screen.

5.7 The PASS Dynamic Graphic shall display on screen with a transparent layer graphic co-terminus with it and on a layer above the PASS Dynamic Graphic.

Note: This is to hinder simple copy and paste functions, although more technical protections of the PASS Dynamic Graphic as set out in s.7 are required to hinder more complex attack vectors for the Graphic.

(a)

PASS Digital Proof of Age Insignia

5.8 The PASS Digital Proof of Age Insignia shall consist of:

(a) The PASS Trade Mark at least 10mm wide and 4 mm high;
(b) The words 'Proof of Age' to the right of the PASS Trade Mark in a suitably clear font.

Supporting Organisation Logos

The Supporting Organisation logos shall be displayed.

The current organisations supporting the PASS Scheme that permit the use of their logo on the Face of the DPoA are:

- *The National Police Chiefs' Council*

NPCC
National Police Chiefs' Council

- *The Security Industry Authority*

sia
Security Industry Authority

5.9 Accredited Providers shall not use any supporting organisations logos in any context other than as the logos would appear on a DPoA issued by the Accredited Provider, in any publicity or promotional materials, unless the Accredited Provider has the direct authorisation in writing of the supporting organisation to do so.

Photograph of the User

5.10 The Photograph of the User shall be served to the DPoA from the photograph obtained and held by the Accredited Provider in accordance with PASS 1, 8.1 – 8.10 (Photograph Standards).

5.11 The Photograph of the User shall display on screen (when permitted by these technical requirements) in a manner that secures it is:

(a) at least 28mm wide;
(b) at least 36mm high;
(c) with square edges (i.e. that the left and right sides of the photograph are at right angles (± 1°) to the top and bottom of the graphic);
(d) with square or cornered edges with ingress to the photograph not exceeding 2mm or have a blended fade background to the guilloche such that the background of the photograph fades to the outer edges;
(e) with a locked aspect ratio if the user reorientates the display;
(f) orientated such that the photograph is parallel (± 1°) to the bottom of the screen.

5.12 The photograph of the user shall be displayed in the pixel aspect ratio as captured in accordance with PASS 1, 8.1 – 8.10 (Photograph Standards).

5.13 The photograph of the user shall be displayed in colour.

5.14 The photograph of the user shall be displayed so that it is free from blemishes and of reasonable clarity and quality so that the user is identifiable to a reasonable person.

(a)

Name of the User

5.15 The name of the user shall be served to the DPoA from the name obtained and held by the Accredited Provider in accordance with PASS 1, 9.1 – 9.7 (Name Standards).

5.16 The name of the user may be displayed in the order of 'secondary identifier' 'primary identifier' with no initials or punctuation.

5.17 The name of the user shall, if shown, be displayed in two co-terminus elements:

(a) A line of text indicating that it consists of a name displayed in a suitably clear font; and
(b) A line of text containing the name of the user displayed in a suitably clear font.

5.18 The line of text required for 5.21 (a):

(a) Shall start with the text 'Name';
(b) For DPoA issued to residents of Wales, shall be followed with the text '/Enw';
(c) For DPoA issued to particular sectors of the community, may be followed with text indicating 'name' in a language familiar to that sector of the community.

(d)

Date of Birth of the User

5.19 The date of birth of the user shall be served to the DPoA from the date of birth obtained and held by the Accredited Provider in accordance with PASS 1, (Identity and Age Verification).

5.20 The date of birth shall, if shown:

(a) Be displayed on screen in the format of DD Mon YYYY or DD MON YYYY; or
(b) If transmitted in a signal, in accordance with ISO 8601-1:2019 – Date and time – Representations for information interchange – Part 1: Basic rules

5.21 The date of birth of the user shall be displayed in two co-terminus elements:

(a) A line of text indicating that it consists of a date of birth displayed in a suitably clear font; and
(b) A line of text containing the date of birth of the user displayed in a suitably clear font.

5.22 The line of text required for 5.26 (a):

(a) Shall start with the text 'DoB' or the text 'Date of Birth';
(b) For DPoA issued to residents of Wales, shall be followed with the text '/Dyddiad Geni';
(c) For DPoA issued to particular sectors of the community, may be followed with text indicating 'date of birth' in a language familiar to that sector of the community.

(d)

Accredited Provider's Identification Number assigned to the User

5.23 The Accredited Provider shall allocate a unique number consisting of 16 – 18 digits that may be displayed in the user number zone.

5.24 The unique number may be the same number as that issued to a PASS Card Holder in accordance with PASS 4, s. 4.32 (Card Numbers).

Note: PASS Card Issuers that use card numbers for dual purposes, such as pre-payment cards or ITSO smart ticketing may need to consider the security implications of display of that number on a Digital Device and, thus issue a different user number for the purposes of the DPoA app.

5.25 The user number should be displayed, if shown, in blocks of 4 digits (other than the 17th or 18th digit, if used) to aid reading and may include for check digits in accordance with an algorithm determined by the Accredited Provider. The first four digits of the User Number shall be allocated by PASSCo to indicate the identity of the Accredited Provider.

5.26 The user number shall, if shown, be displayed in a suitably clear font.

(a)

Age Identifier

5.27 A simple age identifier shall be displayed in the age identifier zone.

5.28 The simple age identifier shall be one of:

(a) If the user is a child, the age that the child is not younger than in whole years (for instance 8+, 13+, 16+, etc); or
(b) If the user is an adult, 18+

5.29 The age identifier for shall be displayed in a suitably clear font.

(a)

Guilloche

5.30 The DPoA screen shall incorporate a guilloche background.

5.31 The guilloche background shall be:

(a) red for the display of any DPoA elements prior to validation;
(b) green for the display of DPoA elements where the user is a child; and
(c) blue for the display of DPoA elements where the user is an adult.

5.32 In these technical requirements, 'red' means the pantone ® colour 032c.

For ease of reference, pantone ®colour 032c may also be referred to as:

RGB	*239 51 64*
HEX/HTML	*EF3340*
CMYK	*0 90 76 0*

5.33 In these technical requirements, 'green' means the pantone ® colour Green C.

For ease of reference, pantone ® colour Green C may also be referred to as:

RGB	*0 171 132*
HEX/HTML	*00AB84*
CMYK	*96 0 68 0*

5.34 In these technical requirements, 'blue' means the pantone ® colour 2925c.

For ease of reference, pantone ® colour 2925c may also be referred to as:

RGB	*0 156 222*
HEX/HTML	*009CDE*
CMYK	*75 18 0 0*

5.35 The background colour is a gradient of the relevant colour: 30% to white (right to left). The guilloche is a gradient of the relevant colour 100% to 30% (right to left). The rosette within the guilloche is a gradient of the relevant colour 90% to 45% (right to left).

DPoA Issuers Zone

5.36 The DPoA issuers zone may be used for the branding or promotional messages of Accredited Providers.

5.37 The content of the DPoA issuers zone shall not mislead or confuse as to the nature or identity of the Accredited Provider.

5.38 The DPoA issuers zone shall have the relevant colour guilloche as the background with the issuer logos having a transparent background.

5.39 The DPoA issuers zone shall display on screen (when permitted by these technical requirements) in a position that does not exceed 10% of the overall display of all DPoA elements on a single screen,

Validation Symbol

5.40 If the DPoA display is activated by a matrix barcode activation in accordance with s.6.7 (a), a Validation Symbol may be displayed on screen.

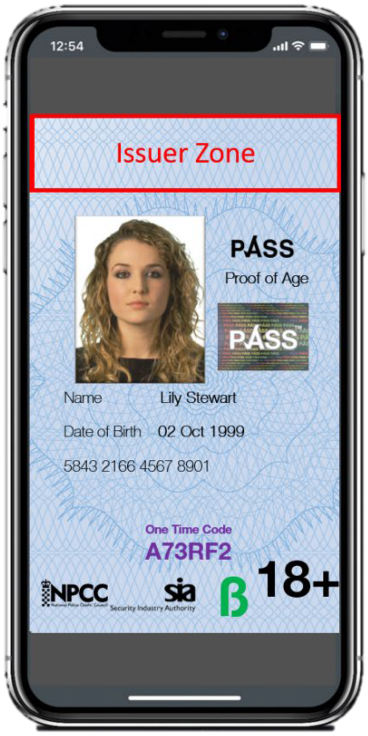
5.41 The Validation Symbol shall be determined by a prompt within the matrix barcode or by other suitable cryptography and be selected to match the Validation Symbol assigned to be used with that matrix barcode.

5.42 The Validation Symbol shall display on screen and be valid for a maximum of 60 seconds.

(a)

Indicative Examples of DPoA Screen Layout

The following provides an indicative example of the DPoA screen layouts in both portrait and landscape.



Issuer Zone

PASS Proof of Age

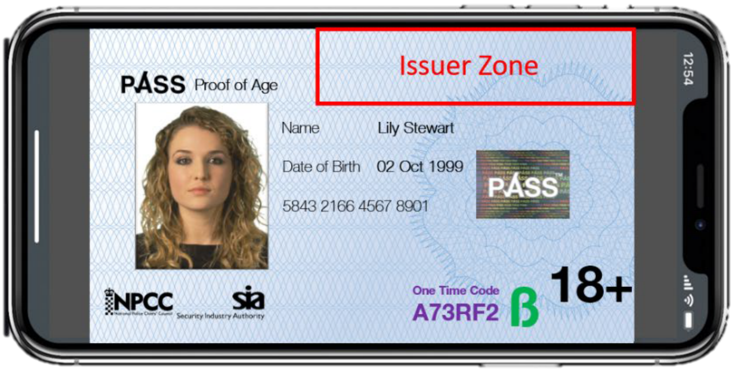
Name Lily Stewart

Date of Birth 02 Oct 1999

5843 2166 4567 8901

One Time Code
A73RF2

18+



Issuer Zone

PASS Proof of Age

Name Lily Stewart

Date of Birth 02 Oct 1999

5843 2166 4567 8901

One Time Code
A73RF2

18+

Note: The one-time code described in the above examples is optional and explained in further detail in s.6.19 – s.6.25. The one-time code may be displayed as a matrix barcode on the same screen or on a separate screen (a swipe to reveal a barcode).

6. Reveal Process for Digital Presentation of Proof of Age

Pre-Reveal Stage

6.1 The DPoA application may include functionality after user authentication, but prior to revealing the validated DPoA, that enables the authenticated user:

(a) to manage their account;
(b) to understand the functionality of the DPoA app;
(c) access to required transparency information in accordance with PASS 3 – Requirements for Data Protection, Privacy and Security;
(d) to know how to contact the Accredited Provider;
(e) to exercise their data rights;
(f) to access an unvalidated display of their DPoA in accordance with paragraph 6.2 (to enable them to know the information that will be shared with a relying party);
(g) to access settings or functionality to enable the user to choose whether or not to display the secondary DPoA elements during a DPoA reveal;
(h) to access such other information or services provided by the Accredited Provider or their agents or partners, provided it does not mislead or confuse as to the nature of the DPoA.

Note: There are no design restrictions on aspects of the DPoA application other than the reveal page. The remainder of the application can be in the corporate branding or style of the Accredited Provider.

Note: Accredited Providers should explain to users that restricting the display of secondary DPoA elements may limit the places that are able to accept the DPoA.

6.2 The DPoA application may incorporate a user interface prior to revealing the validated DPoA which may include the following elements:

(a) the identity of the Accredited Provider;
(b) the photograph of the user;
(c) the age identifier of the user;
(d) instructions on how to validate the DPoA (the suggested location for this is in place of where the PASS Dynamic Graphic element would be displayed).

And, if the user's settings under s.6.1 are set as such:

(a) the name of the user;

(b) the date of birth of the user;
(c) the Accredited Provider's identification number of the user;

But which shall:

(a) Be presented with a guilloche background colour in red (see s.5.39 – 5.44) and include red shading over the DPoA elements to indicate that they are not validated;
(b) Clearly indicate that the display is 'NOT VALIDATED';
(c) Not show the PASS Dynamic Graphic element;
(d) Not show the Validation Symbol;
(e) Not show a one-time code; and
(f) Not allow the transmission of a signal indicating that it is validated DPoA.

6.3 The DPoA pre-reveal elements should be displayed on screen in positions equivalent to the locations described in s.5.

Reveal Activation

6.4 The DPoA reveal activation may be triggered by:

(a) A signal activation
(b) A code activation

6.5 A signal activation for the DPoA shall consist of either:

(a) A device held by the relying party that is capable of issuing a near field communication (NFC) signal that the device containing the DPoA app is capable of reading and the DPoA app is capable of interpreting as a DPoA signal activation; or
(b) An encrypted signal issued by the Accredited Provider in response to a request for a signal activation by the user.

6.6 A signal activation shall not be permitted by transmission over the Internet unless it is an encrypted signal issued by the Accredited Provider under paragraph 6.5 (b).

6.7 A signal activation may be triggered by an application programme interface (API) provided for the purpose as incorporated into an app downloaded to the relying party's own device or into devices or equipment used by the relying party (such as electronic point of sale systems (ePOS) or payment processing equipment).

6.8 A code activation for the DPoA shall consist of either:

(a) A matrix barcode (such as a Quick Response Code) issued to the relying party by an Accredited Provider or PASSCo that can be captured by the device containing the DPoA app and the DPoA app is capable of interpreting as a DPoA code activation; or
(b) A one-time activation code issued by the Accredited Provider in response to a request for a code activation by the user, such as an SMS message.

6.9 A matrix barcode may be displayed in printed form on a document provided to the relying party (with associated validation symbols) or may be an application programme interface (API) provided for the purpose as incorporated into an app downloaded to the relying party's own device or into devices or equipment used by the relying party (such as electronic point of sale systems (ePOS) or payment processing equipment).

DPoA-Reveal Stage

6.10 The DPoA Reveal Stage shall consist of the display of DPoA elements on the screen of the user's device in accordance with the requirements of s.5 or, where the requirements of s6.11 are met, the transmission of DPoA elements to a relying party.

6.11 In addition to or instead of the display of DPoA elements on screen, where biometric user authentication has taken place in accordance with the requirements of s.6.15 to 6.18, the DPoA Reveal Stage may consist of:

(a) The transmission of some primary DPoA elements (as set out in s.6.12) in a signal DPoA reveal between devices utilising near field communication (NFC) capabilities; and/or
(b) The display of a one-time code in accordance with s.6.19 – s.6.25.

6.12 The transmission of a signal from the device utilising near field communication in accordance with 6.11(b) or the display of a one time code in response to a code activation shall not contain personally identifiable information nor any secondary DPoA elements (unless authorised by the user), but may consist of:

(a) The first four digits of the Accredited Provider's User Identification Number (indicating the DPoA Provider);

(b) The Age Identifier;
(c) The Coordinated Universal Time (UTC);
(d) The Validation Symbol (or an electronic representation of it);
(e) A validation code or location code relating to the source of the code activation (s.6.8)
(f) The one-time code.

6.13 Where a user has set appropriate permissions or given user consent, the transmission of a signal from the device utilising near field communication in accordance with 6.11(b) or the display of a one time code in response to a code activation may contain secondary DPoA elements, including:

(a) The name of the user;

(b) The date of birth of the user;

(c) The full Accredited Provider's User Identification Number.

Note: If including the date of birth in the signal transmission, it should be in the format required by ISO 8601-1:2019 – Date and time – Representations for information interchange – Part 1: Basic rules

6.14 The display of the DPoA elements shall be for a maximum of 60 seconds. After this:

(a) the display shall revert to the pre-reveal stage;
(b) the transmission of any signal under s.6.11 (a) shall cease; and
(c) the one time code displayed under s.6.11 (b) shall cease to be valid

6.15 Where the user is a child, the background of the DPoA elements and guilloche shall be green in accordance with s.5.42.

6.16 Where the user is an adult the background of the DPoA elements and guilloche shall be blue in accordance with s.5.43.

Biometric User Authentication

6.17 A Biometric User Authentication required for DPoA signal transmission (s.6.11 (a)) or display of a one-time code (s.6.11 (b)) shall consist of ensuring that:

(a) The presenter of the DPoA device is authenticated as the user through a biometric authentication process as described in s.6.18; and

(b) The presenter of the DPoA is subject to liveness detection as described in s.6.19.

6.18 A biometric authentication process shall require a false accept rate (FAR) and false reject rate (FRR) of less than 1% for:

(a) landmark point matches of any landmark point types if utilising face image data. These can include MPEG4 Features, Anthropometric 2D or 3D landmarks;
(b) ridge counts, core and delta location matches if utilising dactyloscopy (fingerprint) image data; or
(c) appropriately similar matches if utilising other biometric authentication processes (such as iris, geometry or finger vein analysis, for instance).

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

Dactyloscopy ridge count, core and delta location point analysis is described in ISO/IEC 19794-2:2011 - Information technology — Biometric data interchange formats — Part 2: Finger minutiae data.

6.19 Liveness detection shall be in accordance with ISO/IEC 30107 – Information Technology – Biometric presentation attack detection.

One Time Code

6.20 A DPoA system may provide for the creation of a one-time code intended for use in embedded age verification systems.

6.21 If provided, the one-time code shall display on screen (when permitted by these technical requirements):

(a) if in text, in a suitably clear font; or
(b) as a matrix barcode

6.22 The one-time code shall be cryptographically protected.

6.23 The one-time code shall be transmitted to the Accredited Provider's system by an encrypted signal, or detected by a camera, scanner or capture device held by the relying party.

6.24 When entered into a portal operated by the relying party, validation of the one-time code with the Accredited Provider's system can reveal the Age Identifier of the User.

6.25 The one-time code shall display on screen and be valid for a maximum of 60 seconds.

(a) .

DPoA Usage Logs

6.26 The Accredited Provider may receive a log (instantaneously or aggregated periodically) of the use of the DPoA which shall not contain any secondary DPoA elements or personally identifiable information, but may contain:

(a) The source of the signal activation;
(b) The matrix barcode used to establish a code activation;
(c) The device to which a signal transmission took place after the DPoA reveal;
(d) The Coordinated Universal Time (UTC) (which for practical purposes, Accredited Providers may wish to convert to local time for user interfaces).

Note: This may enable the Accredited Provider to track the usage of the DPoA by different relying parties in different locations (and establish fees for their services) without revealing the personal information or tracking the activities of individual DPoA users.

6.27 The relying party may establish a log of the use of the DPoA by reference to keeping a record of:

(a) The Coordinated Universal Time (UTC) (which for practical purposes, Accredited Providers may wish to convert to local time for user interfaces);
(b) The signal transmission following the DPoA reveal to suitable near field communication equipment maintained by the relying party or may be an application programme interface (API) provided for the purpose as incorporated into an app downloaded to the relying party's own device or into devices or

equipment used by the relying party (such as electronic point of sale systems (ePOS) or payment processing equipment);

(c) Obtaining the One Time Code and validating that by arrangement with the Accredited Provider;

(d) Manually entering a record on electronic systems (such as an electronic point of sale (ePOS) device), that a DPoA reveal procedure has taken place and the user was verified as being over the appropriate age eligibility by reference either to the Age Identifier or the Date of Birth revealed;

(e) Entering a record on a manual refusals register or log.

6.28 The Relying Party may, if required by regulatory authorities, maintain a log of DPoA secondary elements (such as name, date of birth and the full Accredited Provider's User Identification Number) only where s.6.13 applies. This shall be limited to the purpose established by the regulatory authorities and set out in writing, such as in licensing conditions. The Accredited Provider shall secure that their systems limit the collation of such data to these requirements. If a relying party wishes to collect additional data about visitors to their premises (such as for marketing or other non-regulatory purposes) they shall have a separate user data capture process for that otherwise than through the PASS DPoA process.

6.29 The Accredited Provider may provide a facility for the User to maintain a log within the DPoA app of:

(a) Each time there is a signal or code activation;

(b) Where known, the relying party or location that the activation was requested;

(c) The Coordinated Universal Time (UTC) (which for practical purposes, Accredited Providers may wish to convert to local time for user interfaces).

7. Security Features and Presentation Controls

Security Controls

7.1 Accredited Providers shall take steps to secure the integrity of the DPoA. This means preventing any element of the DPoA, or the DPoA in its entirety, from being copied, altered, substituted or replicated to the fullest extent possible within the technical limitations of the platform.

Note: Accredited Providers and their sub-contractors are encouraged to follow the advice and guidance of the National Cyber Security Centre on implementation of their DPoA plans.

7.2 When developing a DPoA app, Accredited Providers should seek to make use of any security mechanisms that are built into the platform for which they are developing. They should be aware of many of the common security issues that the DPoA app may fall victim to, in order to protect the DPoA from compromise.

7.3 Accredited providers shall ensure that any DPoA elements stored on a device are secured within any encrypted data storage facility provided on the operating system of the device. Most mobile platforms provide documented APIs that allow data to be stored at different levels of security.

7.4 All DPoA elements shall be encrypted while not in use.

7.5 Access to all DPoA elements shall be guarded by an authentication mechanism in accordance with s.4.5.

7.6 All DPoA elements shall be securely removed, when no longer required on the device. The forced removal of associated files when uninstalling an app shall be enabled (this is enabled by default for most operating systems).

7.7 The DPoA app, in live deployment, shall not be configured to run on an app simulator (i.e. without device binding in accordance with paragraph 4.6). The Accredited Provider or their sub-contractor shall be permitted to run the DPoA app in test configuration on an app simulator.

Cryptography

7.8 Any DPoA elements being transferred between device and server shall be sent over an appropriate encryption mechanism.

Note: Supported ciphers should be restricted on both ends of the communication so that only strong ciphers may be used. Additional steps should be taken in order to maximise the security of the data connection. SSL Pinning for example, would allow the application to be restricted so that it may only form secure connections to a host with a known, trusted certificate.

7.9 DPoA elements shall not be transmitted over an unencrypted connection.

7.10 The encryption keys shall not be stored in the same location as the DPoA elements.

7.11 Accredited Providers should implement an additional layer of data encryption before using data storage APIs provided on a device to help protect DPoA elements in the event that an attacker has compromised the host device.

Note: Storing any cryptographic keys on the device will reduce the effectiveness of an additional cryptographic layer, as keys stored locally could be recovered from the device (though these keys could be combined with a user credential to strengthen them). Storing the keys on a remote server would prevent an attacker with physical access to the device from retrieving them, though would require the application to authenticate to the server, and have an internet connection.

Session Handling

7.12 Accredited Providers shall implement appropriate controls on the backend server to which the DPoA application connects.

7.13 The backend server shall treat the DPoA application as an untrusted entity; only allowing it access to DPoA elements when authenticated.

7.14 The backend server shall enforce a session timeout within a maximum of 15 minutes, requiring the DPoA application to reauthenticate.

7.15 The DPoA application shall enforce a session timeout within a maximum of 15 minutes, requiring the user to reauthenticate.

Stack Protection

7.16 Accredited Providers shall take advantage of any stack protection mechanisms that are available to the platform. Features such as Address Space Layout Randomisation (ASLR) and Stack Canaries should be enforced during compilation in order to make the application more difficult to exploit.

7.17 Accredited Providers shall take steps to make the DPoA application more difficult to reverse engineer.

Note: Using a non-reflection based language such as C to perform sensitive actions will require more effort from an attacker to modify its logic at runtime. Accredited Providers should be careful when implementing this however, as using an unmanaged language can open up the application to memory corruption vulnerabilities.

7.18 Accredited Providers shall implement obfuscation techniques to make the application more difficult to reverse engineer, such as use code obfuscation tools and anti-debugging capabilities.

7.19 Accredited Providers shall take steps to identify jailbroken or rooted devices.

Note: Jailbroken or rooted device detection will always be subject to circumvention by a determined attacker, however tests for common jailbreak/rooting methods allows for the application to take appropriate steps, such as by implementing processes for contra indicators.

Attack Detection

7.20 Accredited Providers shall implement processes and procedures for DPoA system attack detection.

7.21 Accredited Providers shall implement processes to avoid or obstruct brute force attack. This shall include the use of suitable length cryptographic keys and restricting user authentication attempts before account suspension.

7.22 Accredited Providers shall implement appropriate end point authentication to avoid or obstruct man-in-the-middle attacks.

7.23 Accredited Providers shall implement processes to identify repeated presentation attack, multiple failed attempts at biometric authentication and attempts to alter the values or appearance of DPoA elements.

Screen Recording

7.24 Accredited Providers shall implement processes to identify and restrict screen recording or screen capture of a revealed DPoA.

7.25 Screen recording or screen capture shall be treated as a contra indicator and result in account suspension.

Contra Indicators

7.26 Accredited Providers shall treat security breaches caused by users as contra indicators in accordance with PASS 0, 4.4 (confident so they are sure).

Penetration Testing

7.27 Accredited Providers shall conduct penetration testing of their DPoA and associated systems in accordance with the guidance on penetration testing issued by the National Cyber Security Centre.

8. Customer Care and Support

Supporting DPoA Users

8.1 In addition to the requirements for Customer Care set out in PASS 0, 4.17 – 4.22, Accredited Providers shall provide DPoA Users with support services.

8.2 The information required by PASS 0, 4.20 (publicly available information) shall be available within the DPoA app.

8.3 Accredited Providers shall provide the facility for DPoA users to recover a suspended account.

8.4 Accredited Providers shall provide the facility for DPoA users to request an update to their DPoA elements, which if associated with their identity or age verification, shall be re-established in accordance with PASS 1 (Identity and Age Verification).

8.5 Accredited Providers shall take reasonable steps for enabling users with additional needs to make use of the DPoA, including making reasonable adjustments as appropriate. Users with additional needs may be living with disability, poor literacy skills, lack of knowledge or understanding of the DPoA process, who are using the DPoA at a particular time of stress or distress, or who use English as a second language or not at all.

Account Suspension or Closure

8.6 An Accredited Provider shall provide for account recovery mechanisms following account suspension.

8.7 An Accredited Provider may close an account if:

(a) The user makes a request for the account to be closed;
(b) The Accredited Provider has reasonable grounds to believe that the account has been used fraudulently;
(c) The Accredited Provider has reasonable grounds to believe that there are unresolved contra indicators present that mean the Accredited Provider can no

longer comply with the requirements of PASS 0, s.4.4 (confident so that they are sure) with regard to the user identity or age verifications;

(d) The Accredited Provider has reasonable grounds to believe that the user has breached the terms and conditions of use of the DPoA, including attempts to breach the security and integrity of the DPoA elements or system;

(e) The Accredited Provider has reason to believe that the user has died; or

(f) The Accredited Provider is instructed by a competent governmental authority or court to close the account.

App Support Tools

8.8 An Accredited Provider should incorporate the following tools within their DPoA app:

(a) provide a means for users to send messages to the Accredited Provider from within the app;

(b) provide in-app facilities for frequently asked questions;

(c) provide a means for support tickets to be raised, monitored and followed up;

(d) provide in-app facilities for monitoring the progress of support tickets;

(e) provide tools for users to exercise their data rights; and

(f) allow users to easily cancel their subscription or DPoA service.

About PASS

The PASS Scheme is operated by a Community Interest Company providing accreditation to suppliers of Proof of Age Services 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 or digital proof of age 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 or digital proof of age that carries a PASS hologram will have been issued by a provider who has been through a stringent application and accreditation process.

Reliability

The unique PASS hologram is a registered Trademark, making it a criminal offence to manufacture cards or provide digital proof of age applications that have a mark similar to the PASS one.

Confidence

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

Support

Possession of a PASS accredited card or digital proof of age 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