Welcome to B-Trust Documentation

Welcome to B-Trust Documentation

Welcome to the official documentation for B-Trust, your comprehensive solution for secure and efficient identity validation through facial biometric verification. B-Trust is designed to cater to a wide range of applications and industries, offering a flexible and robust platform for confirming identities with precision and ease.

What is B-Trust?

B-Trust represents the forefront of identity verification technology, combining advanced facial recognition algorithms with a suite of integration options to fit every client's needs. Whether you're looking to incorporate biometric verification directly into your mobile app, web application, or prefer a fully managed web experience, B-Trust provides the tools and flexibility necessary for seamless integration.

With B-Trust, you can

- Enhance Security: Utilize cutting-edge facial biometric technology to verify identities, reducing the risk of fraud and unauthorized access.
- Streamline User Experience: Offer your users a quick and effortless verification process, improving satisfaction and trust in your services.
- Adapt to Your Needs: Choose from our Android, iOS, or JavaScript SDKs for direct integration and use our comprehensive APIs to connect with the B-Trust platform. For those seeking a no-setup solution, our managed web experience handles the entire flow from start to finish.

Getting Started with B-Trust

Embarking on your journey with B-Trust's identity validation solutions begins here. This section is meticulously crafted to guide you through the initial setup and integration process, ensuring a smooth and efficient start. B-Trust's integration flexibility, through SDKs or a fully managed web experience, is complemented by a comprehensive suite of APIs. These APIs are integral to all integration paths, facilitating the seamless operation and enhanced functionality of your identity validation workflows.

Initial Steps

Before diving into the technical integration, let's start with the foundational steps to access B-Trust:

1. **Contact Our Sales Team**: To get started with B-Trust, reach out to our sales team. They will guide you through our solutions, helping you choose the best fit for your needs.

2. **Account Setup and Credentials**: Following your discussion with the sales team, they will set up your B-Trust account and provide you with the necessary credentials. These credentials are essential for accessing our SDKs, APIs, and the managed web experience.

Choosing Your Integration Path

With your account set up, it's time to decide how you'll integrate B-Trust into your system:

- **SDKs (Libraries)**: For integrating directly into your mobile or web applications, our SDKs for Android, iOS, and JavaScript offer a native user experience. Utilize B-Trust APIs for data submission and verification results.
  - Android SDK Guide
  - iOS SDK Guide
  - JavaScript SDK Guide
- **Web Experience**: For a quick and easy setup, direct users to our fully managed web page that handles the entire verification flow. This option is complemented by B-Trust APIs for a comprehensive integration.
  - Web Integration Guide

Understanding B-Trust APIs

B-Trust APIs play a crucial role in all integration paths, facilitating the submission of biometric data, managing the verification process, and retrieving results. Familiarize yourself with our API documentation to fully leverage B-Trust's capabilities in your application or service.

API Documentation

Explore our detailed API documentation for information on endpoints, request/response formats, and practical use cases.

- API Reference

Welcome aboard! You're now on your way to implementing B-Trust's advanced identity validation solutions. Should you have any questions or need assistance, our dedicated support team and your sales representative are here to help.

Glossary

ENROLLMENT
The process through which the acquisition of images (facial photograph, front and back of the identity document), eventually fingerprints through external biometric captors, is performed in order to apply internal protocols for reviewing imprint-technical characteristics on the document, as well as comparing the facial features of the document contained within the document against the client's facial photograph at the time of submission.

VERIFICATION
The process through which the acquisition of a facial photograph and/or fingerprint is performed to compare it against those previously existing in the database for the identity in question and determine whether they belong to the same person or not. This process assumes and requires at least one previous successful enrollment before using this functionality.

OCR
Optical Character Recognition, allows the collection of images (front and back of the document) for the purpose of reading the information contained in the identity document presented by the client.

CLIENT
Natural or legal person who acquired the service with ADO and who signs the contract as the responsible party for the demanding part of the service.

END USER
Natural person on whom enrollment and/or OCR reading and/or verification are intended to be executed.

PROJECT NAME
Name created and managed from the ADO platform, which identifies a project within the platform provided by Ado Technologies SAS (hereinafter ADO), for the provision of the service. Within the same website, one or more projects may exist at the same time.

API KEY
Alphanumeric string created and managed from the ADO platform, which grants or denies access to services associated with each of the projects created within the platform.

BASE URL
It is the URL provided by ADO as a platform for the provision of the service, which defines the final interaction site of the SDK with a specific website.

Service Response Dictionary

The final rating of transactions is determined after the user passes through the biometric engine. This rating is found within the JSON object returned by our service, either through a callback or via a data push configuration. This object contains the "StateName" field, describing the final classification, and the "IdState" field, serving as the identification for this same rating. This process provides a precise and secure measure of the quality and validity of the transactions conducted, enabling us to understand the final outcome and how to handle them appropriately.

- **IdState: 1**
  - **NameState**: Pending
  - **Description**: Applies to cases where some indication or alert is detected regarding the documents and/or their correspondence with the bearer. The case is referred to analysis by the BackOffice, and the definitive response will be delivered within the agreed times in the ANS.
- **IdState: 2**
  - **NameState**: Successful Process
  - **Description**: Applies to images of authentic documents with uniprocedence facial (document vs selfie).
- **IdState: 4**
  - **NameState**: Authentic Document without Facial Comparison
  - **Description**: Applies when the facial score does not exceed the approval threshold.
- **IdState: 5**
  - **NameState**: Erroneous Capture
  - **Description**: The user captures partial images of low quality, which prevents a judgment until they are improved.
- **IdState: 6**
  - **NameState**: Invalid Document
  - **Description**: Formats of documents not agreed upon in the service level agreements are provided.
- **IdState: 8**
  - **NameState**: Altered Document
  - **Description**: Documents issued by the real issuing entity but present alterations or adulterations in one or more of their fields or technical characteristics.
- **IdState: 9**
  - **NameState**: False Document
  - **Description**: Documents totally or partially produced outside the issuing entity.
- **IdState: 10**
  - **NameState**: Face does not correspond
  - **Description**: Applies to cases where the facial score of a correspondence between the bearer and the content in the document does not reach the minimum defined as secure between the contrast and the contractor.

- **IdState: 11**
  - **NameState**: Fingerprints do not correspond
  - **Description**: Applies to cases where the fingerprint score of a correspondence between the bearer and the content in the document does not reach the minimum defined as secure between the contrast and the contractor.
- **IdState: 14**
  - **NameState**: Previously Registered Person
  - **Description**: Applies to cases where the face and/or identification number of the client were previously registered before the current attempt.
- **IdState: 15**
  - **NameState**: Error
  - **Description**: Reserved for various communication, slowness, or unavailability errors between the SDK and the server.
- **IdState: 16**
  - **NameState**: Person found in control lists.
  - **Description**: Reserved for matches in control lists for names and identification numbers.
- **IdState: 18**
  - **NameState**: Block
  - **Description**: Reserved for blocking identification numbers for a defined period of time.

DocumentType

*This document type is accepted by our service and is referenced by an integer **ID**. Before using it in any request, verify with **Support** which document type will be validated so we can enable it via the **dashboard**.*

ID	Nombre	País / Entidad
1	Cédula de ciudadanía	Colombia
2	PEP solo con Pasaporte	Colombia
3	Cédula de ciudadanía Ecuatoriana	Ecuador
4	Cédula de extranjería	Colombia
5	Tarjeta de identidad	Colombia
6	Card ID Israel	Israel
7	Cédula de ciudadanía Panameña	Panamá
8	Cédula de ciudadanía Peruana	Perú
9	Cédula de ciudadanía Paraguaya	Paraguay
10	INE México	México
11	Cédula de identidad Chilena	Chile
12	Identificación Puerto Rico	Puerto Rico (EE. UU.)
13	Cédula de identidad Costa Rica	Costa Rica
14	Documento personal de identificación Guatemala	Guatemala
15	Cédula Uruguaya	Uruguay
16	Cédula de Ciudadanía Boliviana	Bolivia
17	PPT (Permiso por Protección Temporal)	Colombia
18	Documento Nacional de Identidad (DNI)	España
19	Documento Nacional de Identidad (DNI)	Argentina
20	Pasaporte	Cualquier país
21	Cédula de Identidad y Electoral	República Dominicana

Changelog Livennes

2.5

- General optimization of the capture and validation flow to improve stability across consecutive sessions.
- Performance adjustments to reduce latency when returning results to the host.
- Initial improvements in evidence reduction (Base64) to decrease payload size.

2.6.0

- Camera pipeline optimization for smoother performance on mid-range devices.
- Evidence compression adjustments to reduce transfer size and improve delivery times.
- UX improvements with clearer feedback during alignment and capture.

2.7.0

- Facial tracking optimization for better face stability within the frame.
- Performance improvements in frame processing to reduce sustained CPU/GPU load.
- Flow logic adjustments to improve consistency between capture, analysis, and results.

2.8.0

- Optimization of evidence return to the host through more efficient Base64 generation and encoding.
- Further reduction of image/evidence size while maintaining reference quality.
- Visual experience improvements for greater consistency across resolutions and devices.

2.9.0

- Optimization of camera startup and shutdown, as well as flow recovery during retries.
- Memory usage improvements to prevent performance degradation after multiple runs.
- User feedback adjustments to reduce friction and increase process clarity.

3.0.0

- Major SDK evolution focused on performance and lifecycle stability of the component.
- Analysis pipeline optimization for smoother execution and more consistent response times.
- Improvements in resource handling (camera and memory) for longer sessions.

3.0.3

- Optimization of camera session startup and transition into analysis to reduce startup times.
- Efficiency adjustments to reduce CPU/GPU spikes during initialization.

3.0.8

- Improvements in evidence compression and serialization: lighter Base64 and faster delivery to the host.
- Flow optimization to reduce latency between capture and final result.

3.1.0

- Logic adjustments for greater consistency in the validation flow.
- Memory usage optimization in repeated sessions to improve stability.

3.1.5

- UX improvements with clearer and more consistent feedback during the capture process.
- Performance optimization on resource-constrained devices to maintain smoothness.

3.2.0

- Optimization of the retry system without full reinitialization to improve flow continuity.
- Evidence compression adjustments to reduce payload size while maintaining adequate quality.

3.2.6

- Optimization of frame processing to reduce sustained CPU/GPU load.
- Camera pipeline stability improvements for uninterrupted analysis.

3.3.0

- Increased robustness of facial analysis under lighting variations and moderate movement.
- Optimization of evidence generation and encoding for faster return to the host.
- Performance adjustments to maintain more stable FPS during the session.

3.3.7

- Optimization of camera module initialization time and analysis preparation.
- Internal adjustments for a more stable experience during prolonged runs.

3.4.0

- Facial tracking optimization for greater consistency of the face throughout the session.
- Performance improvements in evidence compression (Base64) to reduce transfer size and timing.

- Visual experience adjustments for consistency across different resolutions and devices.

3.4.6

- Optimization of memory usage and resource release at the end of the flow to maintain stability.
- UI/Render performance improvements through reduced style load and smoother transitions.

3.5.0.1

- Integration of the new Liveness engine with advanced face detection and emotion/gesture analysis.
- Optimization of the capture and validation flow.
- Design and user experience improvements (UI/UX).
- Reduced latency in the camera pipeline.
- Greater robustness against flow manipulation.

3.5.2.0

- Improved facial detection system for gesture recognition.
- Specific optimization for devices with Snapdragon 8 Elite.
- Strengthened anti-spoofing signals.
- Greater efficiency in resource consumption during active sessions.

3.5.2.1

- Optimization of component initialization and instantiation.
- Localization and language consistency improvements.
- Additional performance adjustments.
- Refinement of control logic and result delivery.