Schedule 1
Specification of Services

Defined Terms

“**iProov Technologies**” consist of certain hosted Software-as-a-Service authentication technologies, the capabilities of which can be consumed through appropriate use of certain Development Tools and specific SDKs that facilitate access to the authentication technologies. References to “**iProov Technologies**” in this Agreement include Development Tools and any other specific SDKs unless the context does not permit such an interpretation.

“**iProov Products**” refers to iProov’s products which use the iProov Technologies, such products being: (1) iProov Enroller, (2) iProov Face Verifier, (3) iProov Basic Enroller, and (4) iProov Basic Face Verifier, as further described in each case in this Schedule.

“**Minimum Requirements**” means those minimum requirements for imagery, device, software, connectivity, and other necessary attributes for the use of the iProov Products are as specified at https://docs.iproov.com/docs/Content/ImplementationGuide/resources.htm.

For the avoidance of doubt, all capitalized terms not defined herein shall have the meaning given in the Agreement (including the Schedules attached thereto, including in particular Schedule 4 (Billing Procedures)).

Dynamic (formerly GPA):

An iProov Product using Dynamic technology is intended to determine whether an End User performing a Dynamic Verification is genuinely present, and (in the case of an Enrolment) the same person whose reference image was enrolled.

iProov’s Dynamic technology is intended to detect different types of spoof attacks, including those using artefacts or images presented to the camera, synthetic videos or replayed imagery of previous Enrolment or Verification sessions injected into a device’s sensors. iProov’s ‘Flashmark’ method uses controlled illumination, with light generated by the device screen, to create a set of unique signals from the light patterns reflected from the End User’s face.

The End User is presented on the screen of their device with an abstracted rendering of the image of their face captured by their device’s front-facing camera. They are invited to align their face. The screen flashes a sequence of colours at a rate complying with international standards for the protection of photosensitive epilepsy (W3C WSAG 2.0 guideline 2.3). The sequence of colours that illuminate the End User’s face changes for each Dynamic Verification attempt of the same End User. This sequence is determined by a code generated on servers deployed by iProov and sent to the device before the Dynamic Verification attempt begins. The combination of the End User’s face and the unique illumination sequence creates a short video which is captured and sent to iProov during the scanning process. The information in the transmitted video is processed by iProov servers to determine the likelihood, as determined by iProov’s Dynamic technology, that the End User is genuinely present, and to provide a response based on this likelihood.

iProov's Dynamic technology relies on machine learning systems to improve iProov Products for anti-bias and anti-fraud purposes and is therefore subject to the necessity of continuous improvement on a per-product basis. It is accordingly an integral part of the delivery of iProov Products that End User data is used to train and test iProov's machine learning classifiers for these purposes on an ongoing basis, using authorised research methodologies. Improvements on a per-iProov Product basis will propagate generically across all iProov Products.

● iProov Enroller using Dynamic technology

The "**iProov Enroller**" is a service intended to enable Client to perform remote identity checks to support automated digital onboarding. A one-time face biometric scan is used to determine a likelihood that the End User is genuinely present during Enrolment, that the Dynamic Verification attempt is taking place in real-time, and if the user was enrolled by a Photo Enrol, that the End User matches a supplied reference image derived from a trusted source, such as a passport.

An End User is enrolled with a pseudonym chosen by Client. iProov Enroller APIs then create a second pseudonym (which is only ever accessible to iProov) to enrol the trusted End User using one of the methods set out below. iProov retains both pseudonyms in accordance with the Retention Schedule in Schedule 7 (Data Processing Agreement).

1. In the case of "**Capture Enrol**"
   a. Capture and transmission to iProov servers of imagery of the End User, by an SDK running on the End User device;

   b. Analysis of the received End User imagery by the Dynamic technology to determine a likelihood that the End User is a person genuinely present in front of the End User device at the time of transmission;

   c. Comparison of this likelihood with a risk profile, producing a result of pass or fail;

   d. Communication of this pass/fail result, together with other information, to the SDK running on the End User device, which shall provide it to the Combined Service running on the End User device;

   e. Receipt by iProov's servers of this pass/fail result, together with other information, including information identifying the Transaction, via an internet connection;

   f. Confirmation of the validity of the identified Transaction, together with other information, by means of an internet connection between iProov's servers and the Client's servers; and

   g. In the event of a Pass result, a biometric template may be created against the End User's pseudonym.

2. In the case of "**Photo Enrol**"
   a. The submission of a single image complying with the Minimum Requirements for size and quality of an image offered for Photo Enrol, by means of a connection between the Client's servers and iProov's servers;

   b. Confirmation by iProov of the successful enrolment of the image and the creation of a biometric template against the End User's pseudonym;

c. Subsequent request by Client to authenticate against the End User's pseudonym by means of a Verification entailing:
    i. Capture and transmission to iProov servers of imagery of the End User by an SDK running on the End User device;
    ii. Analysis of the received End User imagery to determine a likelihood that the End User is:
        1. the person (represented by a pseudonym) whose reference image was enrolled; AND
        2. a person present in front of the End User device at the time of transmission;

    iii. Comparison of these likelihoods with a risk profile, producing a result of pass or fail;

    iv. Communication of this pass/fail result, together with other information, to the SDK running on the End User device, which shall provide it to the Combined Service running on the End User device;

    v. Receipt from the Client's servers by iProov's servers of this pass/fail result, together with other information including information identifying the Transaction, via an internet connection; and

    vi. Confirmation of the validity of the identified Transaction, together with other information, by means of an internet connection between iProov's servers and the Client's servers.

iProov Face Verifier using Dynamic technology

The "**iProov Face Verifier**" is a service intended to authenticate a person's face against a pre-enrolled biometric template, and to determine that the person is a real person and is authenticating in real-time.

The iProov Face Verifier allows a request by the Client to authenticate an End User who previously successfully enrolled using Capture Enrol or Photo Enrol against their pseudonym. The following steps take place:

a. Capture and transmission to iProov servers of imagery of the End User, by an SDK running on the End User's device;

b. Analysis of the received End User imagery to determine a likelihood that the End User is:
    i. the person represented in the enrolled biometric template; AND
    ii. a person present in front of the End User device at the time of transmission;

c. Comparison of these likelihoods with one or more threshold levels, producing a result of pass or fail;

d. Communication of this pass/fail result, together with other information, to the SDK running on the End User device, which shall provide it to the Combined Service software running on the End User device;

e. Receipt from the Client's servers by iProov's servers of this pass/fail result, together with other information including information identifying the Transaction, via an internet connection; and

f. Confirmation of the validity of the identified Transaction, together with other information, by means of an internet connection between iProov's servers and the Client's servers.

Express (formerly LA):

iProov's Express technology is intended to provide a level of assurance that the End User present in front of (and using) a relevant device's camera is a real human being.

The End User is presented on the screen of their device with an abstracted rendering of the image of their face captured by their device's front-facing camera. Visual feedback is provided to the End User during the alignment process. As the End User aligns their face, a number of images are captured. These images, together with other information from the End User's device, are sent to the Platform where they are processed by a number of Platform subsystems which aim to establish whether the appearance of the face in front of the camera, the change in the appearance across the frames, and other data from the End User device, are or are not consistent with a bona fide End User. Unlike Dynamic, Express is not intended to determine whether the End User is genuinely present and authenticating in real-time.

iProov's Express technology relies on machine learning systems to improve iProov Products for anti-bias and anti-fraud purposes and is therefore subject to the necessity of continuous improvement on a per-product basis. It is accordingly an integral part of the delivery of iProov Products that End User data is used to train and tests iProov's machine learning classifiers for these purposes on an ongoing basis, using authorised research methodologies. Improvements on a per-iProov Product basis will propagate generically across all iProov Products.

- ## iProov Basic Enroller, using Express technology

The "**iProov Basic Enroller**" is a service which uses the Express technology and is intended to provide some assurance that the End User authenticating is a real person, and, if the End User was enrolled by a Photo Enrol, that the End User matches a supplied reference image derived from a trusted source, such as a passport.

An End User is enrolled with a pseudonym chosen by Client. iProov Basic Enroller APIs then create a second pseudonym (which is only ever accessible to iProov) to enrol the trusted End User using one of the methods set out below. iProov retains both pseudonyms in accordance with the Retention Schedule in Schedule 7 (Data Processing Agreement).

3. In the case of "**Capture Enrol**"
   a. Capture and transmission to iProov servers of imagery of the End User, by an SDK running on the End User device;

   b. Analysis of the received End User imagery to determine the likelihood that the End User is a bona fide person in front of the End User device at the time of transmission;

c. Comparison of this likelihood with a risk profile, producing a result of pass or fail;

d. Communication of this pass/fail result, together with other information, to the SDK running on the End User device, which shall provide it to the Combined Service running on the End User device;

e. Receipt by iProov's servers of this pass/fail result, together with other information, including information identifying the Transaction, via an internet connection;

f. Confirmation of the validity of the identified Transaction, together with other information, by means of an internet connection between iProov's servers and the Client's servers; and

g. In the event of a Pass result, a biometric template may be created against the End User's pseudonym.

4. In the case of "**Photo Enrol**"
   a. The submission of a single image complying with the Minimum Requirements for size and quality of an image offered for Photo Enrol, by means of a connection between the Client's servers and iProov's servers;

   b. Confirmation by iProov of the successful enrolment of the image and the creation of a biometric template against the End User's pseudonym;

   c. Subsequent request by Client to authenticate against the End User's pseudonym by means of a Verification entailing:
      i. Capture and transmission to iProov servers of imagery of the End User by an SDK running on the End User device;
      ii. Analysis of the received End User imagery to determine a likelihood that the End User is:
         1. the person (represented by a pseudonym) whose reference image was enrolled in the source ID photo; AND
         2. the bona fide person in front of the End User device at the time of transmission;

      iii. Comparison of these likelihoods with a risk profile, producing a result of pass or fail;

      iv. Communication of this pass/fail result, together with other information, to the SDK running on the End User device, which shall provide it to the Combined Service running on the End User device;

      v. Receipt from the Client's servers by iProov's servers of this pass/fail result, together with other information including information identifying the Transaction, via an internet connection; and

      vi. Confirmation of the validity of the identified Transaction, together with other information, by means of an internet connection between iProov's servers and the Client's servers.

● iProov Basic Face Verifier, using Express technology

The "**iProov Basic Face Verifier**" is a service which uses the Express technology and is intended to check the presence of the person and provide some assurance that the authenticating End User is a real person. Express use cases are most applicable in areas of lower threat or low risk.

The iProov Basic Face Verifier APIs allow a request by Client to authenticate an End User who previously successfully enrolled using Capture Enrol or Photo Enrol against their pseudonym. The following steps take place:

a. Capture and transmission to iProov servers of imagery of the End User, by an SDK running on the End User's device;

b. Analysis of the received End User imagery to determine a likelihood that the End User is:
   iii. the person whose facial image is represented in the enrolled biometric template; AND
   iv. the person present in front of the End User device at the time of transmission;

c. Comparison of these likelihoods with one or more threshold levels, producing a result of pass or fail;

d. Communication of this pass/fail result, together with other information, to the SDK running on the End User device, which shall provide it to the Combined Service software running on the End User device;

e. Receipt from the Client's servers by iProov's servers of this pass/fail result, together with other information including information identifying the Transaction, via an internet connection; and

f. Confirmation of the validity of the identified Transaction, together with other information, by means of an internet connection between iProov's servers and the Client's servers.

The following provisions apply to iProov Products:

An image of the End User captured by iProov will be provided by iProov in its response to the request by the Client for confirmation of the validity of the result.

iProov Products use automated technology in the endeavour to detect impersonation and spoofing attempts. Since the iProov Technologies used by iProov Products rely on a probabilistic automated decision-making system there can be no guarantee that all impersonations and spoofs will be detected. There is also a chance that genuine End Users may have Verification attempts refused.

Where mention is made in this document of: (a) "**iProov's servers**", these servers may be provided by contracted service providers, (b) "**pseudonyms**", these are pseudonyms specified by Client in respect of an End User, which are associated by iProov with a separate pseudonym randomly generated by iProov, and (c) "**risk profile**", this is a risk profile selected by the Client from a menu of such profiles provided by iProov during implementation of the iProov Technologies.

Interfaces / APIs

The iProov Products are delivered via interfaces/APIs as specified in the Documentation maintained in the directory of links at https://portal.iproov.com/help (requires log-in).

Open Source and Free Software

SDKs may include Open Source Software (as such term is defined by the Open Source Initiative) and/or Free Software (as such term is defined by the Free Software Foundation) which are specific to those SDKs. It is the responsibility of the Client to comply with the terms of the licences of such software, consent to which is deemed by use of the SDKs by Client or any persons or entities contracted directly or indirectly to Client. These licences are available for download and included with the relevant SDK. For the avoidance of doubt, the SDKs do not include any so-called “copyleft” licences.