AU10TIX

IDENTITY INTELLIGENCE

Au10tix Credential (IDV) Policy

Contents

Legal Notice

1. Introduction

1.1. Purpose and Scope

This document describes the AU10TIX Credential (IDV) Policy for enrollment and identity proofing of applicants and end-users. The Credential (IDV) Policy details the **acceptability, validation, and verification** of identity evidence presented by an applicant and end-user to support their claim of identity.

Au10tix takes privacy issues very seriously and invests significant resources and time to protect the privacy of personal data. Au10tix functions mainly as a data processor, and therefore is prepared to work according to the obligations under the General Data Protection Regulation 2016/679 (the "GDPR"), and all currently in effect state consumer privacy and data protection laws of the United States (together: "U.S. Privacy Laws", and collectively with the GDPR: "The Laws") and assist controllers in exercising their own obligations under The Laws.

The Laws require data controllers to engage with Au10tix under contractual agreements that will include: the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the data controller. The Laws also requires a set of legal, technical and operational safeguards and controls that apply to data processor and must be stipulated in the contract, and further requires data processors to assist the data controllers.

This document is intended for AU10TIX's staff, applicants, end-users, and customers who want to receive a high-level description to understand the Credentials (IDV) Policy. Any other description on Au10tix's functions as a data processor can be found in the Master Service Agreement and in the different company policies.

1.2. Overview

AU10TIX provides a service that validates and verifies acceptable credentials. The service operates on scans of identity documents, such as ID cards, passports, and driving licenses; on bills and other documents related to physical addresses; videos and selfies recorded on a

mobile device. The service validates that the submitted materials were not forged and submitted by legitimate actors.

AU10TIX provides a service to business and not directly to applicants and end-users. Customers grant access to services and benefits to their end-users and set policies, restrictions and eligibility requirements or limitations to initiate enrollment to applicants and end-users.

1.3. The ID Document Life Cycle

Once a customer initiates the service, the credentials are collected and sent to AU10TIX. There are several different ways to capture and send ID documents to AU10TIX. Acceptable ID documents are then validated and verified before the process results are presented to the customer.

1.3.1. Collection

There are several different ways to capture and send ID documents to AU10TIX.

- Customers can internally collect images of the ID documents and process them directly to AU10TIX using the appropriate API calls.
- Customers can embed AU10TIX elements in their website or mobile application. The end users then use those elements to upload the image files to AU10TIX.
- Customers can redirect end users to the AU10TIX Web App. End users then use the AU10TIX Web App to upload image files of ID documents and selfies to AU10TIX.

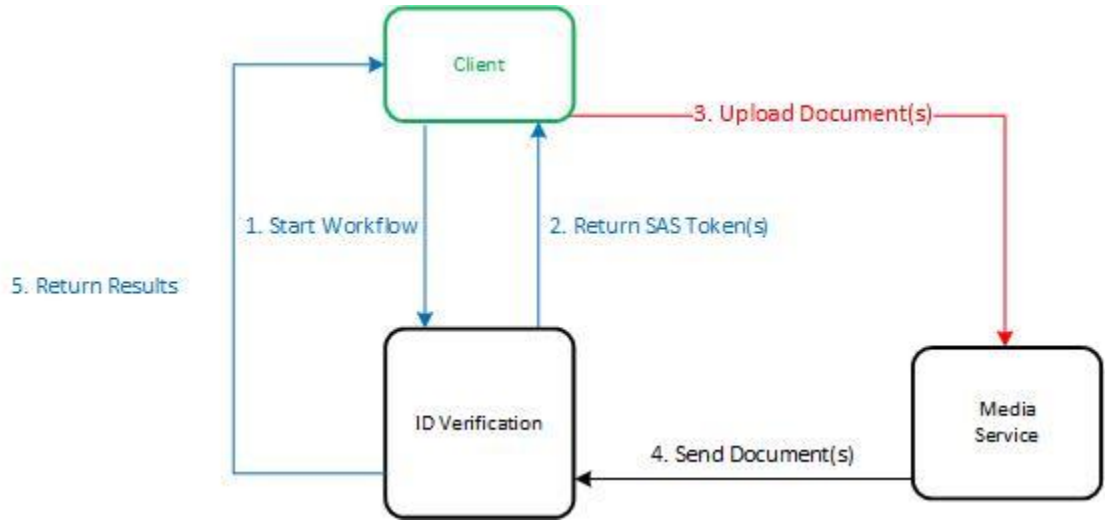
1.3.2. Processing and Results

Once the image files are collected in the ways described above, they are automatically processed and analyzed unsupervised. AU10TIX then delivers the results of the analyses to the customer. The image files are kept according to Customer's instruction in a signed Data Protection Agreement or by AU10TIX'S data retention and deletion policy. The analysis results are saved; customers can access them later through a web interface (Console). The results are retained for a period defined by the customer in a signed Data Protection Agreement or by AU10TIX'S data retention and deletion policy.

2. The Credentials (IDV) Process Steps

Each ID submitted to AU10TIX for authentication is subjected to a series of procedures and tests to determine, to the greatest extent possible, whether the ID is authentic.

2.1. Workflow Diagram



1. Customers must undergo an authentication process (see below, under **2.2 Authentication**). AU10TIX accepts only authenticated API calls.
2. Customers receive a response with authentication tokens needed to upload the media files. A separate authenticity token is generated for each media file.
3. Image files undergo a preparation process before the automatic verification process (see below, under **2.3 Credentials Preparations**)
4. The image files of the submitted ID documents are analyzed (see under **2.4 ID Validation** and later sections)
5. The customer receives the results of the verification process (automatic, and manual for customers who select it, see under **2.6 Exception Management**).

2.2. Authentication

AU10TIX only accepts API calls with verified access tokens in their header to preserve privacy and security. All the collection methods described above require the customers to use access

tokens. Customers issue private and public key pairs during onboarding, maintaining access integrity. Customers who did not undergo the proper onboarding process will not have a proper key pair and will be unable to issue an operative access token.

As a further precaution, access tokens are issued for a limited time, based on the collection method. Once a token expires, customers must generate a new access token. API calls with outdated access tokens are not accepted.

The credentials process tests uploaded credentials and checks that they are image files and have the minimum required resolution for proper analysis. The credential process validates the uploaded credentials in multiple ways.

2.3. Credentials Preparations

Accepted credentials undergo preparation processes before undergoing validation and verification.

- **Qualification:** Assesses if the image quality meets the minimal standards required for successful processing. It also determines whether or not the image is an ID.
- **Optimization:** The image is optimized to compensate for any deficiencies in the image quality. This involves, for example, straightening the alignment and sharpening the image.
- **Classification:** The credential is automatically classified by country or state of issue and by document type (for example, Passport, Driver's License, and ID Card) and version number. This is done by comparing the submission against a catalog of Format Profiles which contains detailed information about the structure and format of various ID credential types. The catalog of Format Profiles has over 17,000 samples and frequently updates. This classification enables the system to proceed with the data extraction and authentication tests. The full list of supported Format Profiles can be found on the AU10TIX documentation knowledge base (you must be a customer to have access to the knowledge base).

- **Data Extraction**: The data shown on the ID is extracted field by field using the AU10TIX OCR (Optical Character Recognition) engine. Each data element is identified separately (for example, Name, Date of Birth, Place of Birth and so on) based on the Format Profile for that ID type. This enables the execution of a wide range of tests to verify the validity of the information given in each field. AU10TIX offers an option to optimize the data extraction process by comparing the OCR results with ID information submitted by the applicant in their application form.

2.4. ID Validation

The **ID Authentication Process** establishes that the ID conforms to the layout of an official ID of the specified type and that neither the physical ID nor the submitted image has been replaced, fabricated, or altered. This ensures that all identity information shown in the ID is accurate.

2.4.1. ID Layout

The credentials process validates the layout of the submitted credentials and checks against the correct layout of that type of ID document. The process verifies that the structure of the submitted ID conforms to the structure and format specifications of the Format Profile for that ID Type. This includes elements such as fonts and text alignment.

2.4.2. Data Integrity

AU10TIX verifies that all data is valid for the fields in which it appears. This includes validating the checksum for each numeric data element and verifying that all dates are valid and reasonable for the specified fields. It also involves ensuring that all identity data are shown in the Visual Inspection Zone (VIZ), Machine Readable Zone (MRZ), and Two-dimensional (2D Barcode) and Machine-Readable Chip (MRC) sections are identical.

2.4.3. Authentic Image

The credentials process validates that neither the physical ID nor the image in the uploaded credentials was fabricated or doctored. The process checks elements in the image for signs of image manipulation, the digital attributes of the files themselves, and compares them to other

files to identify forgeries. The process verifies that the image was not manipulated using digital means, for example, image editing software.

2.5. Legitimate Actor

The credentials process validates the submission made by the person represented in the ID document by comparing the picture in the ID document with the selfie picture taken during the submission or other verified images. The process can also check the selfie for signs of manipulation.

2.5.1. Biometric Tests

The **Biometric Tests** establish that the submission is being made by a live person whose image matches the ID image and provided its consent to the Controller for biometric processing. Biometric Tests attempt to detect instances of identity theft.

2.5.2. Face Matching Test

The Face Matching test compares the ID photo to a selfie submitted by the customer applicant to check for similar facial features. The Face Matching test consists of the following stages:

- Capturing a selfie or acquiring a facial image from a video stream (when using Mobile SDK).
- Face detection, alignment, and cropping to create an ovoid facial image.
- Normalization of portraits using the Viola-Jones method.
- Comparison of the faces which captured to the one on the ID using deep learning models.

2.5.3. Liveness Test

For submissions made using our AU10TIX Mobile SDK, the biometric test includes a liveness test to verify that the face-matching selfie is captured from a live person, not a static image.

The test is executed by instructing the subject to follow a randomized series of gestures. While the subject makes these gestures, the system identifies his/her face and tracks its movements to ensure that the captured face in the selfie is the same as the person making the gestures.

In the Liveness Test, AU10TIX detects:

- 3-dimensionality
- Face reflection
- Face texture
- Axial movement

2.6. External Validation

AU10TIX checks verified external records of living people and validates the details in the ID document correspond to verified details in the records. AU10TIX also checks that the person is not flagged as a threat or a suspect of money laundering or other fraudulent acts.

2.6.1. Data Verification and Screening and Proof of Address

The **Data Verification & Screening (DVS),** together with the **Proof of Address (POA),** establishes that the ID information corresponds to external records for this person. AU10TIX compares the ID data with issuing and authoritative sources to verify the claims on the ID. The DVS also screens for blacklisting based on money laundering or fraud risk factors. The solution is available globally.

- **Personal Verification:** AU10TIX verifies that the identity information submitted matches the records that appear in external databases for that identity.
- **Anti-Money Laundering (AML)**: AU10TIX checks if the identity submitted poses a risk for money laundering. AU10TIX checks both domestic and international Politically Exposed Person (PEP) lists as well as blacklists based on criminal records or problematic online activity.
- **Proof of Address (POA):** The applicant submits a utility bill or bank statement showing their address (in addition to the ID submission). AU10TIX uses Optical Character Recognition (OCR) to extract the name and address and verifies that the name in the document matches the name shown in the ID.

2.7 Exception Management

AU10TIX offers an ad hoc manual verification service to which clients can opt-in. Manual verification is performed on images lacking sufficient quality to be processed automatically.

The manual verification service is performed by trained personnel, ensuring accurate and complete document inspection. The Exception Management service is quick and has no unsupported documents. All documents are recognized and properly classified.

The results of the manual verification service are combined with the automated verification service and made available through the same communication channels, and both raw and compiled results are returned.

The Exception Management service maintains data protection consistency with the automatic verification service. Once the agent completes the verification, the data is erased.

3. Serial Fraud Monitor

The Serial Fraud Monitor is an optional service. It is an adaptive analytics and data platform that monitors the documents AU10TIX collects and detects bad actors and fraudulent documents based on emerging patterns and similarities to other fraudulent documents and actors.

The Serial Fraud Monitor captures the results from the verification process described above. The Monitor hashes and archives the mathematical descriptors. For customers who subscribe to the Serial Fraud Monitor service, during the credentials process, the Monitor compares the mathematical descriptors in the processed ID documents with the existing mathematical descriptors. The Monitor returns two new entities:

- Repetition - risk indicator that holds the number of repeated occurrences.
- Conflicts – a risk indicator indicating a mismatch between the new and existing archived data.

Revision History

Revision	Description of Changes	Author	Date
1.0	Initial release	Sarath Laufer	July 1, 2023


AUTØTIX
IDENTITY INTELLIGENCE