AU10TIX

IDENTITY INTELLIGENCE

Au10tix Credential (IDV) Policy

Contents

Legal Notice 3

1. Introduction 4

1.1. Purpose and Scope 4

1.2. Roles and Responsibilities 4

1.3. Data Protection and Privacy 4

1.4. Standards and Methodology 5

1.5. GPG45 Methodology Overview 5

2. Identity Profiles Supported 6

3. The Credential Verification (IDV) Process Steps 6

3.1. The Credential Life Cycle 6

3.1.1. Evidence Collection 6

3.1.2. Processing and Results 7

3.2. Workflow Diagram 7

3.3. Authentication 8

3.4. Credentials Preparations and Evidence Strength 8

3.5. Credential Validity check 9

3.5.1. Data Integrity 9

3.5.2. Image Authenticity and Tamper Detection 10

3.5.3. Cryptographic Security Features 10

3.6. Identity Fraud Checks 10

3.6.1. Serial Fraud Monitor 11

3.7. Verification and Biometric Controls 11

3.7.1. Face Matching Test 11

3.7.2. Liveness Detection 11

3.8. External Data Verification, Screening, and Proof of Address..... 12

3.9. Exception Management..... 13

AU10TIX
IDENTITY INTELLIGENCE

Legal Notice

This document contains proprietary and confidential material of Au10tix ("**AU10TIX**") and its subsidiaries. Any unauthorized reproduction, use, or disclosure of this material, or any part thereof, is strictly prohibited. This document is solely for the use of AU10TIX employees and authorized AU10TIX customers. The material furnished in this document is believed to be accurate and reliable. However, no responsibility is assumed by AU10TIX for the use of this document, or any material included herein, and it is not intended to constitute a warranty by AU10TIX that such details, specifications, or other information or documentation satisfy any applicable laws or other.

AU10TIX reserves the right to make changes to this document or any material included herein at any time and without notice.

For more information, visit: www.AU10TIX.com

Copyright © AU10TIX 2026

All Rights Reserved.

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.

This document is intended for AU10TIX's staff, applicants, end-users, Conformity assessment Bodies, auditors, and customers (relying parties) who want to receive a high-level description to understand the Credentials (IDV) Policy.

1.2. Roles and Responsibilities

AU10TIX acts as an **Identity Service Provider** supporting customers (relying parties) by performing identity evidence checks and verification controls. AU10TIX does not make access, eligibility, or entitlement decisions and does not assert identity outcomes on behalf of customers.

Customers remain responsible for:

- Selecting the applicable identity profile or assurance level according to their use case(s)
- Determining whether a transaction meets regulatory or business requirements
- Making final decisions based on the outputs provided.

1.3. Data Protection and Privacy

AU10TIX takes privacy issues very seriously and invests significant resources and time to protect the privacy of personal data. Au10tix comply with the relevant obligations under the General Data Protection Regulation (EU) 2016/679 (the "**GDPR**"), the UK 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 and the UK GDPR: "**The Laws**") and assist controllers and customers in exercising their own obligations under The Laws.

Data processing is governed by contractual agreements with customers, including Data Processing Agreements that define the subject matter, purpose, duration, data categories, retention periods, and safeguards. Image data and identity verification results are retained in accordance with customer instructions or AU10TIX's Data Retention and Deletion Policy.

Any other description of Au10tix's functions as a data processor can be found in the Master Service Agreement and in the different company policies.

1.4. Standards and Methodology

AU10TIX's Credential (IDV) Policy is designed to align with:

- NIST SP 800-63A identity proofing requirements for Identity Assurance Level 2
- The UK Digital Identity and Attributes Trust Framework (DIATF)
- The UK government guidance "How to prove and verify someone's identity" (Good Practice Guide 45, GPG45)

NIST SP 800-63A provides control objectives and identity proofing requirements, while GPG45 provides an outcome-based methodology for describing identity checking through defined checks and identity profiles. AU10TIX aligns its controls to support both frameworks consistently.

1.5. GPG45 Methodology Overview

GPG45 defines identity checking as a set of five checks:

1. Evidence strength
2. Evidence validity
3. Activity history
4. Identity fraud
5. Verification

These checks combine to meet defined **identity profiles**. Profiles are not calculated by summing scores. Each required check must meet or exceed the required level for the profile to be achieved.

2. Identity Profiles Supported

AU10TIX has been independently assessed under the UK Digital Identity and Attributes Trust Framework and has demonstrated the capability to support the following GPG45 identity profiles, subject to customer configuration and evidence availability:

- M1A
- M1C
- H1A
- H2D

AU10TIX provides the evidence checks and verification controls required to support these profiles.

3. The Credential Verification (IDV) Process Steps

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

3.1. The Credential Life Cycle

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

3.1.1. Evidence Collection

There are several different ways to collect and upload ID documents to AU10TIX.

- Customers can internally collect images of the ID documents and upload them directly to AU10TIX using the appropriate API calls.

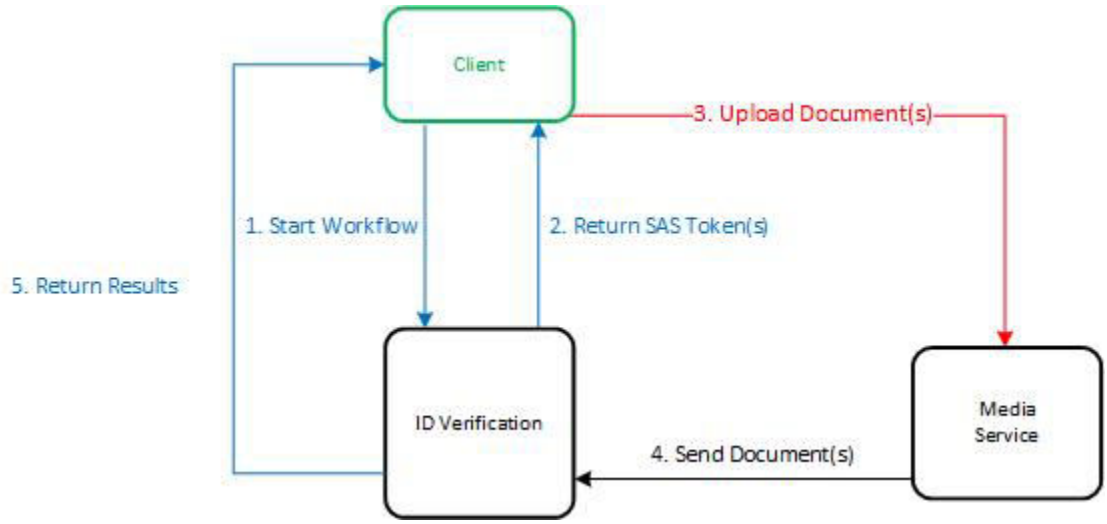
- Customers can embed AU10TIX elements in their website or mobile application. The end users then use those elements to upload the image files to AU10TIX.
- Customers can redirect end users to the AU10TIX Web App. End users then use the AU10TIX Web App to upload image files of ID documents and selfies to AU10TIX.

All methods require authenticated access tokens issued during customer onboarding.

3.1.2. 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 analysis to the customer. The analysis results are saved; customers can access them later through a web interface (Console). The images files and 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.

3.2. Workflow Diagram



1. Customers must undergo an authentication process (see below, under **3.2 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 **3.4 Credentials Preparations**)

4. The image files of the submitted ID documents are analyzed (see under **3.5 Credential Validity check** 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**).

3.3. Authentication

AU10TIX only accepts API calls with verified access tokens in its 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 complete the proper onboarding process will not have a valid key pair and will be unable to issue an operational access token.

As a further precaution, access tokens are issued for a limited time, between 10 minutes and 24 hours, 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.

3.4. Credentials Preparations and Evidence Strength

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 1,879 samples and is frequently updated. 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.

3.5. Credential Validity check

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.

3.5.1. 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.

3.5.2. Image Authenticity and Tamper Detection

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.

3.5.3. Cryptographic Security Features

Where identity evidence includes cryptographic security features, AU10TIX validates digital signatures and verifies that signing keys:

- Belong to the issuing authority
- Are of the correct type
- Have not been revoked

3.5.4. Expiry and Status Checks

Where supported by the evidence type and available sources, AU10TIX checks document expiry and may support cancellation, lost, or stolen status checks where configured.

3.6. Identity Fraud Checks

AU10TIX supports identity fraud risk checks to identify indicators of stolen, synthetic, deepfakes or high-risk identities, where configured by the customer and supported by authoritative sources.

Identity fraud checks are distinct from AML or sanctions screening and are designed specifically to support GPG45 identity fraud requirements.

Where elevated risk is detected, AU10TIX supports escalation through additional evidence, verification controls, or manual review.

3.6.1. Serial Fraud Monitor

The Serial Fraud Monitor is an optional service but mandatory to support GPG45 identity fraud requirements. 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. The Monitor hashes and archives the data into an Operational Data Store (ODS). For customers who subscribe to the Serial Fraud Monitor service, during the credentials process, the Monitor compares the new data in the processed ID documents with the existing data in the ODS. 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.

3.7. Verification and Biometric Controls

3.7.1. 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 oval facial image.
- Normalization of the portraits using the Viola-Jones method.
- Comparison of the faces using deep learning methods.

3.7.2. Liveness Detection

AU10TIX performs liveness detection to verify that biometric samples are captured from a live person and to detect spoofing or replay attacks. The test is executed by instructing the applicant or end-user 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
- Deepfakes

3.8. External Data Verification, Screening, and Proof of Address

Where required, mandated or configured by the customer, AU10TIX performs external data verification checks using governmental, authoritative, or other trusted data sources that are expected to maintain reliable identity information. These checks are used to support verification of identity attributes, and evaluation of identity fraud risk, in accordance with the applicable use case and confidence requirements.

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.

3.9. 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.

Revision History

Revision	Description of Changes	Author	Date
1.0	Initial release	Sarath Laufer	July 1, 2023
2.0	Review of policy	Udi Abram	March 1, 2024
3.0	Review of policy and update header information.	Sarath Laufer Udi Abram	November 13, 2025
4.0	Mapping UK GPG 45 identity profiles	Sarath Laufer	January 25, 2026

AUTØTIX
IDENTITY INTELLIGENCE