Digital Scotland
Digital Identity Scotland

Digital Identity Scotland

Outline In-person Identification Requirements

Version 0.1 Work in Progress
Date 6th March 2019

Document Status
This is a work-in-progress document and is subject to change.

Digital Scotland

Digital Identity Scotland

Contents

1. Introduction

1.1. Scope

This document proposes the high level requirements for an in-person checking service, as part of the service offered by Digital Identity Scotland.

In-person checks can provide a means to establish the identity of an individual where doing so digitally is not possible. This could be because the person concerned does not have an existing digital footprint (e.g. financial history) or to support cases where the person needs assistance in completing the process.

An in-person process may also provide the opportunity to issue the person with an authentication credential, if that has not already been done through some other means.

1.2. Status

Work in progress

1.3. Audience

Scottish Government and OIX Alpha Participants

2. Requirements

2.1. Objective of in-person checks

To enable the digital identity account belonging to a person to achieve LoA2.

2.2. Sequencing of in-person checks

In-person checks could occur at different points in the user journey depending on the service being accessed and previous use of digital identity services by the individual.

In-person checks can be triggered in several places. For example:

- Individual advised to complete in-person process by relying party as part of application for a service.
- Individual advised to complete in-person process by identity provider.

The individual's digital identity could be in one of several states. For example:

- Individual has had no previous interaction with Digital Identity Scotland (included for completeness but probably not a supported scenario – see next bullet)
- Individual has created an identity account (with an IDP) and has been issued with an LoA1 authentication credential e.g.
- Individual has created an identity account (with an IDP) and has been issued with an LoA2 authentication credential e.g.

2.3. Initiating in-person check

When an in-person check is required, the individual will be provided with the following information:

- Where to go to complete the in-person check
- The date(s) and time(s) that the individual should attend the in-person check
- A list of the items the individual should take with them to the in-person check[1]
- What the individual should do if they do not have the necessary items
- A transaction reference that will be used to link the request to attend an in-person check, with the in-person check process itself. The individual will need to take this reference with them.

[1] Care should be taken to ensure all options are clearly defined.

2.4. Evidence that can be presented in an in-person check

The evidence that a person will be required to present is determined by the requirements described in GPG 45. It defines a number of profiles as follows. These define different combinations of evidence that can be presented to achieve LoA2, depending on the strength of the evidence.

GPG 45 Profile	Evidence Strength
Medium Profile 1	Requires 1 item with score 4
Medium Profile 2	Requires 1 item with score 3
Medium Profile 3	Requires 2 items with score 2
Medium Profile 4	Requires 1 item with score 3 and another with score 2
Medium Profile 5	Requires 2 items with score 3
Medium Profile 6	Requires 3 items with score 2

Refer to GPG 45 for more detail on the characteristics of identity evidence at each level.

2.5. In-person validation and verification processes

GPG 45 describes the characteristics of the validation and verification processes that can be used to determine the scores associated with the validation and verification processes.

The validation and verification processes that are required are determined by profiles defined in GPG 45, as follows:

GPG 45 Profile	Required Validity Score	Required Verification Score
Medium Profile 1	3	3
Medium Profile 2	3	3
Medium Profile 3	Score 2 for each evidence item	3
Medium Profile 4	Score 3 for the evidence item with strength 3 Score 2 for the evidence item with strength 3	2
Medium Profile 5	Score 2 for each evidence item	3
Medium Profile 6	Score 2 for each evidence item	2

Refer to GPG 45 for more detail on the characteristics of identity evidence at each level

2.6. Alternative methods of Identity Validation and Verification

In the event that an in-person process cannot be completed in line with the requirements outlined in this document, it may be possible to employ alternative methods, such as:

- Trust escalation – achieving a lower LoA from the in-person process and then building trust in the person's identity over time as transactions are performed and services provided.
- Biographical checks – ask questions about the person's story that can be corroborated by third parties, e.g. employers, embassies, landlords etc

- Online service access – witness the person accessing an online service (e.g. personal banking) during an in-person check.
- Corroboration – corroborate the claimed identity with the person's parents or guardian
- Notarised Passport Photo – for when the person is unable to provide identity evidence that contains a photo.

The requirements and rules for the use of alternative methods are to be defined.

3. Validation

3.1. Capabilities required to meet GPG 45 Requirements

In-person validation can be used to satisfy the validation requirements of GPG 45.

In order to achieve LoA2, in-person validation should be capable of meeting the requirements to achieve a score of 2 or 3. The score that is required will depend on the identity profile being used to achieve LoA2.

The following table summarises the capabilities required to achieve a score of 2 or 3

Key Process	**Key Required Capabilities**	**Score 2**	**Score 3**
Confirm the evidence is valid	• Connectivity to evidence issuer	One of these	All of these
Use natural light to confirm any physical security features on the evidence are genuine	• Scripted and auditable in-person process • Staff trained to detect false documents • Appropriate technology to examine physical documents		
Use ultraviolet (UV) or infrared (IR) light to confirm any physical security features are genuine	• Scripted and auditable in-person process • Staff trained to detect false documents • Appropriate technology to examine physical documents		
Confirm the cryptographic security features are genuine	• Appropriate technology to read and validate cryptographic information	Not applicable	Alternative process

The detailed relevant requirements from GPG 45 are provided verbatim in Appendix B, for convenience.

4. Verification

4.1. Capabilities required to meet GPG 45 Requirements

In-person validation can be used to satisfy the validation requirements of GPG 45.

In order to achieve LoA2, in-person validation should be capable of meeting the requirements to achieve a score of 2 or 3. The score that is required will depend on the identity profile being used to achieve LoA2.

The following table summarises the capabilities required to achieve a score of 2 or 3

Key Process	**Key Required Capabilities**	**Score 2**	**Score 3**
Make sure someone matches the photo in-person	• Scripted and auditable process • Staff trained to detect imposters • Staff trained to detect false documents (only required for score 3) • Good lighting	One of these	One of these
Make sure someone matches biometric information	• Appropriate technology to perform biometric comparison • Staff trained to operate technology correctly		
Asking the person to complete dynamic KBV challenges	• Access to appropriate data sources to generate KBV questions		

The detailed relevant requirements from GPG 45 are provided verbatim in Appendix C, for convenience.

5. Credential Issuance and Binding

5.1. Credential Issuance

An in-person process may, in some cases, be an appropriate place to issue an authentication credential to the individual.

[Need to expand this]

5.2. Credential Binding

Depending on the status of the individual's digital identity account (see section 2.2) it may be necessary for the in-person process to include an binding process, to link the in-person check to the individual's digital identity account and the associated credential.

[Need to expand this]

6. Appendix A – In-person Proofing Checklist

Item	Response
Identity Evidence	
Score 4 Identity Evidence supported	[List Evidence Types]
Score 3 Identity Evidence supported	[List Evidence Types]
Score 2 Identity Evidence supported	[List Evidence Types]
Score 1 Identity Evidence supported	[List Evidence Types]
Validation	
Connectivity to evidence issuer	[Yes/No]
Scripted and auditable process	[Yes/No]
Staff trained to detect false documents	[Yes/No]
Appropriate technology to examine physical documents	[Yes/No]
Appropriate technology to read and validate cryptographic information	[Yes/No]
Verification	
Scripted and auditable process	[Yes/No]
Staff trained to detect imposters	[Yes/No]
Staff trained to detect false documents (only required for score 3)	[Yes/No]
Good lighting	[Yes/No]
Appropriate technology to perform biometric comparison	[Yes/No]
Staff trained to operate technology correctly	[Yes/No]
Access to appropriate data sources to generate KBV questions	[Yes/No]
Credential	
Issuance	[List types of credential that could be issued]
Binding	[List types of credential for which binding could be performed]
Alternative methods of Identity Validation and Verification	
Alternative methods	[List potential alternative methods]

7. Appendix B – Validation Requirements from GPG 45

This section provides an extract of the relevant requirements from GPG 45 to achieve a score of 2 or 3 for an in-person validation process.

7.1. Score 2

The evidence will have a score of 2 if you do **one** of the following:

- confirm the evidence is valid
- use natural light to confirm any physical security features on the evidence are genuine
- use ultraviolet (UV) or infrared (IR) light to confirm any physical security features are genuine

7.1.1. Confirm the evidence is valid

The person or system doing the check can confirm the evidence is valid by making sure the details on it match those held by either:

- the organisation that issued it
- another authoritative source

7.1.2. Use natural light to confirm the physical security features are genuine

The person or system doing the check will need to make sure:

- they're checking the original evidence the evidence has not expired
- they don't accept scans, photo uploads or photocopies (this is because these are easier to forge or counterfeit) the evidence was shared with the person or system in a way that protects it from being altered (for example it could be sent by secure delivery)
- the evidence (or the image or video of the evidence) is clear enough to be able to examine its security features

If any of the following features are on the evidence, the person or system will also need to check they're correct against official templates, such as the Public Register of Authentic travel and identity Documents Online (PRADO):

- background printing
- fonts and alignment
- holograms and positioning
- the way it's been laminated
- designs printed with optical variable ink (and check they look the way they should at certain angles)
- the format of any 'compound identifiers', such as a Driver and Vehicle Licensing Agency (DVLA) driver number or a machine-readable zone (MRZ)
- the position of any photographs on the evidence (they should not have been replaced or edited)

If the evidence is being checked by a person, they must:

- be trained in how to detect false documents by a specialist trainer, such as the Home Office, National Document Fraud Unit or Centre for the Protection of National Infrastructure (CPNI)
- refresh their training at least every 3 years

If the evidence is being checked by a system, it must:

- have been built following good practice, such as the Home Office's guidance on identification document validation technology
- update the templates it checks the evidence against at least every 3 years

7.1.3. Use UV or IR light to confirm the physical security features are genuine

The person or system doing the check will need to make sure:

- the evidence has not expired
- the paper the evidence is printed on looks the way it should
- the alignment of the evidence looks the way it should
- any fluorescent features (such as fluorescent inks or fibres) look the way they should
- the evidence has not been altered (for example a UV light will show where UV features have been covered by glue if something has been stuck on the evidence)

If any of the following features are on the evidence, the person or system will also need to check they're correct against official templates, such as the Public Register of Authentic travel and identity Documents Online (PRADO):

- background printing
- fonts and alignment
- holograms and positioning
- the way it's been laminated
- designs printed with optical variable ink (and check they look the way they should at certain angles)
- the format of any 'compound identifiers', such as a DVLA driver number or a MRZ
- the position of any photographs on the evidence (they should not have been replaced or edited)

If the evidence is being checked by a person, they must:

- be trained in how to detect false documents by a specialist trainer, such as the HomeOffice, National Document Fraud Unit or CPNI
- refresh their training at least every 3 years

If the evidence is being checked by a system, it must:

- have been built following good practice, such as the Home Office's guidance on identification document validation technology
- update the templates it checks the evidence against at least every 3 years

7.2. Score 3

There are 2 ways the evidence can have a score of 3.

It will have a score of 3 if you check the evidence is both genuine and valid. You can do this by doing **all** of the following:

- confirm it's valid
- use natural light to confirm the physical security features on the evidence are genuine
- use UV or IR light to confirm the physical security features are genuine

Alternatively, you can do this by checking the cryptographic security features are genuine .

7.2.1. Confirm the evidence is valid

The person or system will need to do the same checks to confirm the evidence is valid that are needed at score 2.

7.2.2. Use natural light to confirm the physical security features are genuine

The person or system will need to do the same natural light checks to confirm the evidence is genuine that are needed at score 2.

They'll also need to:

- use evidence that's been shared in a way that prevents it from being 'replayed' (intercepted and reused)
- make sure any shadows or glare do not stop the security features on the evidence from being examined
- update any official templates that are used (such as those from PRADO) every year
- if the checks are being done by a person, they'll need to refresh their training in how to detect false documents every year

They must also confirm:

- designs printed using intaglio (raised) ink look the way they should
- designs that have been laser etched look the way they should
- features are consistent and correct across sections of the evidence

To check this, they must use one of the following:

- a magnification tool (such as a magnifier)
- other inspection equipment used to identify forged or counterfeit documents

7.2.3. Use UV or IR light to confirm the physical security features are genuine

The person or system will need to do the same UV or IR light checks to confirm the evidence is genuine that are needed at score 2.

They'll also need to:

- use evidence that's been shared in a way that prevents it from being 'replayed' (intercepted and reused)

- make sure any shadows or glare do not stop the security features on the evidence from being examined
- update any official templates that are used every year if the checks are being done by a person, they'll need to refresh their training in how to detect false documents every year

7.2.4. Confirm the cryptographic security features are genuine

To make sure the cryptographic security features are genuine, the system that checks the evidence will need to:

- make sure the evidence has not expired
- read the cryptographically protected data
- provide any required cryptographic keys
- check the digital signature is correct
- check the signing key belongs to the organisation that issued the evidence
- check the signing key is the correct type for that evidence
- check the signing key has not been revoked

8. Appendix C – Verification Requirements from GPG 45

This section provides an extract of the relevant requirements from GPG 45 to achieve a score of 2 or 3 for an in-person verification process.

8.1. Score 2

The person will get a score of 2 if you do **one** of the following:

- make sure the person physically matches the photo on (or associated with) the strongest piece of genuine evidence you have of the claimed identity (you can do this in-person or remotely)
- make sure the person's biometric information (such as their face or fingerprints) matches biometric information from (or associated with) the strongest piece of genuine evidence you have of the claimed identity
- ask the person to complete multiple 'dynamic' KBV challenges that only the claimed identity should be able to do

8.1.1. Make sure someone matches the photo in-person

The person doing the match must have:

- been trained in how to detect impostors
- good enough eyesight (with or without prescription lenses) to effectively compare the person to the image

When doing the match, you must make sure:

- the person whose identity is being checked is present
- the light conditions are good enough to clearly see the person and the image on the evidence (for example there should be no obscuring glare)
- if the photo is taken from a piece of evidence, it must not have been tampered with

The person whose identity is being checked must not:

- be wearing a head covering (unless it's for religious or medical reasons)
- have their eyes closed
- have anything covering their face or eyes (such as shadows or their hair)

8.1.2. Make sure someone matches the photo remotely

[These requirements not applicable to an in-person process]

8.1.3. Make sure someone matches biometric information

When doing the biometric comparison, you must make sure:

- your 'false match rate' (how many people you falsely match who aren't the claimed identity) and 'false non-match rate' (how many people you reject who are the claimed identity) are appropriate for your security and usability needs
- you match the person to biometric information that's known to belong the claimed identity (this is known as 'one-to-one verification')

- the biometric information has not been tampered with (if it's taken from a piece of evidence)
- the system can identify if the person's biometric information has been intercepted and reused ('replayed')
- the biometrics have been shared in a way that prevent them from being tampered with
- the person successfully completes a test to confirm they're real (known as a 'liveness' test)
- the system can identify if someone's using an artefact to convince the system they're someone else (known as 'spoofing') - this could mean making sure they're not holding up a photo or playing a recording of someone's else's voice if you're checking a facial or vocal biometric

8.1.4. Asking the person to complete dynamic KBV challenges

To be 'dynamic', the answers to a KBV challenge must change over time. This will make it harder for impostors using information from things like data breaches to successfully complete the challenge.

The KBV challenges must follow the same quality rules that should be followed to get a score of 1.

The KBV challenges must also not be based on data from a single source. An account and a mortgage from the same bank count as different sources if the claimed identity went through a different application process to get each one.

How many KBV challenges you ask the person to complete depends on the quality of the questions. You should ask them to complete one of the following:

- 4 low quality KBV challenges
- 2 medium quality KBV challenges
- 2 high quality KBV challenges
- 8 low quality multiple choice KBV challenges
- 3 medium quality multiple choice KBV challenges
- 2 high quality multiple choice KBV challenges

8.2. Score 3

The person will get a score of 3 if you do **either** of the following in-person or remotely:

- make sure the person physically matches the photo on (or associated with) the strongest piece of genuine evidence you have of the claimed identity
- make sure the person's biometric information matches biometric information from (or associated with) the strongest piece of genuine evidence you have of the claimed identity

8.2.1. Make sure someone matches a photo in-person or remotely

The person doing the match must have all the skills and training needed to get a score of 2.

They must also:

- have been trained in how to detect false documents by a specialist trainer, such as the Home Office, National Document Fraud Unit, Centre for the Protection of National Infrastructure (CPNI)

- refresh their training at least every 3 years

The person or system doing the match must do everything needed to check someone matches a photo (in-person or remotely) at score 2. You must also make sure:

- your process has a way to identify if someone is wearing a mask, makeup or prosthetics to look like someone else
- if the person is wearing glasses, their eyes are visible without any glare or reflections

8.2.2. Make sure someone matches biometric information

The system doing the match must do everything needed to check someone matches biometric information at score 2. It must also:

- have a false match rate that's a lot lower than its false non-match rate and has been chosen to increase the security of the biometric matching process
- use a biometric algorithm that's been proven to be effective by testing it against a recognised benchmark, like the National Institute of Standards and Technology's (NIST's) face recognition vendor test guidance
- make sure the person's biometric information is captured under conditions that do not reduce the accuracy of the type of biometric check being used (things like light, noise, and humidity impact the success rates for different types of biometric and should be adjusted if needed)
- be able to identify when someone's spoofing the system using an artefact that's taken time, money and effort to create - this could mean making sure the person is not using a 3D printed mask of someone's likeness or changing the pitch and adding background noise to a recording if you're checking facial and vocal biometrics
- ask the person to complete unpredictable tests to confirm they're real (known as a 'liveness' test)