## What is a Digital Profile Platform?

## Features

### Core Identity

Okta Stuff

### Identity Proofing and Biometric Capability

Gartner’s 2020 Market Guide for Identity Proofing and Affirmation[[1]](#endnote-2) provides an overview of this capability.

1. *Identity Proofing* is the combination of activities during an interaction that brings an identity claim within organizational risk tolerances, such that:
   1. The real-world identity exists
   2. The individual claiming the identity is, in fact, the true owner of that identity and is genuinely present during the process.
2. *Identity Affirmation* is the combination of activities that provide supporting evidence for an identity claim to establish trust in an interaction, such that confidence is increased during the identity-proofing process that fraud isn’t taking place.

The identity assurance achieved with this capability used in isolation is relatively strong, relying on both “something *only* you have” and “something *only* you are”.

### Detecting Fraud

To ensure the individual creating the owner is in fact the true owner, there are a variety of methods that can be used to increase the confidence level to bring the identity claim within risk tolerances required by an organization or entity.

#### Something Only You Have

A form of issued identification, such as a State Id, Driver’s License, or Passport is the most common form of documentation. The Transportation Security Administration (TSA) maintains a list of [acceptable IDs](https://www.tsa.gov/travel/security-screening/identification)[[2]](#endnote-3).

The first step in determining validity usually involves taking a picture of the identification via a smartphone’s camera. A smartphone is preferred due to the camera resolution and additional device checks that can be performed.

Device Verification

Using a smartphone device for enrollment and local storage requires that we ensure the trustworthiness of the device and build a device specific profile.

1. Device Trustworthiness
2. Device Profile
3. Device Fraud

Document Verification

Once captured, optical character recognition (OCR) is used to extract the information from the image. This allows integrity, validity, and verification checks to be performed.

1. *Document Integrity* is the process of determining whether the document being presented has not been tampered with. For examples of the type of integrity controls used see The Electronic Code of Federal Regulations (e-CFR) for Minimum Documentation, Verification, and Card Issuance Requirements[[3]](#endnote-4) as it pertains to Real Id Driver’s Licenses and Identification cards.
2. *Data Validation* is the process of determining whether a particular piece of information falls within the acceptable range of values for a given field.
3. *Data Verification* performs a check of the current data to ensure that it is accurate, consistent, and reflects its intended purpose.

Presentation Attack Defense and Detection

Ease of Enrollment

### Consent

Grant Right to Use

Revoke Right to Use

### Present

Performance

Presentation Attack Detection

### Document Digitalization Capability

Driver’s License

Passport

## Common Features

Privacy

Performance

Security

## Glossary

Machine Readable Travel Documents (ICAO 9303)  
With the worldwide implementation of International Civil Aviation Organization (ICAO) 9303, machine-readable travel documents (MRTDs), such as passports, smart-chip-enabled MRTDs offer a high degree of protection against forgery. Coupled with easily available MRTD solutions using embedded capabilities in smartphones and other consumer devices, this offers high levels of identity assurance for in-person and remote verification and corroboration.  
<https://www.icao.int/publications/pages/publication.aspx?docnum=9303>

1. Gartner’s Market Guide for Identity Proofing and Affirmation. <https://github.com/mikelor/architecture/identity/gartner/G00719390.Market%20Guide%20for%20Identity%20Proofing%20and%20Affirmation.pdf> [↑](#endnote-ref-2)
2. The Transportation Security Administration’s (TSA) list of acceptable IDs.

   <https://www.tsa.gov/travel/security-screening/identification> [↑](#endnote-ref-3)
3. Electronic Code of Federal Regulations (e-CFR) Title 6 - Domestic Security CHAPTER I - DEPARTMENT OF HOMELAND SECURITY, OFFICE OF THE SECRETARY PART 37 - REAL ID DRIVER'S LICENSES AND IDENTIFICATION CARDS Subpart B - Minimum Documentation, Verification, and Card Issuance Requirements.

   <https://www.law.cornell.edu/cfr/text/6/part-37/subpart-B> [↑](#endnote-ref-4)