Digital ID checklist:

Eight questions to ask before you choose your digital ID verification provider

thirdfort

thirdfort

1. Will your clients find it easy to use?

User experience is one of the key benefits of digital identity verification.

You should confirm that the solution you're considering:

- ✓ Has clear instructions and is easy to use. There should be no technical jargon and each step should be obvious even to novice users.

- ✓ Offers a high level of support to those users who do run into problems. For example, at a minimum, support should be offered through the phone, live chat and email.

- ✓ Covers the countries where you operate. Most digital providers will have solutions for most passports around the world.

- ✓ Can be used by a smartphone anywhere, as long as the phone is connected to the internet.

The provider should be able to explain to you how it has ensured that the solution is accessible to novice and less digitally-savvy users. It should also be able to give you statistics such as the percentage of verifications that are successful over a period of time (called the 'completion rate').

thirdfort

2. How will you get the efficiency benefits of digital identity verification?

This technology should be a time saver, not a time suck. It's important to understand how a provider will support your business and your clients if they have technical issues or questions.

The provider you're considering should:

✓ Provide a well-designed, clean and well-signposted verification process for your clients so that incomplete or failed attempts are minimised.

✓ Good-quality providers will have a dedicated support team to help your clients so that it won't be your team on the hook to answer client's questions about how to use the app.

✓ Report results to your staff in the format best suited to your business. You should be able to download results as spreadsheets or in PDF format at minimum.

You could ask the provider you're considering if they have any data around the average time saved per ID check. This will allow you to calculate a rough estimate of how much you'll save versus the cost of implementation.

By implementing Thirdfort in their businesses, our customers cut the average time spent onboarding a client by 80%, with a reduction of the average number of days to onboard going from 5 to 1.

thirdfort

3. Will your firm achieve 'safe harbour' from a recourse claim by HM Land Registry in the event of fraud?

It's important that the solution you are considering achieves HM Land Registry's Digital ID Standard.

The provider you're considering should:

- ✓ Understand the requirements of the Digital ID Standard, and why they are important to your firm

- ✓ Be able to read the NFC chip data from biometric forms of ID such as passports, and EU ID cards.
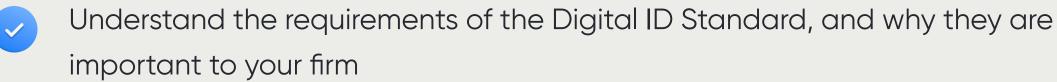
Thirdfort worked closely with HM Land Registry in their development of the Digital ID Standard. Whilst other providers are able to read NFC chips, we believe we are the only one to read them to the standard HMRC requires.

Thirdfort reads the digital signature and signing key of the document, which is what confirms the document as being government-issued. By comparison, other providers have NFC technology, but it will only confirm that the passport has a chip, not that it's government-issued.

thirdfort

4. Check the provider's compliance with data regulations such as GDPR

Privacy and the safeguarding of confidential personal data should be a primary focus for all digital ID verification solutions. It's important to ensure that any solution you use has carefully aligned its technology and processes with legal data requirements.

You should confirm with a prospective provider:

- ✓ How they handle your clients' data generally and also internally, and with its own suppliers.

- ✓ If they function as the data controller or the data processor – and which data points it controls or processes.

- ✓ How long the provider and any of its suppliers retain your and your clients' data.

- ✓ How a user can make a SAR and request for their data profile to be deleted in adherence with the right to be forgotten.

- ✓ Whether the provider has a privacy policy that is in plain English and accessible to all users.

f thirdfort

5. How will your ID solution integrate with your Case Management System?

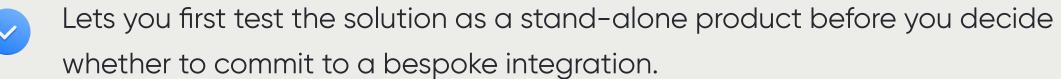Some digital identity verification providers offer 'out-of-the-box' integration solutions, while others are able to support bespoke integrations tailored to you and your firm. While using a bespoke solution can have its benefits, it is often quicker and easier to set up and get started with an 'out of the box' solution.

Check that the provider:

- ✓ Has explained the different implementation options available.

- ✓ Provides a complete list of 'out of the box' CMS integrations they already support (if they support any).

- ✓ Lets you first test the solution as a stand-alone product before you decide whether to commit to a bespoke integration.

thirdfort

6. What security is in place?

It's important to understand how the provider will increase your level of protection from cyber attacks.

Questions to ask:

✓ Does the provider have cybersecurity accreditations?

✓ Are you satisfied that any external security experts that the provider contracts with have a track record in the security sector?

SECTION A: THE VALUE TO YOUR FIRM

SECTION B: THE VALUE TO YOUR FIRM

SECTION C: ABOUT FUNDING AND THE CONTRACT

thirdfort

7. Decide on the best funding and contractual options for your firm

Some of the funding will be upfront cost and may be considered to be capital expenditure. There will be a portion that will be operating expenditure. Make sure that the solution that you choose matches how you want to fund your digital identity verification system.

You should ensure that the provider gives you options:

- ✓ If you do few checks a month, a Pay-As-You-Go option will suit you best.

- ✓ If you are confident of doing a higher number of checks a month, you should be offered a monthly contract with volume discount and the ability for your unused allowance to rollover.

- ✓ If there is a lock-in period, it should be kept to a maximum of 12 months (if over a year, lock-in periods might pose additional risks for your firm as your needs might change over time).

thirdfort

8. Understand any 'extras' to your contractual fee

Some providers will charge supplementary costs that sit in addition to the initial per check fee that you are quoted. Hidden costs can dramatically increase the amount you need to pay, even if the stated cost per check seems low. This is a common marketing tactic to be aware of and understand before deciding on a supplier.

Ask the provider if they charge extra for:

✓ Incomplete, failed and repeat ID checks (the provider should charge only for completed checks).

✓ Dedicated support for clients.

✓ Additional users within your organisation .

✓ Any other functionality that you might use regularly.

Make sure that you weigh up these extras for the present year as well as your future situation. For example, in the future, you might need more staff members to access the solution.

thirdfort

Thirdfort is an app-based solution that lets conveyancers verify client ID and source of funds in minutes. Combining ID scanning technology to check a client's identity with open banking to prove money is from a legitimate source, Thirdfort is being used by award-winning conveyancers around the UK.

Let's chat

contact@thirdfort.com

www.thirdfort.com