ABBYY

ABBYY® Proof of Identity 1.0

Integration Guide

© 2022 ABBYY Development, Inc. All rights reserved.

Table of Contents

Introduction

ABBYY Proof of Identity provides a complete solution for confirming the identity of a customer with the help of a selfie photo and an ID document scan. This guide will help you integrate Proof of Identity into your website.

- Configuration
  Setting up the service
- Integrating Proof of Identity built-in UI
  Starting, pausing, and continuing the workflow for the end user
- Getting the results
  Receiving and processing the data from the identity documents and additional documents uploaded by the user

Configuration

Before using Proof of Identity, you'll need to configure its processing settings and optionally appearance.

Initial setup

ABBYY Proof of Identity is using ABBYY Vantage platform. You will need an ABBYY Vantage tenant with Proof of Identity capabilities enabled. If you don't have one, please contact sales.

When you first log in to admin interface https://poi-us.abbyy.com/admin as a Tenant administrator, you will see an **Onboarding** page that will help you get started. This page will also be available later if you need to change anything. On this page, go through the steps:

1. Create user roles needed for Proof of Identity. The super user for your tenant will have **Tenant administrator** role and will be able to create new users and assign roles.
2. Create credentials for the technical user. We strongly recommend using the e-mail address and password generated by the form. This e-mail address will be a fake one, but it will use the same domain name as the e-mail of the tenant administrator who is creating the technical user.
   Store these credentials securely: you will not be able to access or restore them later. If you lose the technical user credentials, you will have to create a new one and change the credentials on all your application instances.
3. Create client ID and secret for access to the API. If you already have a Public API client from Vantage with Resource Owner Password Credentials flow enabled, you can use that as well. Save the generated credentials.
4. Enter the URL which will accept the results on your side and select **Create configuration**.

⚠ **Important!** The result URL should accept POST requests. You will be able to tune its security parameters after the configuration is created.

5. To get all credentials generated during this procedure, select **Download credentials**. You will receive a JSON file with technical user e-mail, password, client ID and client secret. Save this data, as you will need it to start a workflow with Proof of Identity.

Settings

⚠ **Important!** To change the settings, you'll need to be logged in as a **Tenant administrator** or **POI Configuration manager**. See more in Role-based access.

Once you have created the user roles and generated credentials, you will be able to access other settings.

Global tenant settings

- Set the time the user has to complete identity verification workflow.
- Configure data retention period to ensure that the sensitive data is stored for exactly as long as you need.
- Tune the parameters of the receiving webhook that the Proof of Identity will call for each completed workflow:
  - set up the headers you require for the request
  - set mutual TLS authentication if needed
  - make Proof of Identity send the data for each completed workflow encoded in a JWT token
- See the list of all reviewer e-mails. After you add a new user with **POI Reviewer** role, use the **Synchronize users** button to update the list. All these users will receive an e-mail notification when a transaction needs review.

Workflow

The same settings apply to all workflows of a tenant.

- Auth options:
  - the verification methods you allow: e-mail, SMS to a phone number, QR code
  - whether you require confirmation of the user's address or number to transfer the session to another device
  - the lifetime of authorization code
  - choose if you want to always continue the workflow if the same identifier is passed, or you would like to restart
- ID capture: set the number of attempts and types of documents you allow, configure if you accept manually uploaded documents or only images directly from the mobile device's camera
- Selfie capture: set the number of attempts and if we should verify selfie liveness (which we recommend)
- Additional documents: choose Vantage skills to process the documents
- Custom status messages: enter messages you would like to display if our defaults don't work for you
- Workflow steps: specify if you allow or require the user to review the captured data

UI Customization

Set the colors and logo for your service.

Note: If any workflows are already running, changing the configuration won't affect them. Only the workflows started after configuration update will have the new settings.

Integrating Proof of Identity UI

This article will help you integrate Proof of Identity into your portal in the simplest way, requiring almost no code to be written on your side.

Prerequisites

Obtain the credentials as described in Configuration > Initial setup.

Configure the processing settings and optionally the appearance of Proof of Identity user interface. See Configuration > Settings.

Step-by-step implementation

Let's walk through the simple use case: the user logs into your portal, you open ABBYY Proof of Identity UI that guides the user through the required steps, then after processing completes, the Proof of Identity service sends you the results.

1. After the user has logged into your portal and started some process that requires proving their identity, you need to start a workflow in Proof of Identity. The workflow will be associated with the credentials of your tenant and the user identifier you choose to provide, but the user themselves will not have to log into Proof of Identity.
   For security reasons, we strongly suggest that you don't allow your service front end to access the client ID and secret. From a secure context—probably your back-end environment—send a POST request to the **workflows** resource:

   ```
   POST https://poi-us.abbyy.com/public/workflows
   ```

   The JSON body of the request must contain:

   - A unique identifier for the new workflow.
     This identifier will be used to resume the workflow after a pause. If you don't allow workflow pause, you may pass any string for this parameter.
   - The credentials for the technical user (**POI Technical user** role), client ID and client secret.
     See Configuration to find out how to create a technical user and an API client, and Role-based access for details on the roles.

   You can also optionally include:

   - User identifiers for your system.
     After the workflow completes, these identifiers will be sent attached to the results. For example, a user's ID in your system can be used here to let you know when this user has successfully proved their identity.

- Verified e-mail addresses and phone numbers.
  If at any point the user needs to switch to another device—for example, to take a selfie with their smartphone—Proof of Identity will send them a link in an SMS or e-mail. Normally, they would need to verify the phone number or e-mail address first, but if you provide an already verified number or e-mail here, they will be able to skip verification and receive the link directly.

Here is a sample request body:

```
{
   "processIdentifier": "unique_workflow_identifier",
   "externalIdentifiers": [ "id1", "id2"],
   "verifiedEmailAddresses": [
      "trusted_email_address_of_end_user@mail.net",
   ],
   "verifiedPhoneNumbers": [
      "+1234567890",
   ],
   "credentials": {
      "clientId": "your_client_id",
      "clientSecret": "client_secret_string",
      "username": "technical_user@your_mail_domain.com",
      "password": "technical_user_password"
  }
}
```

The response will contain a short-living unique key that will identify the session with ABBYY Proof of Identity:

```
{
    "workflowSessionUrl":"url_endpoint"
    "SessionKey":"unique_key"
}
```

2. Redirect to our service or embed it into an iframe on your page, using the URL returned in workflowSessionUrl: *url_endpoint*

If you have set up a different appearance for the service, the embedded UI will look as specified in your settings.

3. The user can perform all the steps required to prove their identity: upload or capture an image of their ID, take a selfie photo, and add trailing documents. If at some point they need to switch to another device—most likely to mobile for selfie capture—Proof of Identity will prompt them to select the convenient way of receiving the new link and send it to them: via e-mail, SMS, or scanning a QR code.

Note: We are using cookies to store information about the workflow. The user will need to accept cookies from Proof of Identity website.

4. If your settings allow self-review of the data, the user will be able to see the fields extracted from their documents, and retake the images if anything was extracted incorrectly.

5. If your workflow is configured to be resumeable, the user may pause it at any time and come back later. When that happens, send exactly the same request to the **sessions** resource as in step 1, with

the same `processIdentifier`. You will get a new unique key, and follow up with the same redirect. Proof of Identity will recognize that the user hasn't finished their previous workflow and prompt them to continue with the unfinished steps.

6. After the user is done capturing and uploading their images, they quit the page, and the service continues background processing. The results will be sent to the URL specified during configuration.

7. All the details about the workflow are stored in the Admin page. Your back office reviewers may access the information and the results, and audit the transactions flagged by the service as suspicious, for example in case of doubts about the authenticity of the documents or the user's selfie.

Getting the results

Once processing is complete, Proof of Identity service will send in the data by making a POST request to the URL you specify in your tenant configuration. The data is sent in JSON format and includes user's identifier in the service, all fields extracted from the documents uploaded by the user, and the status of identity check.

Key data

The JSON file contains the full set of data extracted from the user's documents, and you can review or process any of it. But to know what actions to take, you only need to check the workflow status in the **Status** key:

Status	Description	Is user's identity verified?	Action needed
Active	Still in progress.		Wait for processing to finish.
Complete	Finished successfully.	**Yes**	Go on with the process for which you asked to verify the user's identity.
Audit	Requires back-office review.		Log into Admin UI as a POI Reviewer and check the workflow data. Confirm or reject the user's identity.
Failed	The user didn't provide valid or enough documents.	**No**	Ask the user to verify their identity in another way, for example, by coming to your office in person.
Rejected	The manual reviewer rejected the results.	**No**	
Canceled	The user decided not to go through with verifying their identity.	**No**	

Status	Description	Is user's identity verified?	Action needed
Expired	The user didn't complete the process within the time limit.	**No**	

You will also need to connect the result to the particular user. To do that, read the contents of the **UserIdentifiers** key. It contains the e-mail addresses, phone numbers, and external identifiers that you entered while starting the workflow.

For finer control, each of the workflow steps has a **Status** of its own:

Status	Description	Effect on the workflow status
Active	Waiting for the user to take pictures or upload files.	
Processing	Working with the images obtained from the user.	
Waiting	Waiting for another step to complete.	
Verified	Processed the images and successfully verified the documents or selfie pictures, depending on the step type.	
Audit	Requires back-office review.	Workflow goes to **Audit**.
ReCapture	The user needs to send different documents or rescan the ones they provided.	Workflow goes to **Audit**. If the recapture limit was reached, workflow is **Failed**.
Rejected	The manual reviewer rejected the results.	Workflow is **Rejected**.
Failed	The service encountered an error processing the documents. Back-office review is required.	Workflow goes to **Audit**.

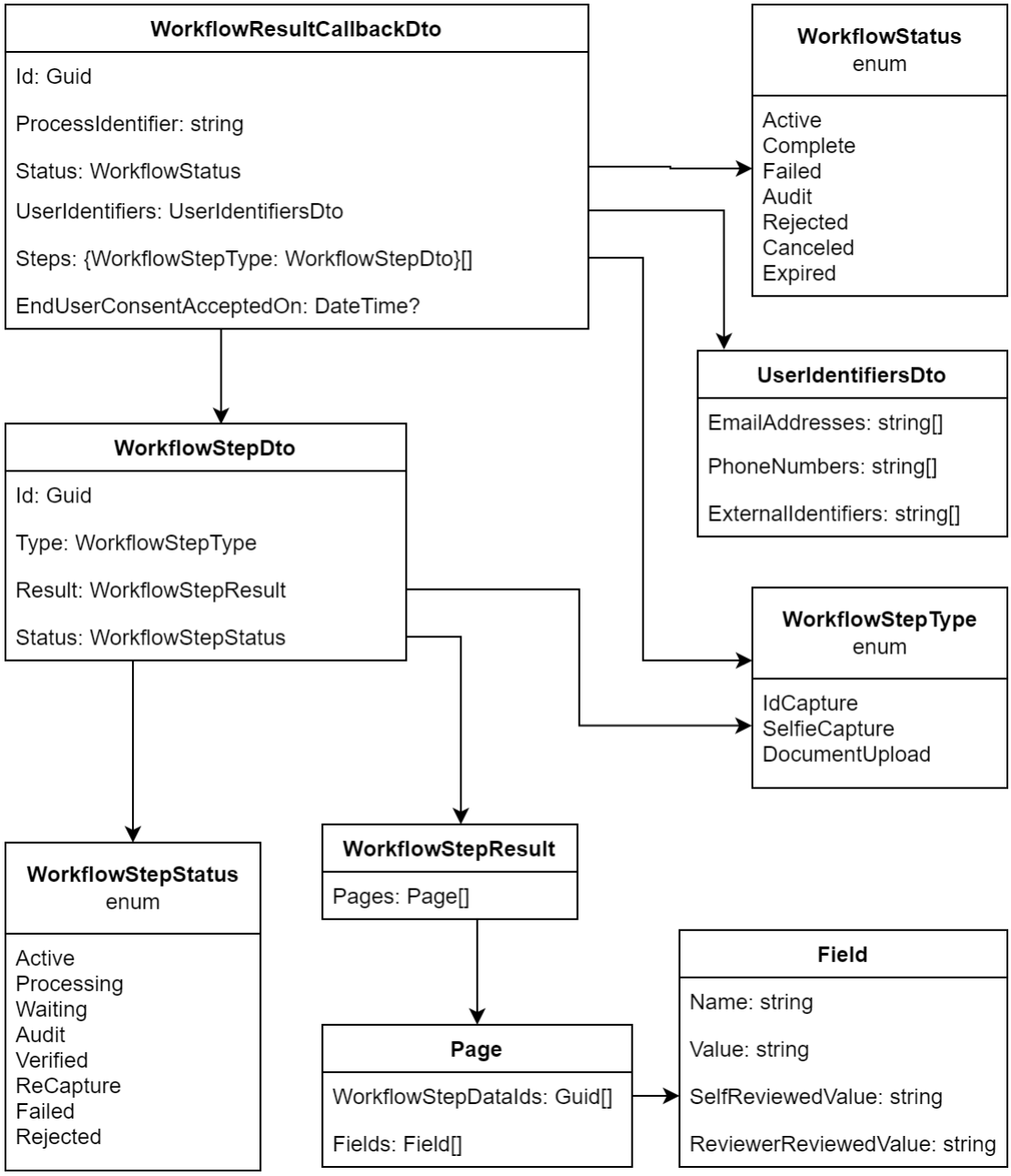
The results extracted from an ID document depend on its type. Each field has the following structure:

Key	Value
Name	The name of the field. For example, "FullName".
Value	The value extracted during processing. For example, "Jane Doe".
SelfReviewedValue	The value the user entered during self-review of the data.

Key	Value
ReviewerReviewedValue	The value entered by the manual reviewer.

If you would like to also see the images from the workflow, go to **Transactions** in the Admin UI and select **Review** for the transaction.

JSON Schema



See a sample response in the Appendix.

Role-based access

Access to resources in ABBYY Proof of Identity is managed using various roles:

- **Tenant administrator**
  Has all the rights of the other roles and can also manage the users: create new users and assign roles.
- **POI Configuration manager**
  Can set up processing settings and access Admin UI dashboards. However, this user has no access to the workflow data.
- **POI Reviewer**
  Can audit the completed workflows.
- **POI Technical user**
  Can only run workflows. You can have one or several technical users per tenant and use their credentials to start identity proof workflows. The actual end user of your application or website is anonymous to Proof of Identity.

Device requirements

iOS®

- iOS 13 or later
- iPhone X or later

Android™

- Android™ 8 or later
- Rear camera 12 MP or more
- Video recording capabilities — 2160p@30fps or more
- CPU with multiple processing cores with 2.2GHz frequency or more

Appendix

Sample result


```
{
    "Id": "5d6e79f4-ad61-4308-9a93-0d4f55f19bdb",
    "ProcessIdentifier": "Autotest 331882",
    "Status": "Complete",
```

```
"UserIdentifiers": {
    "EmailAddresses": [
        "sample@mail.com"
    ],
    "PhoneNumbers": [],
    "ExternalIdentifiers": []
},
"Steps": {
    "IdCapture": {
        "Id": "63a4b6c1-f0ae-4ebf-a640-7a68123529be",
        "Type": "IdCapture",
        "Status": "Verified",
        "Result": {
            "Pages": [
                {
                    "WorkflowStepDataIds": [
                        "83466b38-b66f-428c-98be-0418e097bb7c",
                        "9056b6c6-a9ea-4fa9-bd82-c8249e2991e1"
                    ],
                    "Fields": [
                        {
                            "Name": "FirstName",
                            "Value": "Jane",
                            "SelfReviewedValue": null,
                            "ReviewerReviewedValue": null
                        },
                        {
                            "Name": "Surname",
                            "Value": "Doe",
                            "SelfReviewedValue": null,
                            "ReviewerReviewedValue": null
                        },
                        {
                            "Name": "MiddleName",
                            "Value": "",
                            "SelfReviewedValue": null,
                            "ReviewerReviewedValue": null
                        },
                        {
                            "Name": "GivenName",
                            "Value": "",
                            "SelfReviewedValue": null,
                            "ReviewerReviewedValue": null
                        },
```

```
{
    "Name": "FullName",
    "Value": "",
    "SelfReviewedValue": null,
    "ReviewerReviewedValue": null
},
{
    "Name": "Address",
    "Value": null,
    "SelfReviewedValue": null,
    "ReviewerReviewedValue": null
},
{
    "Name": "AddressState",
    "Value": null,
    "SelfReviewedValue": null,
    "ReviewerReviewedValue": null
},
{
    "Name": "AddressPostalCode",
    "Value": null,
    "SelfReviewedValue": null,
    "ReviewerReviewedValue": null
},
{
    "Name": "AddressCity",
    "Value": null,
    "SelfReviewedValue": null,
    "ReviewerReviewedValue": null
},
{
    "Name": "AddressLine1",
    "Value": null,
    "SelfReviewedValue": null,
    "ReviewerReviewedValue": null
},
{
    "Name": "Sex",
    "Value": null,
    "SelfReviewedValue": null,
    "ReviewerReviewedValue": null
},
{
    "Name": "BirthDate",
    "Value": "01/Jan/2000",
    "SelfReviewedValue": null,
    "ReviewerReviewedValue": null
},
```

```
                        {
                            "Name": "BirthPlace",
                            "Value": null,
                            "SelfReviewedValue": null,
                            "ReviewerReviewedValue": null
                        },
                        {
                            "Name": "DocumentName",
                            "Value": "Identification Card",
                            "SelfReviewedValue": null,
                            "ReviewerReviewedValue": null
                        },
                        {
                            "Name": "DocumentNumber",
                            "Value": "000000AA",
                            "SelfReviewedValue": null,
                            "ReviewerReviewedValue": null
                        },
                        {
                            "Name": "DocumentSeries",
                            "Value": "2018",
                            "SelfReviewedValue": null,
                            "ReviewerReviewedValue": null
                        },
                        {
                            "Name": "ExpirationDate",
                            "Value": "//",
                            "SelfReviewedValue": null,
                            "ReviewerReviewedValue": null
                        },
                        {
                            "Name": "IssueDate",
                            "Value": "//",
                            "SelfReviewedValue": null,
                            "ReviewerReviewedValue": null
                        },
                        {
                            "Name": "IssuerCode",
                            "Value": "HUN",
                            "SelfReviewedValue": null,
                            "ReviewerReviewedValue": null
                        }
                    ]
                }
            ]
        }
    },
```

```
"SelfieCapture": {
    "Id": "80c6fd67-48f4-4edd-b4dd-7ffca90b2a78",
    "Type": "SelfieCapture",
    "Status": "Verified",
    "Result": {
        "Pages": [
            {
                "WorkflowStepDataIds": [
                    "5ae3a8e7-4564-4334-b513-fb60eb490b99"
                ],
                "Fields": [
                    {
                        "Name": "Selfie0",
                        "Value": "100",
                        "SelfReviewedValue": null,
                        "ReviewerReviewedValue": null
                    }
                ]
            },
            {
                "WorkflowStepDataIds": [
                    "425bece3-3dde-4611-a84a-a594c035f2a3"
                ],
                "Fields": [
                    {
                        "Name": "HeadShot",
                        "Value": "0",
                        "SelfReviewedValue": null,
                        "ReviewerReviewedValue": null
                    }
                ]
            }
        ]
    }
},
"DocumentUpload": {
    "Id": "eece440b-0126-4c6c-837b-29070ab83403",
    "Type": "DocumentUpload",
    "Status": "Verified",
    "Result": {
        "Pages": [
            {
                "WorkflowStepDataIds": [
                    "d4517e93-59cd-4940-81ed-073bcfd941e9"
                ],
```

```
                        "Fields": [
                            {
                                "Name": "Address",
                                "Value": "27 1/2 GRAND AVE\nLONG BEACH, CA 90803-8715",
                                "SelfReviewedValue": null,
                                "ReviewerReviewedValue": null
                            },
                            {
                                "Name": "FullName",
                                "Value": "JANE DOE",
                                "SelfReviewedValue": null,
                                "ReviewerReviewedValue": null
                            }
                        ]
                    }
                ]
            }
        }
    },
    "EndUserConsentAcceptedOn": null
}
```

ABBYY Proof of Identity powered by ABBYY Vantage © 2022 ABBYY Development, Inc.
ABBYY, ABBYY Vantage, Vantage are either registered trademarks or trademarks of ABBYY Software Ltd. in the United States and/or other countries.
All other product names, trademarks and registered trademarks are the property of their owners.

Information in this document is subject to change without notice and does not bear any commitment on the part of ABBYY.

The software described in this document is supplied under a license agreement. The software may only be used or copied in strict accordance with the terms of the agreement. It is a breach of the United States copyright law and international laws to copy the software onto any medium unless specifically allowed in the license agreement or nondisclosure agreements.

No part of this document may be reproduced or transmitted in any from or by any means, electronic or other, for any purpose, without the express written permission of ABBYY.