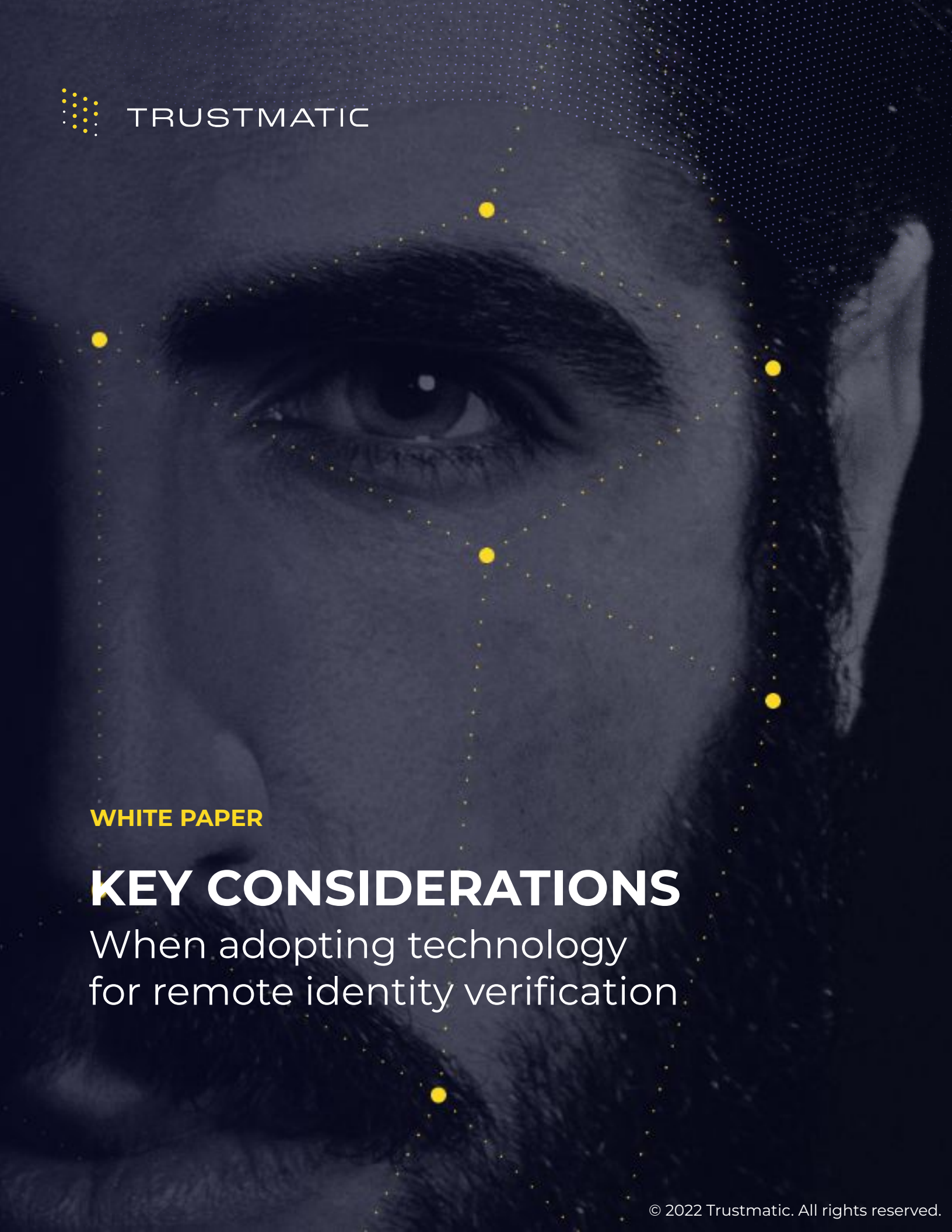


TRUSTMATIC

WHITE PAPER

KEY CONSIDERATIONS

When adopting technology for remote identity verification

TRUSTMATIC

CONTENTS

EXECUTIVE SUMMARY

This white paper sets out the key topics any organization should consider when adopting automated technology for remote customer identity verification.

Prior to the COVID-19 global pandemic, adoption of remote identity verification technology was “slow and steady”, with the majority of deployments happening in the financial services sector.

In light of restrictions on the movement of people brought about by the response to the pandemic, organizations of all sizes have been forced to rethink the way they interact with their customers and users, in particular needing to re-evaluate how they establish trust with their customers during the initial onboarding process.

The remote identity verification industry, previously dominated by a small number of established players, has recently experienced unprecedented growth. There are now hundreds of vendors offering seemingly similar solutions, and organizations who wish to adopt this technology could be forgiven for thinking that it is simply a commodity and, therefore, that they should work with the vendor offering the most favourable commercial terms.

In this paper, we will deep-dive into the technical idiosyncrasies of these solutions and conclude with key recommendations on vendor selection. The aim of this paper is not to convince readers that Trustmatic offers the best solution on the market, rather to ensure they carry out the necessary due diligence when drawing up a shortlist of potential vendors.

WHY REMOTE IDENTITY VERIFICATION?

Until recently, organizations with operational or regulatory requirements to reliably verify the identity of their customers relied on manual processes. For example, the process of opening a bank account or obtaining a SIM card usually involved going to a bank or network operator branch, completing the necessary paperwork, and asking a customer to hand over their identity document.

In many cases, the identity document was then scanned and stored electronically and the in-branch employee visually confirmed that the person in front of them was indeed the true holder of the identity document.

This process took between 20 and 40 minutes and one major European retail bank reported the cost of this and associated administration to be €147 per new customer acquired.

Remote identity verification technology enables customers to open accounts with service providers from the comfort of their own homes. The technology is now at a stage of maturity where error rate are extremely low, especially when compared to human error rates associated with traditional identity verification methods. Additionally, the amount of time required to onboard new customers can be decreased from 20 minutes to ***under 60 seconds***, with the cost falling from over €100 to under €2.

Convenience, security, and cost-effectiveness are all increased by adopting remote identity verification technology, however it is critical that organizations carry out in-depth assessments of the solutions they intend to adopt, as their exposure to regulatory penalties and identity fraud can increase if their chosen vendor's technology contains weaknesses and/or is not integrated properly.

ACQUIRING PERSONAL IDENTIFIABLE INFORMATION (PII)

Personal Identifiable Information (PII) is information that, when used alone or with other relevant data, can identify an individual. PII may contain direct identifiers (e.g., passport information) that can identify a person uniquely, or quasi-identifiers (e.g., race) that can be combined with other quasi-identifiers (e.g., date of birth) to successfully recognize an individual.

In the context of remote identity verification, PII usually refers to (but is not limited to):

- Identity document images and data contained therein
- Identity document data read from Machine Readable Travel Documents (MRTDs) containing RFID chips
- Face “selfie” images
- Proof of address documents
- Phone numbers, residential addresses, and email addresses
- IP addresses

This data can be captured either via a web interface or via smartphone mobile apps. It is critical that this data, once captured, is stored in accordance with GDPR or other relevant data protection legislation. One of the key challenges in remotely capturing PII is in ensuring the data is legitimate and is not part of an attempt at identity theft or other fraudulent activity.

KEY CONSIDERATIONS

1. No data should be allowed to be captured using “manual upload” methods. For example, when asking a customer to submit their identity document image or selfie, this should be facilitated via live capture from the device camera, not via uploading a saved file from their device.

2. Remote identity verification solutions should offer web and mobile SDKs to allow organizations to integrate “controlled capture” components into their web or mobile applications.

3. Controlled capture components should feature document and face auto-capture, as opposed to allowing users to manually capture images. These components should contain neural-network based detectors, which at least ensure that a physical identity document is being captured and that the selfie is being taken by a live person, not of a picture of a person (one of the most common forms of presentation attacks).

4. Data processing such as optical character recognition (OCR), face verification, or liveness checks may be carried out on the user’s device, but this must be repeated on the server-side, where more complex algorithms can carry out checks with increased accuracy.

5. Where possible, the NFC function of smartphones should be used to read and authenticate data contained in the RFID chip of MRTDs.

IDENTITY DOCUMENT PROCESSING & AUTHENTICITY CHECKS

Once a high-quality image of the identity document has been captured, this should be sent securely to a server for processing. As a minimum, the following checks should be carried out:

KEY CONSIDERATIONS

1. Automated document type and version classification - users should not need to manually pre-select their document type from a list.

2. Optical Character Recognition (OCR) of the textual data fields, with associated per-field confidence scoring.

3. Extraction of the facial portrait image from the identity document with age estimation and comparison against the date of birth on the document data page.

4. If applicable, data cross check between the data contained on the document data page and the data contained in the Machine Readable Zone (MRZ).

5. Data validity checks to ensure the ID is not expired.

6. Image analysis to ensure the image is of a physically present document, not a photocopy or an image captured from a computer screen.

7. Tampering detection to ensure the textual data or face portrait have not been tampered with or overlaid.

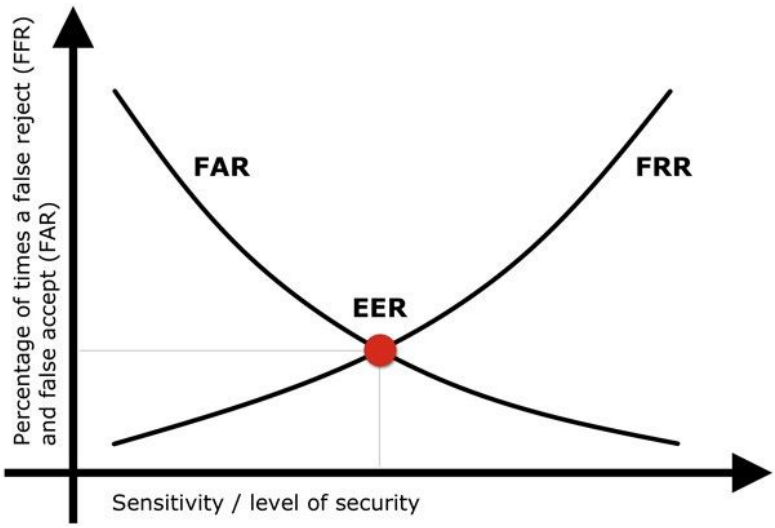
8. Comparison of the visual data with the data extracted from the RFID chip via NFC.

BIOMETRIC VERIFICATION

When the face portrait image has been extracted from the identity document via visual extraction, NFC, or both, it should be compared to the selfie image and assessed for similarity.

Biometrics is an inherently probabilistic process and it's accuracy is expressed in terms of False Accept Rate (FAR) and False Reject Rate (FRR). In simple terms, FAR indicates the percentage probability a pair of non-matching faces will be incorrectly indicated as matching. FRR indicates the percentage probability a pair of matching faces will be incorrectly indicated as matching.

As the number of false acceptances (FAR) goes down, the number of false rejections (FRR) will go up and vice versa (see the figure below). The point at which the lines intersect also has a name: the Equal Error Rate (EER). This is where the percentage of false acceptances and false rejections is the same.



KEY CONSIDERATIONS

1. How does this affect the security level and user convenience?

If you try to reduce the FAR to the lowest possible level, the FRR is likely to rise sharply. In other words, the more secure your system, the less convenient it will be, as users are falsely rejected by the system. The same also applies the other way round. Do you want to increase user convenience by reducing the FRR? In this case the system is likely to be less secure (higher FAR).

2. How do I know the true accuracy of the biometric algorithm in my system?

Very few identity verification technology vendors develop their own proprietary biometric algorithms. This, in and of itself, is not a major problem. However, your vendor should be open with you about which algorithm is inside their solution.

The National Institute of Standards and Technology (NIST), carries out an ongoing benchmark of facial biometric algorithms, called Facial Recognition Vendor Test (FRVT). FRVT is divided into a number of categories, and the most relevant for remote identity verification use cases is NIST FRVT 1:1.

We recommend only choosing a solution with an algorithm that is ranked in the top 100 in all categories of NIST FRVT 1:1.

FACE PRESENTATION ATTACK DETECTION

Face Presentation Attack Detection (PAD) is an algorithm's ability to determine that it is interfacing with a physically present human being and not an inanimate spoof artifact or injected video/data. Some common types of spoof artefacts are shown below:

A: Hi-res paper & digital photos, hi-def challenge/response videos and paper masks.

B: Commercially available lifelike dolls, and human-worn resin, latex & silicone 3D masks under $300 in price.

C: Custom-made ultra-realistic 3D masks, wax heads, etc., up to $3,000 in creation cost.

ISO/IEC 30107-3:2017 establishes:

- principles and methods for performance assessment of presentation attack detection mechanisms;
- reporting of testing results from evaluations of presentation attack detection mechanisms;
- a classification of known attack types (in an informative annex).

As with facial biometrics, most remote identity verification solutions integrate PAD algorithms from third parties.

KEY CONSIDERATIONS

1. Has my PAD algorithm been tested in accordance with ISO/IEC 30107-3?

The most commonly used NIST NVLAP certified testing lab for PAD evaluations is iBeta. iBeta tests in accordance with the ISO/IEC 30107-3 standard and in alignment with the ISO/IEC 30107-1 framework.

The testing levels and performance requirements are identified as:

Level	Time	Expertise	Artefact source	Limit
1	8 hours per subject or species	None	Cooperative subject and equipment is readily available in a normal home or office environment	0% penetration or match rate allowed
2	2-4 days per subject or species	Moderate – participated in at least 1 other PAD test with the target modality and has an understanding of the liveness detection functionality of the test target	Cooperative subject and equipment is more expensive (such as a 3D printer, resin mask, latex mask)	1% penetration or match rate allowed

2. How well does the PAD algorithm perform in relation to my use case?

While iBeta Level 2 accreditation is the highest level of PAD evaluation in widespread use today, simply passing the evaluation is not a guarantee of security in real-world use cases (in fact, there are no guarantees when it comes to biometrics in general).

Almost all of the algorithms listed on the iBeta Level 2 confirmation letters page have inherent weaknesses and can be spoofed with varying degrees of difficulty. For reference, the vendors with Level 1 and Level 2 accreditation are:

• Idemia • Innovatrics • Unissey • VU Security • OZ Forensics • NEC • Imageware • EyeVerify	• Zoloz • HID Global • ID Mission • iProov • ID R&D • Aware • OCR Labs • FaceTec

It is strongly recommended to only choose a vendor which uses a PAD algorithm from the above list. In the interest of transparency, Trustmatic is a strategic partner of Innovatrics and uses its PAD algorithm as its primary PAD solution.

Once a vendor has been shortlisted, you should test their algorithm via a demo app or API, either via internal testing or with an external biometrics testing lab. If you identify any weaknesses, a good vendor should be able to suggest a remedy and deliver a retrained algorithm for further testing.

MANUAL ADJUDICATION OF EDGE CASES

Most remote identity verification solutions will assign an overall trust level (or similar) to every onboarding session. It is not feasible that 100% of onboarding sessions will be automatically accepted or rejected based on the available data.

The best solutions are the ones that reduce the amount of edge cases to the lowest possible percentage of overall session, without compromising on security or user experience.

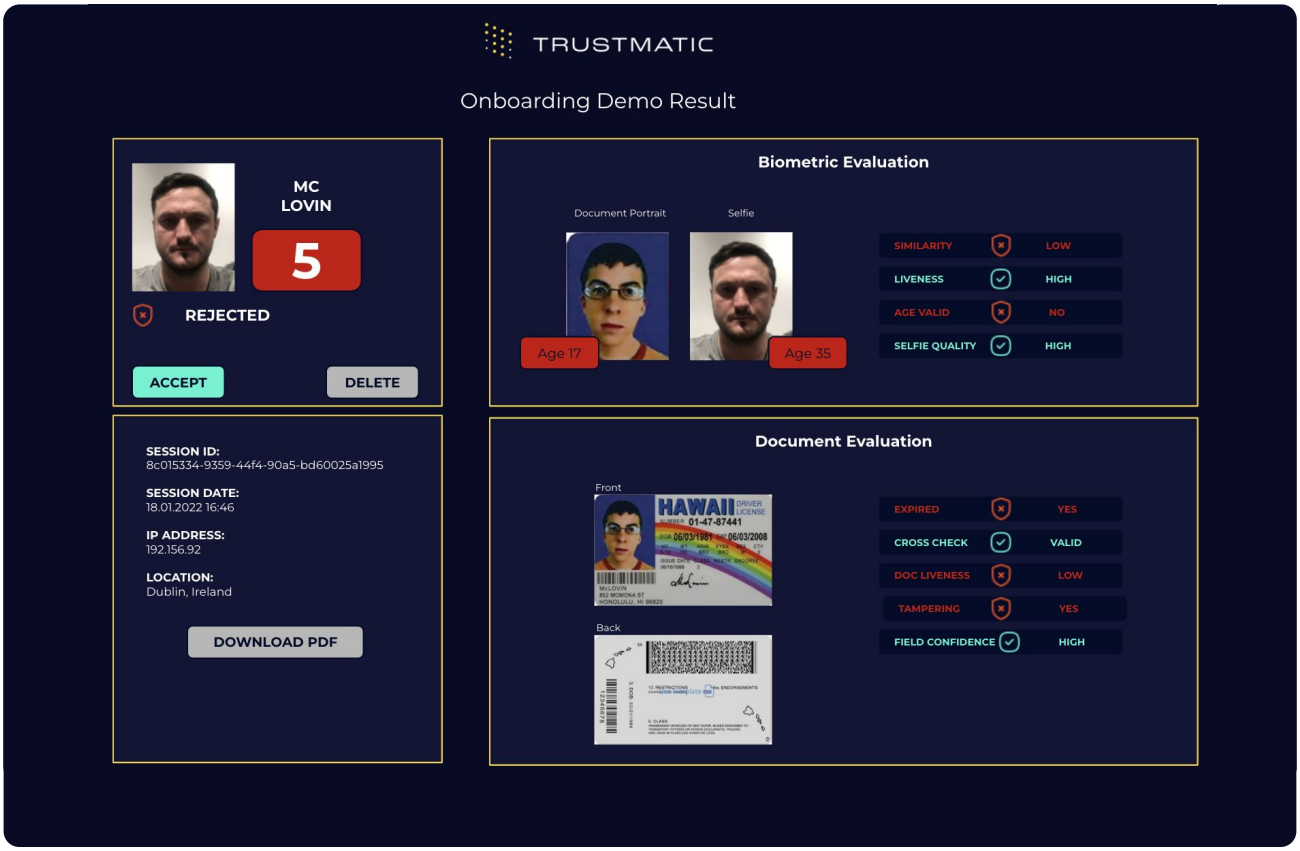
Edge cases are the sessions which fall in between the two confidence thresholds, set for auto reject (lower threshold) and auto accept (higher threshold). From our experience, 5-10% of onboardings end up as edge cases. Examples of edge cases include:

- Document quality is compromised and all data could not be read accurately
- Age validation is inconclusive
- User is onboarding from a location far away from their place of residence
- Document portrait image vs selfie match is inconclusive
- Liveness score is inconclusive

These cases should be referred to a fraud analyst or customer service representative for manual adjudication. The solution should include a user-friendly adjudication functionality, where fraud analysts can easily inspect the onboarding data visually and, where necessary, initiate a video call with the customer to double check their data.

The next page contains an example of Trustmatic's manual adjudication dashboard.

TRUSTMATIC MANUAL ADJUDICATION DASHBOARD



RECOMMENDATIONS ON VENDOR SELECTION

Below is a checklist which organizations can use as a guide when drafting a shortlist of potential vendors:

- ☐ Identity document auto-capture component (web & mobile)
- ☐ Selfie auto-capture component (web & mobile)
- ☐ Mobile NFC reader component
- ☐ OCR accuracy of above 95%
- ☐ Good set of document authenticity check features
- ☐ Facial biometric algorithm ranked in top 100 of NIST FRVT 1:1
- ☐ Facial biometric algorithm also submitted to NIST FRVT 1:N
- ☐ PAD algorithm with iBeta Level 1 & 2 accreditation
- ☐ Manual adjudication dashboard with user-friendly interface
- ☐ SaaS and on-premise delivery model
- ☐ Solution can be customized according to project requirements
- ☐ Good support level

Once the above criteria are met, the next step should be to test the top 2-3 vendors in relation to your use case. After that, the best performing solution with a favourable commercial model should be selected.

Trustmatic, as well as offering its own proprietary remote identity verification solution, offers consulting services to organizations considering adopting such solutions. We realise our solution may not suit all use cases, and we would be happy to work with you to ensure you choose the best solution for your organization.

Our experts have decades of experience in identity management and know the potential pitfalls which your organization should avoid. Reach out to us for a free initial consultation by emailing: info@trustmatic.io

Donal Greene, CEO at Trustmatic