Mitek

WHITE PAPER:
MOBILE VERIFY

Comprehensive, AI-powered identity verification that brings real identities into our digital world

Artificial intelligence (AI) for maximum efficiency

Mitek's technology unleashes a combination of sophisticated AI analytics (computer vision, machine learning and deep learning) to swarm over photos of IDs and end user's face selfies, collecting massive amounts of evidence for identity verification. A higher level of machine learning weighs the results from hundreds of these algorithms, making an intelligent decision about the relative importance of each piece of evidence, then predicts whether or not the ID is genuine and belongs to the end user. This process is fully automated, extremely accurate, and takes only a few seconds to run.

While the number of products consumers can apply for online is growing, accounts that can be opened through a 100% digital experience are still the minority — and those that can be opened via mobile devices are even fewer.

Verifying that online and mobile applicants are who they say they are is one of the main challenges preventing businesses from reaching their digital transformation goals. And with all the data breaches across a multitude of industries, it's not getting any easier.

While safeguards around personally identifiable information (PII) must continue to improve, we can no longer assume that "private" means "secret". This is the fundamental flaw with traditional knowledge-based authentication (KBA), a method for identity verification that has become ineffective at best and potentially dangerous at worst.

One of the strongest methods for verifying real-world identities is to digitally authenticate government-issued IDs – bringing the element most predominantly used for proving one's identity in the physical world into the digital world. Once the ID is authenticated, the portrait from the ID is compared against a selfie taken by the end user.

This approach uses ubiquitous mobile phones to combine two factors of security: 1) “what you have” (something only the end user possesses) and 2) “who you are” (biometrics of the end user). This process balances the need for accurate identity verification with the convenient customer experience essential for successful digital businesses today. It returns quick, definitive answers, enabling enterprises to convert more digital customers, faster.

Today’s needs for modern identity verification can be met only through a combination of cloud-based services, end-to-end process automation and artificial intelligence. Mitek employs all of these elements in a proven solution that delivers frequent performance improvements driven by a continuous feedback loop. Both AI algorithms and human experts learn constantly from the huge quantities of ID documents being analyzed — building ever-higher levels of predictive power.

Great customer experience starts with onboarding

Identity verification at account onboarding plays a dual role: While helping to keep identity forgers out, it’s also one of the first steps for bringing legitimate customers in. This initial experience matters. It’s an opportunity to create great first impressions and start building strong and loyal relationships with consumers.

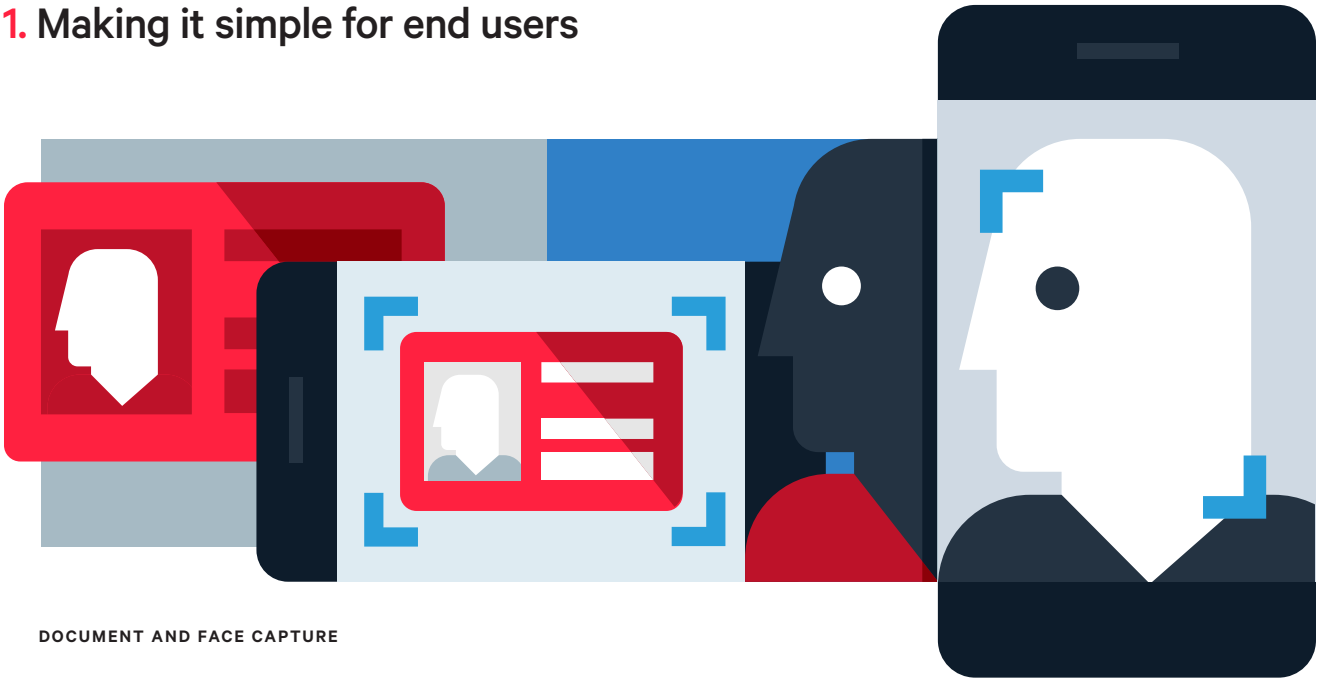
“By 2023, 85% of organizations will be using document-centric identity proofing as part of their onboarding workflows, which is an increase from approximately 30% today.”

BUYER’S GUIDE FOR IDENTITY PROOFING
Gartner, April 2021

Multi-layered artificial intelligence provides dependable identity verification

HERE IS AN OVERVIEW OF HOW MOBILE VERIFY WORKS:

1. Making it simple for end users



DOCUMENT AND FACE CAPTURE

It all starts with the quality of the image submitted. Mitek MiSnap™ auto-capture software evaluates lighting, focus, glare, document alignment, and other factors, interactively guiding users through commands as they hover their smartphone over their ID document.

This real-time guidance is made possible by video frame analysis running in the background, which also allows for an auto-capture of the best possible image from the video stream. As a result, end users are able to take an ideal photo of their ID document as well their selfie, which is literally captured in the blink of an eye.

MiSnap's image analytics and guided experience result in a substantial uplift in images that are acceptable ("passing") for authentication purposes compared to manually captured images. The first snap is usually successful, which encourages widespread, rapid user adoption.

The MiSnap SDK is fully brandable and can easily be embedded into an application. It provides omnichannel support, including native apps, mobile and desktop web apps, and employee-assisted service. To protect user PII, ID images and data are never stored on a mobile device.

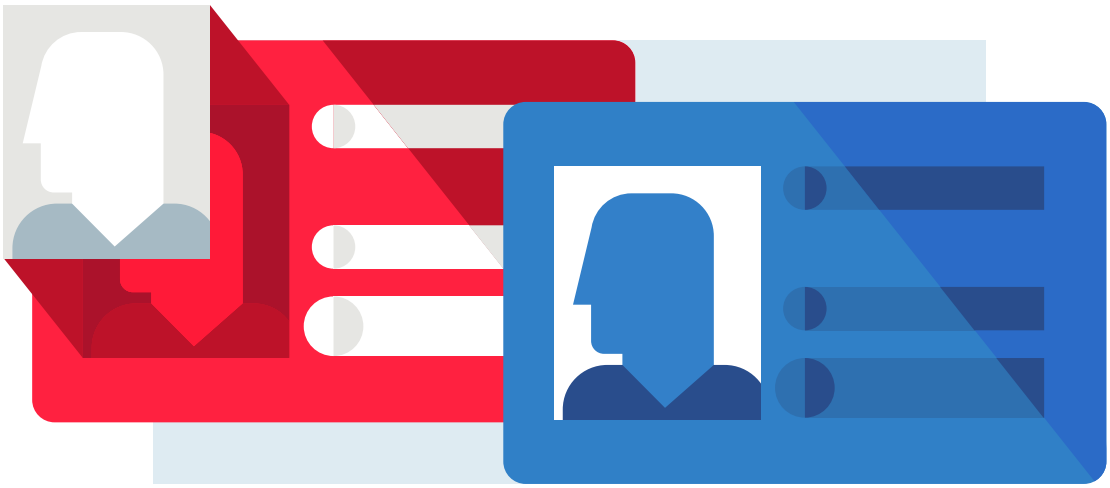
2. Classifying ID documents

MITEK REPOSITORY OF LEGITIMATE ID TEMPLATES

Once the image has been captured and submitted, Mobile Verify uses computer vision algorithms to match the image of the ID document to one of the thousands of formats of government-issued IDs from around the globe that Mitek maintains in a cloud-based repository. Mitek constantly refreshes this repository with new template releases.

In case of a non-match, a separate investigation process is triggered. Through a series of automated and human expert steps, Mitek can determine if the image is a new format from a government issuer. These new formats are then queued into development for automated classification.

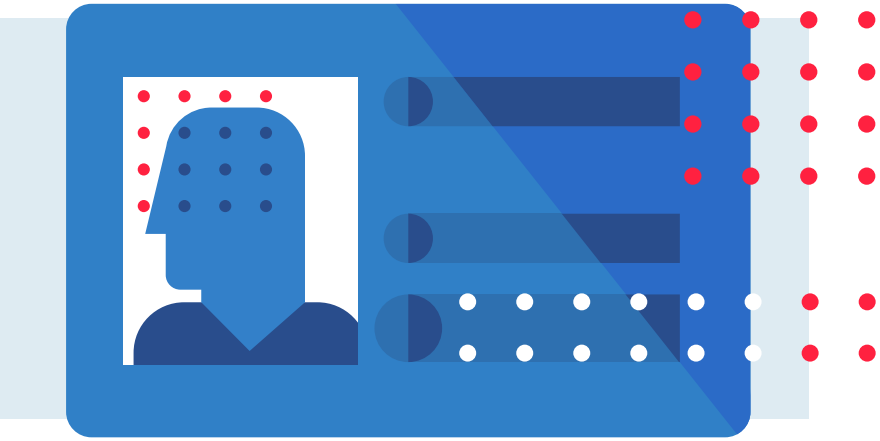
3. Extracting data and initial checks



COMPARING ID STRUCTURE AGAINST THE CORRESPONDING DOCUMENT TEMPLATE

Through a combination of computer vision techniques, optical character recognition (OCR) and rules, Mobile Verify compares the structure of the ID image against the corresponding document template. Are components like biographical information, signature block, portrait area, machine readable zone (MRZ) and barcode exactly where they should be? Extracting information from these elements, the software then checks to make sure the ID data is internally consistent. For example, does the data encoded into the MRZ and barcode match up with the biographical information?

4. Gathering evidence



To further determine if the ID document is original and unaltered, the software unleashes hundreds of AI-based analytics on the image and extracted data, each one examining the ID in a different way to find anything suspicious. Analysis includes:

Computer vision (CV) algorithms evaluate details like the overall structure of the ID document, photocopy indicators or elements pointing to digital alterations (such as a portrait being digitally generated). They also examine the image quality (very low and very high can both be red flags).

These algorithms are constantly evolving based on the hundreds of thousands of ID documents that Mitek processes every year for customers around the globe.

> **Verification power**
>
> CV techniques are able to process groups of pixels and understand what they represent — for example, evaluating the structural integrity of specific ID document layouts, or determining if there is an unexpected shadow or if the photograph corresponds to the face of a human.

Machine learning (ML) algorithms that scrutinize the ID for a wide range of characteristics, such as font usage and consistency.

Utilizing Mitek's repository, the algorithms are trained to spot an enormous set of identified characteristics of both forged and legitimate ID documents.

Going beyond individual ML forensic checks, the use of ensemble ML techniques is equivalent to simultaneously running hundreds of forensic check permutations.

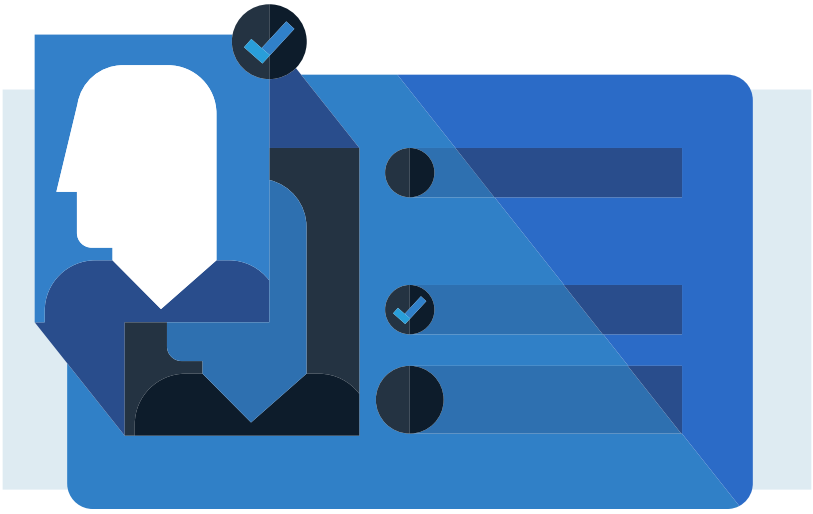
> **Verification power**
>
> ML techniques learn which characteristics and patterns of characteristics (both usually referred to as "features" in analytic modeling) are indicative of forgery or counterfeiting. They work with nonlinear data relationships at levels of complexity and speed far beyond natural human capacity.
>
> Using ensemble ML techniques, Mitek is able to exploit the power of the learned data, and perform what would be the equivalent of hundreds of forensic check permutations on each ID document.

Deep learning algorithms (DL) that can find subtle problems with IDs, such as slight irregularities appearing on or between certain letters.

They are trained to identify problematic features on their own by analyzing massive quantities of IDs labeled as "genuine" or "forged/counterfeited."

> **Verification power**
>
> DL techniques uncover indicators of forgery/counterfeiting that may not be discernible by human experts and thus are unlikely to be codified as rules or pre-identified features.
>
> An additional advantage is that deep learners become more accurate as they analyze more IDs. Unlike conventional predictive models, they cannot be fed too much data.

5. Weighing the evidence

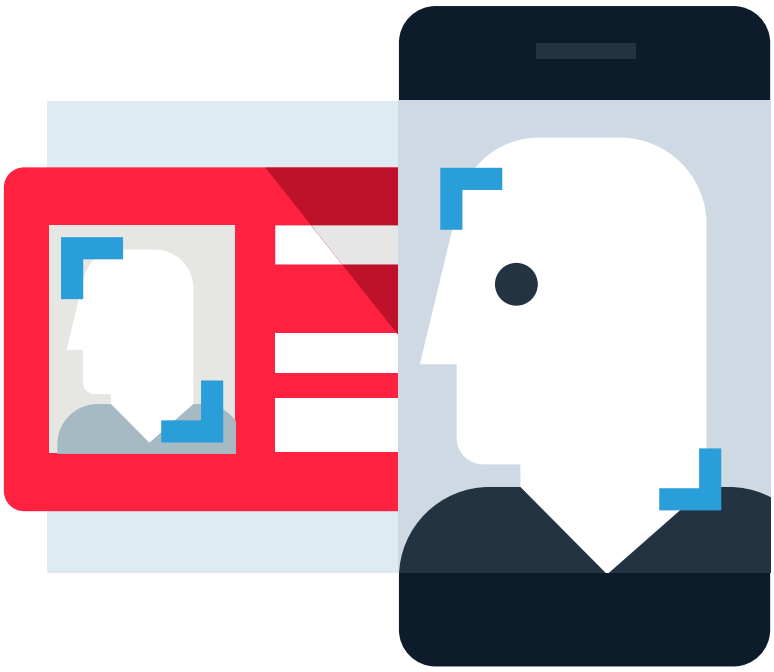


Each of the hundreds of evidence-gathering algorithms output a fractional score between 0 and 1 (with zero representing highest risk and 1 representing lowest risk) — most scores falling in "gray zones" between the two. This range of values is more accurate and nuanced than a simple binary result would be, but it creates an immense challenge: How do you combine all of these gradations of score values into a single definitive answer?

If one approached this challenge using techniques based on rules for determining minimum values or allowable ranges, the result would be a loss of accuracy and nuance. Therefore a more intelligent analytic approach is needed.

Mobile Verify uses an additional level of machine learning to examine all of the outputs from the evidence gatherers. This higher-level ML decides how much weight (relative importance) to give each point of evidence based on everything discovered about the ID being examined and everything known about the genuine and counterfeited IDs in the repository. It is an immensely complex task, but Mitek's ML algorithms perform it in near-real time.

6. Matching the face selfie to the picture on the imaged ID



Once the ID document has been authenticated, Mobile Verify uses biometric facial comparison to determine whether or not the face in the ID matches the face in the selfie. The software's ability to quickly and reliably make this match is substantiated by both "passive" and "active" anti-spoofing techniques. First, passive tests operate in the background of the capture experience, helping to ensure that the selfie is from a real person and not the result of video replay or digital reproduction. Then the end user is prompted to take an action, such as blinking or smiling, which is an active technique that ensures a real-life interaction.

Mitek face comparison technology has been tested against millions of images and has proven to be reliable across age, race and gender. By default, Mitek's image "passing" threshold yields an outstanding <1% false positive rate. Additionally, the customer has the ability to set their own "passing" standard according to their needs or requirements.

7. Delivering a clear decision

Mobile Verify will return a definitive “yes” or “no” answer to the question: “Is this identity genuine and does it belong to the applicant?”

For those cases where the customer may want to further evaluate the identity proofing result, they can either request additional information from the applicant, or they can escalate these transactions to Mitek’s identity document experts for a reevaluation process.

Conclusion: modern identity verification for a digital world

Mobile Verify is a better identity verification method for today's digital economies because it doesn't depend on "secret information" remaining secret in our connected world. Instead, Mobile Verify uses ubiquitous mobile devices and an innovative combination of AI to allow the element most predominantly used for proving one's identity in the physical world — government-issued IDs — to be instantly authenticated in the digital world.

And because both the physical and digital worlds never stop changing, Mitek runs its development and production systems in parallel, driving a rapid iteration cycle of continuous adaptation and improvement. While CV, ML and DL algorithms learn from analyzing huge quantities of identity documents, Mitek's data scientists and ID document experts also use the latest iterations of these algorithms to explore trends and ways to increase performance. The process combines machines that quickly crunch through massive amounts of complex data with human experts who can leverage their knowledge to investigate issues and confer with other specialists. **It is this powerful combination of technology and industry expertise that allows Mobile Verify to provide a fully-automated and dependable solution for digital identity verification.**