



Digital Vouch with Photo

An OIX Proposal | July 2022 | Version 1.0

Produced by: Nick Mothershaw, Chief Identity Strategist

OPEN IDENTITY EXCHANGE

The Open Identity Exchange vision is a world where we can all prove our identity and eligibility anywhere, using a simple universally trusted ID.

We create a community for all those involved in the ID sector to connect and collaborate. Together we create the rules, tools and confidence to support the acceptance of universally trusted IDs and eligibility information.

We are uniquely dedicated to ID Trust. We are a membership organization, offering education, information and collaboration around the topic of universally trusted identity.

We bring together buyers of ID Services (reliant organizations, or Relying Parties) with ID Service organizations such as tech vendors, consultancies, along with regulators and market influencers to work together to drive adoption of ID Trust.

Our guides and papers form the bedrock of Trust Frameworks to support the creation and use of interoperable, universally trusted identities.

OIX has a wide programme of events, thought-leadership and working groups. Members access a suite of resources including support for Pilot Projects and Business Case Development.

Contact:

Nick Mothershaw, Chief Identity Strategist

nick.mothershaw@openidentityexchange.org

DOCUMENT HISTORY

Version	Comments	Author	Date
1.0	Initial release	Nick Mothershaw	01/06/2022

CONTENTS

1	INTRODUCTION.....	3
2	PURPOSE.....	3
3	HOW DOES A DIGITAL VOUCH WORK?	4
4	ASSUMPTIONS	4
5	HOW WOULD THIS WORK?.....	5
5.1	STEP 1 – VOUCHER CREATES A DIGITAL VOUCH WITH PHOTO USING THEIR OWN PERSONAL DIGITAL ID.....	5
5.2	STEP 2 – VOUCHEE USES THE DIGITAL VOUCH WITH PHOTO TO CREATE THEIR OWN PERSONAL DIGITAL ID	6
5.3	ALTERNATIVE FLOW 1	6
5.4	ALTERNATIVE FLOW 2	6
6	SCORING OF THE DIGITAL VOUCH WITH PHOTO IN AN ASSURANCE POLICY.....	7
7	REFLECTIONS ON THIS PROPOSAL	8
8	IMPLEMENTATION CONSIDERATIONS	9

1 Introduction

The ability for all those who wish to have a Digital ID to be able to obtain one is a key principle in ID ecosystems. This means that all potential users must be able to go through an issuance or enrolment process for a Digital ID.

In some countries, Digital IDs are issued directly to citizens by the government, often through a face-to-face process, based on the government's relationship with the individual. This is an inclusive approach to Digital ID enrolment where government have comprehensive records on all their citizens.

However, there are many circumstances where users cannot readily prove who they are in order to obtain a Digital ID. For example, where:

- there is no comprehensive central government record for all citizens,
- the enrolment process for Digital ID is through digitization of pseudo ID documents, such as passports or driving licences, which not all citizens have.
- evidence of an individual's existence in databases, such as credit databases, is relied upon as part of the proofing process
- the possession of a bank account is a key factor in ID enrolment.

Individuals without such information are described by OIX as being "ID Challenged". OIX has identified that in the UK around 11% of the adult population are ID Challenged. In other countries with lower passport and driving licence holding rates, and no "positive" credit databases, this may be much higher.

Vouching is a process to bring the ID Challenged into the Digital ID Ecosystem. This process involves a person who is already trusted legally, vouching for another individual they have known for some time.

In the UK for example, the Digital Identity and Attribute Trust Framework supports the use of vouching. The use of vouching is currently limited to two parts of the proofing process:

- Evidence
- Activity

However, as the framework is currently drafted, a Vouch cannot be used for:

- Identity Fraud
- Verification

With this restriction on the use of a Vouch for Verification, how will the ID challenged, who have no photo ID Document and no Data for KBVs, be able to assure their identity to the levels of confidence defined in by the UK Trust Framework?

This discussion paper explores how a Vouchers assured Digital ID could be used to create a "Digital Vouch with Photo" that the Vouchee can then use as a **Validation and Verification** proof to create their own assured Digital ID.

This process could be applied in any Trust Framework across the globe. The legal status of the Vouch may need to be supported by local legislation, with consequences on the Voucher for a fraudulent vouch being clear.

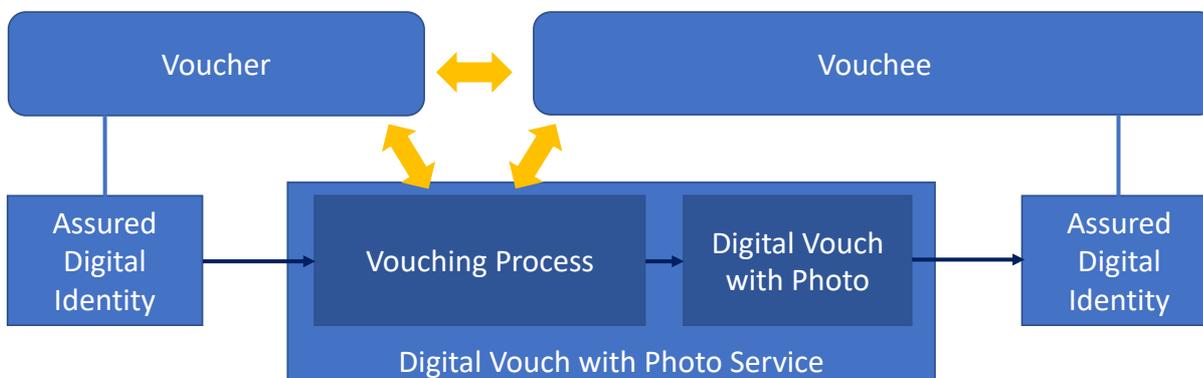
2 Purpose

The purpose of this document is to propose a process for the creation and use of a Digital Vouch to enable a more inclusive Digital ID ecosystem.

This document also explores the legal and commercial considerations for those considering implementing Digital Vouching.

3 How does a Digital Vouch work?

The Voucher and Vouchee both interact with a Digital Vouch with Photo Service to create a Digital Vouch with Photo:



The Voucher will already have a Digital ID assured by the trust framework. The level of assurance for the Voucher should be a high level of trust, to mitigate impersonation risk by Vouchers.

The Voucher and Vouchee will interact with each other in a Vouching Process, the result of which is a Digital Vouch with Photo. This is essentially a credential issued to the Vouchee by the Digital ID with Photo Service with the Voucher playing the role of authoritative source.

There are several alternatives as to how the vouching process might work, which are explored further below.

The Vouchee can then use the Digital Vouch with Photo as a 'root of trust' credential to create their own assured Digital ID.

4 Assumptions

The implementing Trust Framework (e.g., the UK Digital Identity and Attribute Trust Framework) recognizes a "Digital Vouch with Photo" from a "Digital Vouch with Photo Service" as a source of evidence.

A "Digital Vouch with Photo Service Provider" could be a certified role within the Trust Framework. Identity Providers (IdPs) might also play this role alongside their general services.

The Digital Vouch with Photo Service Provider must meet record keeping requirements for the trust framework, for example to retain the data of the Voucher and Vouchee for a minimum of number years.

The Voucher has a smart phone.

5 How would this work?

5.1 Step 1 – Voucher creates a Digital Vouch with Photo using their own personal Digital ID

Pre-requisites:

The Voucher has a Digital ID assured to trust framework defined Level of Assurance (for example under the UK Trust Framework a High GPG45 Level of confidence with GPG44 High Protection credentials).

The Voucher uses a trust framework certified “Digital Vouch with Photo Service”. These may be provided by IdPs or specialist third party services linked to an Identity Provider service(s) (this link is important for the vouch to be traced back to the vouchers Digital ID).

Digital Vouch with Photo creation Process

1. The Voucher uses a “Digital Vouch with Photo Service” to create the Digital Vouch with Photo.
2. The Voucher logs on to the “Digital Vouch with Photo Service” with their Digital ID.
3. The Voucher enters key Personally Identifiable Information (PII) for the Vouchee:
 - Full Name
 - Current Address
 - DoB
 - Email address
 - Phone Number
4. The Digital Vouch with Photo Service verifies Vouchee control of email or phone number, for example by sending a link or one time code.
5. The Voucher takes a photo of the Vouchee using the “Digital Vouch with Photo Service” to a defined standard on a secure platform. This necessitates a face-to-face interaction between the Voucher and the Vouchee. This photo taking process must include a liveness check to trust framework standards built into the Digital Vouch with Photo service.
6. The Voucher declares:
 - Who they are, using PII taken from their Digital ID
 - They have the authority vouch*.
 - They understand the criminal consequence of a false vouch.
 - That the PII they have provided about the Vouchee is correct.
 - How long they have known the Vouchee (which contributes to a measure of “Activity” in a identity assurance process) and in what capacity (e.g. professional, community).
 - That the photo they have taken was live and is a true likeness of the Vouchee.
7. The “Digital Vouch with Photo Service” creates a “Digital Vouch with Photo” containing the Vouchee’s PII, the photo of the Vouchee and the vouchers declarations. This “Digital Vouch with Photo” is signed by the “Digital Vouch with Photo service provider” and contains the Vouchers signature from their Digital ID. *(There would be a number of technical optional here (e.g. digital certs, verifiable credentials, QES) – needs further discussion.)*
8. The “Digital Vouching with Photo Service” sends the Vouchee an email with a link / code for their Digital Vouch with Photo. (Or this could be delivered to the Vouchee as a credential in their wallet).

Result: The Vouchee has a Digital Cryptographically signed Photo ID issued by a Trust Framework recognised issuer and authoritative source.

** - Ideally verification that the Voucher has the authority to vouch, for example is of the correct profession to vouch, should be formalized. The authority to vouch is a critical part of the liability model. For example, the Voucher could have a credential in their Digital ID that allows them to prove the role they have, which could be issued by an authoritative source such as a professional body.*

5.2 Step 2 – Vouchee uses the Digital Vouch with Photo to create their own personal Digital ID

1. The Vouchee chooses an ID Provider who accepts a Digital Vouch with Photo.
2. The Vouchee enters their key PII:
 - Full Name
 - Current Address
 - DoB
 - Email address
 - Phone Number
3. The Vouchee pastes the link / code for their digital vouch into the IDPs evidence collection process (or presents their Digital Vouch with Photo from their wallet).
4. The Vouchee entered PII is cross matched to the PII from the Digital Vouch with Photo.
5. The IdSP service captures a photo of the Vouchee. This photo taking process includes a liveness check to GPG45 standards.
6. The photo taken by the ID Provider is matched to the photo contained in the Digital Vouch with Photo using GPG45 standards. (Note that two pictures taken by a camera are being matched here, not a photo from an ID document and a selfie. Standards to photo taking need to be considered).
7. If the photo matches, the Digital Vouch with Photo is accepted for GPG45 evidence, validation, activity and verification purposes. (see later section for scoring).
8. The Digital Vouch with Photo is then used by the ID Provider to issue the Vouchee a Digital ID.

Consideration should be given to whether there is a temporal aspect to step 2 as part of risk mitigation. Step 1 needs to be completed when the Vouchee and Voucher are together. Should the Step 2 be completed while they are still together? This puts additional burden on the Vouchers time.

5.3 Alternative Flow 1

A pre-cursor to Step 1 could be that the Vouchee initiates the process with the “Digital Vouch with Photo service” and indicates who their Voucher will be via entering / scanning / presenting a unique code for that voucher.

The Voucher would then receive a request from the “Digital Vouch with Photo service” to create the Digital Vouch with Photo.

This pre-cursor process would help track (and charge the user for) the vouch.

5.4 Alternative Flow 2

Another alternative flow could be:

1. Vouchee creates a Digital ID with an Identity provider of their choice. The Digital ID contains self-declared Name, DOB, Address, Email, Phone Number and takes a Selfie.
2. Vouchee creates QR Code of their claimed PII and presents it to the Voucher.
3. Voucher scans QR Code in a Digital Vouch with Photo Service.
4. Digital Vouch with Photo Service receives all the Vouchee’s PII and Selfie.
5. Voucher takes a Photo of the Vouchee with the Digital Vouch with Photo Service. Must be face to face.
6. Voucher confirms the Vouchees PII is correct agrees to declaration requirements.
7. Selfie from the user’s Digital ID and Photo taken by Voucher are matched by the Digital Vouch with Photo Service.
8. Digital Vouch with Photo is created and delivered to the Vouchee by the Digital Vouch with Photo Service.
9. The Vouchee pastes the link / code for their digital vouch into the ID Providers evidence collection process.

6 Scoring of the Digital Vouch with Photo in an Assurance Policy

Each Trust Framework will need to determine what a Digital Vouch with Photo scores within its Assurance Policy.

As a key goal of the vouching process is inclusion, the Digital Vouch with Photo should score sufficiently highly to allow the user to be issued with a meaningfully useful Digital ID.

In the UK Trust Framework, it is proposed that the Digital Vouch with Photo could score the following under the GPG45 Assurance Policy:

GPG45 Element	Score	Rationale
Strength	4	<p>The evidence came from the Voucher, who has a GPG45 High Digital ID, which is equivalent to an eIDAS High Digital ID listed as Strength score 3 in the creation of the Digital Vouch with Photo the following was also done to elevate the score to 4:</p> <ul style="list-style-type: none"> includes biometric information (the photo) all digital information (including biometric information) is protected by cryptographic security features the cryptographic security features can prove which organisation issued the evidence (the Voucher and the Digital Vouch with Photo Vouching Service) whoever issued the evidence – then (the Digital Vouch with Photo Vouching Service) proved the claimed identity by (having the Voucher) comparing and matching the person to an image of the claimed identity from an authoritative source (the photo captured by the Digital Vouch with Photo Vouching Service)
Validation	3	“evidence protected by cryptographic security features will have a score of 3”. The IdP can confirm “these security features are genuine” with the Digital Vouch with Photo Vouching Service
Activity	0-3	<p>Assume row 1 of the table in GPG45 applies as the Voucher themselves has not done a separate “Identity Check” on the Vouchee.</p> <p>So based on how long the Voucher has known the individual:</p> <p>Less than year – Score 0</p> <p>1-2 years – Score 1</p> <p>2-3 years – Score 2</p> <p>3+ years - Score 4</p>
Identity Risk	-	The Vouch does not provide any form of Identity risk assessment.
Verification	4	Assuming the biometric matching of the photo in the Vouch to the photo taken by the Vouchee of themselves using the IdPs service meets the GPG45 standard to score 4.

With no addition of Identity Risk checks, the profile achieved would be **M1C**.

With the addition of Identity Risk checks by the IdP, the profile achieved would be **H1A**.

7 Reflections on this proposal

The proposal suggests a Digital Vouch with Photo equivalent to a Passport. On the face of it this digital vouching process has more robust features than passport issue: it is digital and has the liveness check on the photo for instance. So, this makes sense. However, there is no separate agency assessing the vouch for risk as there is with the passport application process (e.g. a passport issuing agency). So, this positioning may be over optimistic.

In the UK specifically, if this equivalence to passports is accepted, a Voucher with a GPG45 LoC High ID can vouch for a Vouchee who then gets a GPG45 LoC High ID as a result, with limited Identity Fraud checks applied. One bad actor could rapidly cause a proliferation of invalid High LoC IDs.

There is a lot of risk management that goes on behind the scenes when a passport is created, so this equivalence feels like somewhat of a stretch.

To mitigate these risks Velocity and other mandatory fraud checks, such as Voucher and Vouchee address proximity checks, could be implemented by the Digital Vouch with Photo service Provider to look for Vouchers doing more Vouches than normal. Normal being only very occasionally.

8 Implementation Considerations

OIX has created the below list of considerations aimed at those creating a Digital Vouch with Photo process:

1. How would someone become a Voucher? Is self-declaration as a member of a profession sufficient? Should a cross check with a professional body, digital or manual, be required?
2. Why would someone become a Voucher? For passports, people do this today as they are approached by people who know them to declare that fact as part of the passport application process. The processes for a Digital Vouch is arguably more complicated. Rather than ticking a few boxes in a form and signing the back of a couple of photos, the Voucher must use their Digital ID, or an associated app, to go through the vouching process. How can a trust framework encourage authority figures to become Vouchers? Payment would be a perverse incentive, so should not be considered. The framework should play on the Voucher's social responsibility as an authority figure.
3. To discourage false vouching, the trust framework should ensure participating trusted professions have the mechanisms in place to sanction bad actors and remove them from that profession.
4. The legal position of vouching in the target implementation territory needs to be considered. In the UK for example there is some protection when using vouching for some existing public sector use cases, e.g.:
 - Passports – offence of knowingly providing untrue statements (Criminal Justice Act 1925) (*protecting against a false vouch*)
 - Visa applications – deliberate or recklessly making false statements (British Nationality Act 1981) (*protecting against a false vouch*)
 - (*Repealed*) Identity register – offence of providing or confirming false information (Identity Cards Act 2006) (*protecting against a false vouch – digital focus*)

Other public sector use cases, and private sector use cases, have some protection, albeit less direct, against a false vouch:

- Possessing false *identity docs (passport etc) or production apparatus* (Identity Doc. Act 2010)
- Fraud by false representation (Fraud Act 2006) (*intent and action*)
- Making/using false instrument (Forgery & Counter. Act 1981) (*intent and action*)
- Breach of contract (civil matter) & misrepresentation / misstatement (tort)

The dishonest creation of a false Digital Identity by the voucher knowingly providing false information would likely represent the criminal offence of 'fraud by false representation' under laws that apply in England, Wales and Northern Ireland – or similar fraud or dishonesty offences in other regions (such as common law fraud in Scotland).

5. Is there a use case for Activity Only vouches? Users may have evidence to prove who they are but no electronic record of activity. In which case the vouch would only cover the Vouchers attestation of how long they have known the individual.
6. Some party will need to pay the "Digital Vouch with Photo vouching service" for the creation of the Digital Vouch with Photo. This party could be:
 - The Vouchee themselves, in the same way they pay for passport applications and PASS cards today
 - The Relying Party, in order to do business with the Vouchee.
 - The IdSP, who may also be the "Digital Vouch with Photo vouching service", so as to monetize the ID elsewhere.
 - Government, to support inclusion in the Digital ID ecosystem. Government would need to beware of Vouchees who have ID documents such as passports and driving license unnecessarily using this service.