



# G-Cloud 15 iProov Physical Access Solution Suite Service Definition

## Service Overview

**iProov Physical Access** is a biometrically enabled access control solution designed to help UK government departments and public sector organisations modernise their physical access security. It delivers robust, high-assurance authentication to streamline border crossings and secure sensitive facilities and critical assets, enhancing overall operational efficiency.

Its modular architecture supports **border management deployments across aviation, rail, and maritime ports of entry**, accelerating the processing of travellers and enhancing security. It enables faster identity checks for both pedestrian and vehicular traffic, reducing bottlenecks and improving frontline operational efficiency.

The same trusted biometric capability is extended to **government facilities, enabling seamless, secure entry for authorised personnel and ensuring only vetted employees have access to sensitive operational areas.**

iProov Physical Access can utilise **facial, fingerprint, and palm biometrics** to deliver fast and reliable access. Depending on the deployment, the system can capture and verify biometric traits during remote onboarding or pre-travel checks, as well as during on-site authentication. It also supports options such as **liveness detection** and **document matching** where required. These capabilities allow organisations to create a trusted digital identity for each traveller or employee, supporting secure and efficient access across a range of physical environments.

See the architecture example on the next page.

## User Journey

- 1. Remote Onboarding:** Individuals enrol by capturing their biometric(s) using a smartphone, tablet, or laptop. Alternatively, they can be enrolled by the organisation from a source database.  
**\*Available as a standalone service and combinable with Physical Access for onsite authentication.**
- Please refer to iProov Biometric Solution Suite - Service Definition for information about remote verification with liveness detection capabilities.**

2. **On-site Authentication:** Individuals are authenticated at the physical location with an image capture of their biometric, which is matched to their pre-enrolled biometric. Depending on the requirements, the software can be integrated with non-specialised and specialised hardware.



Figure 1: Architecture Example

## BORDER MANAGEMENT

Proven in high-traffic, high-security environments, **iProov Physical Access for Borders & Travel** streamlines **entry and exit border processing** with automated workflows that reduce the need for manual on-site checks. Powered by on-the-move biometric technology, it delivers a robust framework for accurate, real-time validation of traveller identities and smooth transit through checkpoints for both pedestrian and vehicular traffic.

With streamlined data handling and automated reporting, border officials can manage traveller flows more effectively, boosting operational efficiency while reducing wait times and minimising friction for travellers.

Travel operators and governments worldwide are adopting iProov to create secure, seamless travel experiences at scale. We've forged strong relationships with key border agencies, including the UK Home Office for Electronic Travel Authorization (ETA) scheme, the U.S. DHS CBP, and integrated into the Travel to Europe App with Frontex for the pilot of EES remote verification.

**The following examples showcase two real-world scenarios where iProov Physical Access is deployed to support border and travel operations:**

## 1. The iProov On-the-move Solution for EPP (Enhanced Passenger Processing)

### Pedestrian processing

It delivers a seamless, passenger-friendly transit at designated checkpoints. Developed to expedite entry for U.S. citizens arriving on international flights, it is trusted by U.S. Customs and Border Protection (CBP) and powered by iProov's on-the-move facial biometric screening, the same technology used in CBP's Seamless Border Entry (SBE) programme.



#### Real-time Identity Check

Facial biometrics supports the validation of passenger's identities in real-time by matching their faces to images in passports, held in the CBP Traveler Verification Service (TVS).



#### Seamless, Continuous Flow

Onsite devices capture passengers' faces on the move, enabling consistent processing in under 3 seconds compared to 30–60 seconds at booths.



#### Faster Border Crossings at Scale

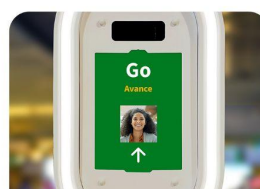
Full-scale implementation across multiple ports of entry, seamlessly integrated with CBP TVS.



STEP 1  
Arrival at U.S. Border



STEP 2  
Face Image Capture at Checkpoint



STEP 3  
Passenger Cleared if No Red Flags



STEP 4  
Seamless Entry into the U.S.

Figure 2: How it works, SBE/EPP deployments, major airports, USA.

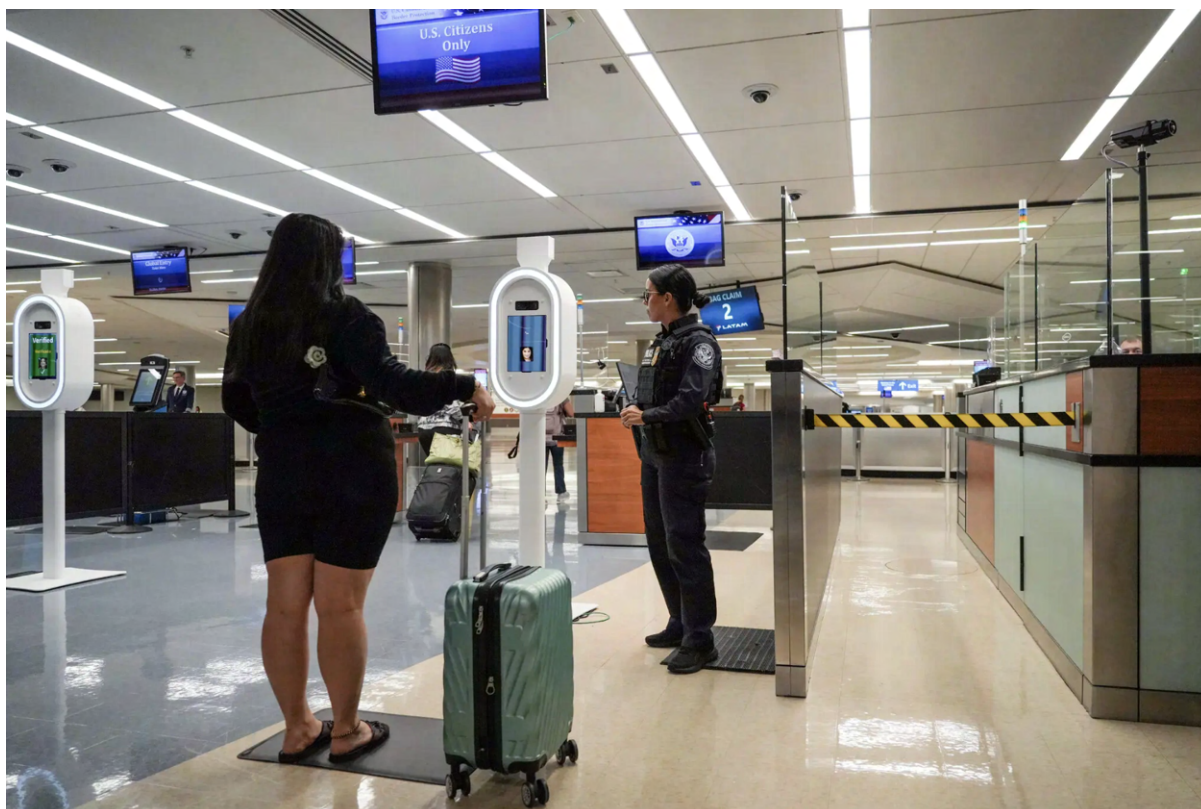


Figure 3: Biometric technology made by iProov and deployed at Orlando International Airport (MCO).  
The New York Times. (2025, December 8) [Link](#)

## 2. The iProov Solution for Land Vehicle Traveller Processing

### In-vehicle Processing

In the United Kingdom, iProov was selected and participated as one of four suppliers for the UK Home Office research and development environment trials between December 2024 and February 2025 to enhance security and efficiency at UK maritime ports. One of the most important goals of the trials was to help identify innovative solutions that could be considered for introduction in border control processes for people in vehicles.

iProov's solution used advanced facial biometric technology to capture high-quality facial images of people within stationary vehicles, and ensure the supporting software application successfully conveyed captured images to the border control for processing.



Figure 4: Concept image. Biometric technology made by iProov for deployment at UK Ports.

The **Land Vehicle Traveller Processing solution** uses a “capture session” to link all passengers to a single vehicle.

- Captures license plate images and occupant faces of all vehicle types – from passenger to goods vehicles.
- Image capture is triggered by the detection of a vehicle by the ANPR cameras, with the license plate being used as the vehicle identifier.
- Onsite pods capture and process high-quality face images of all travellers, with auto-prompts to lower windows.
- It leverages our existing technology powering SBE/EPP to provide user guidance, capture, and deployment.

## User Experience & Usability

Designed with travellers and border officials in mind, the user-centric experience features a **simple, intuitive Traveller Feedback System** that requires minimal interaction. Proven in UK Home Office trials and U.S. Customs and Border Protection (CBP) deployments, it delivers:

- **Significant reductions in processing times:** High-quality facial image capture and improved biometric matching reduce the need for manual document inspection.
- **Enhanced traveller engagement:** Travellers feel guided and involved throughout the process.
- **Optimised productivity:**
  - Frontline staff no longer need to adjust travellers’ posture, clothing, or face positioning.

- Focus shifts to higher-value tasks, supporting travellers who require more personalised attention.



*Figure 5: User Interface of the iProov On-the-move Solution used for Enhanced Passenger Processing (EPP) and Seamless Border Entry (SBE) in pedestrian use cases.*



*Figure 6: User Interface of iProov Solution for Land Vehicle Traveller Processing.*

## ACCESS TO FACILITIES

Access to government-owned and government-operated facilities, including workplaces for public-sector staff, prisons, and military bases, requires strict identity verification and authorisation controls. These environments manage access for employees, contractors, and

approved visitors, and demand high-assurance security measures to protect sensitive operations, assets, and personnel.

The **iProov Physical Access solution** enables government organisations to enforce stringent on-site access controls, reducing the risk of unauthorised entry and threats to the safety and integrity of personnel, infrastructure, classified material, and personal data.

Working with your existing access control system, the iProov Physical Access offers multiple onboarding options for seamless setup. Accessing a restricted area becomes as simple as a quick scan at the entry point, removing the need for access cards, keys, or manual document checks.

## Differentiated Features

### Remote Onboarding

1. **Biometric Capture:** Remotely capture face, palm, and fingerprint biometrics for authentication at physical locations.
2. **Liveness Detection:** Analyse the captured biometric with liveness detection for advanced mitigation of presentation and injection attacks.
3. **End-User Mobile Wallet :** Leverage Verifiable Credentials - an SDK integration with an existing mobile app or via a white-label version of the Partner wallet app, powered by iProov Identity.

### On-site Authentication

4. **Real-time Traveller Feedback System:** clear guidance for successful capture (multilingual and audio options).
5. **High quality Image Capture Rates:** 99% pedestrian, 95% vehicular. Performs consistently well across diverse lighting conditions.
6. **High-throughput:**
  - a. Pedestrians: 20+ passengers/line/min, <3 sec/passenger;
  - b. Vehicles: avg 150cars/hr | 20–25 sec/car
7. **Seamless Integration & Deployment:** Leverages existing IT infrastructure.
8. **Accessibility Conformance:** Accessible design supporting diverse users, mobility aids, and groups.
9. **Privacy by Design:** Consent-driven solution with mechanisms to protect privacy and minimise data sharing.
10. **Data Storage:** Enrolment data can be stored on the iProov server, by the organisation, or on the user's device to support a transition to verifiable credentials.

## Differentiated Benefits

1. **On-the-move biometrics** capture and process multiple faces simultaneously.
2. **Seamless, traveller-friendly transit** at high-security, high-traffic checkpoints: pedestrian and in-vehicle.
3. **Modular, hardware-light architecture:** supporting high-volume entry and exit points.
4. **Maximised efficiency:** faster traveller flow and scalable capacity without physical footprint expansion.
5. **Consistent, accessible performance** for families, groups, and mobility aids, in any lighting conditions.
6. **No-code enrolment:** Remotely enrol individuals via a Partner app for a no-code proof of concept (POC) and faster time to revenue.
7. **Multiple onboarding options for seamless setup.**
8. **Robust, low-risk delivery plan** that covers deployment and managed service.
9. **Easy maintenance with affordable upgrades** using readily available components.
10. **Full-service, local support** reduces risk, ensures smooth operations, and eases IT burden.

## Deployment

### Step 1: Onboarding / Enrolment – Optional Step

There are multiple ways an organisation can handle remote enrolment.

**a) Embedded experience on a website or app**

The enrolment process is embedded into a native app or website using our SDKs.

**b) Database enrolment**

The organisation can enrol users from a database of trusted imagery. As long as consent has been captured, this version of our solution doesn't require the user to do anything but show up onsite and authenticate with their biometric.

**c) Partner App**

End users download the app and upload their credentials, such as their ID document and a selfie. The data is verified in the cloud and a biometric profile is created for future authentication. This can be stored in the iProov server, by the organisation, or on the user's device. This enrolment method enables seamless integration with the organisation, making it ideal for POCs and those requiring speed to production.

### Step 2: Onsite Authentication

There are multiple ways an organisation can manage the onsite setup, depending on its operational and infrastructure requirements.

#### a) **Hardware integrated, configured, and delivered by iProov**

For use cases where fast processing in an attended environment is key, organisations can designate a “fast lane” where opted-in individuals simply pass through for authentication using their pre-enrolled biometric. iProov supplies hardware built from readily available, easy-to-maintain components, delivered with integrated software and managed services.

##### **Device type can include:**

- Standalone biometric capture device operating in a fully self-contained pedestrian mode
- Display screens for user guidance and feedback
- Water-resistant cameras designed for outdoor or in-vehicle installations

#### b) **Pre-existing Hardware**

Organisations with existing hardware, such as a gate or a turnstile, can integrate the software using the iProov SDKs.

We can provide a device-agnostic SDK designed for integration with your pre-existing hardware as a standalone option.

iProov Physical Access can supplement and work alongside your existing (e.g. card-based) access control system.

## **Verification Process**

iProov provides access to numerous biometric and identity verification technologies that can be combined to suit the organisation's needs.

### **1. Remote Onboarding – Optional Steps**

- a. Biometric Capture:** The user captures their chosen biometric(s) using their device camera.
  - i. Liveness:** Liveness detection analyses the device and imagery for spoofs presented to the camera, such as masks or videos, or injected into the system, such as deepfakes or face swaps.
  - ii. Biometric Match:** The (facial) biometric is matched to the ID document or a source database.
- b. Document Capture:** The user captures an image of their ID document.
  - i. OCR:** Data extraction via Optical Character Recognition (OCR).
  - ii. NFC:** Biometric identity documents (ePassports, biometric identity cards, and residence permits) are cryptographically validated using Near Field Communication (NFC) technology.

### **2. On-site Authentication - Optional Steps**

- a. Biometric Capture:** A new image of the biometric is captured at the entry point.

- i. **Biometric Match:** The biometric is matched to the pre-enrolled biometric.
- ii. **Liveness:** Liveness detection analyses the device and imagery for spoofs.

## Data Storage

### Biometric Profiles

When the individual enrolls in the service, a Biometric Profile (BP) is created. This contains an encrypted presentation of their biometric that is used for ongoing authentication.

There are various data storage options available with fully flexible data retention periods available.

For further details please refer to:

- **iProov Biometric Solution Suite - Service Definition**
- **iProov Decentralised Identity - Service Definition**

### On-site Devices

On the day of intended access, a one-way hashed Biometric Profile is sent to the onsite Physical Access device. The BP is stored in a temporary gallery of those requiring access within the timeframe defined by the organisation (eg: that day).

When the individual approaches the Physical Access device, a new image is captured and matched against the BP. The data can be instantly deleted or retained until access is no longer needed.

## Data Protection

iProov has extensive experience in hosting cloud security services in-country for our national-security-grade customers. iProov's technology, service, and operations are compliant by design with our obligations as a data processor under GDPR. There are detailed Data Processing Agreements with all of our customers.

## Certifications and Audits

### Company Certifications and Audits:

- Compliant with the requirements of the Cyber Essentials scheme.
- SOC 2 Type II, ISO 9001:2015, CSA Star Attestation Levels 1 & 2 (CCM v4)
- Certified to ISO/IEC 27001:2013 Information Security Management System
- Complies with GDPR (EU) 2016/679
- Complies with iRAP (Information Security Registered Assessor Program) and IP3 (Identity proofing level three) in Australia

**Face Liveness Certifications (applicable to product as appropriate):**

- iProov meets the biometric verification requirements of NIST SP 800-63-4 through independent ISO-accredited testing and supporting certifications for accessibility, data privacy, and cybersecurity.
- Independently evaluated to CEN/TS 18099 for injection attack detection by Ingenium Biometric Laboratories.
- Evaluated to meet iBeta PAD Level 1 and 2, and FIDO Face Verification Certification for presentation attack detection.
- Remote Onboarding: WCAG 2.2 AA (2.1 and 2.0 inclusive).
- Certified as a Component Service Provider and an Orchestration Service Provider under the UK Digital Identity Attributes Trust Framework (DIATF).
- Conforms with ISO/IEC 19795-1:2006 for testing biometric verification performance, audited by the UK National Physical Laboratory (NPL)
- eIDAS - conforms to EN 319-401 for Qualified Signatures, certified by independent auditors including TÜV & Ernst & Young for conformance to eIDAS Clause 24 1(d). Compliant with ETSI EN 319 401 and ETSI EN 319 411-1/2 to provide verification and authentication services as a Trust Service Provider to Qualified level for Modular Certification.

## Service Definition

The iProov Service consists of a hosted Software-as-a-Service (“SaaS”) platform (“Platform”), the capabilities of which can be consumed through the appropriate use of the defined API endpoints in conjunction with front-end SDKs. The specifications below describe the API endpoints available for the Service Provider to consume the iProov Service.

All up-to-date guides and directories of current API integration for the Platform and Front- end Software are available at <https://docs.iproov.com/>

## iProov Physical Access Service

The service consists of:

**Onboarding / Enrolment\**

1. A request to onboard a new User
2. The capture and transmission of Imagery of the User to iProov servers, by the iProov SDK and running on the User’s device
3. The analysis of the received User imagery to determine the likelihood that the User is:

- a. the right person e.g. user's face matches the document captured or relevant information as configured/specified
  - b. a bonafide user and not a spoof attempt
- AND;
- c. the person is genuinely present at the time of transmission
- 4. The comparison of points 3a, 3b, and 3c to produce a pass/fail result
- 5. The communication of this pass/fail result, together with other information, including an image of the User, to the Service Provider

#### **On-site Authentication:**

- 1. The User arrives at the physical location, where a new image is captured and matched to their pre-enrolled biometric.
- 2. The analysis of the received User imagery to determine the likelihood that the User is:
  - a. the right person e.g. User's face matches the document captured or relevant information as configured/specified
  - b. a bonafide user and not a spoof attempt
- AND;
- c. the person is genuinely present at the time of transmission
- 3. The comparison of points 2a, 2b, and 2c to produce a pass/fail result
- 4. The communication of this pass/fail result, together with other information, including an image of the User, to the Service Provider

## **Comprehensive Data Backup, Restore, and Disaster Recovery**

Each physical device is self-contained and comprises easily replaceable, readily-available electronic components. For a typical installation, we supply easily swappable spares that can ideally be replaced within 60 minutes or less.

Our backend systems are replicated across multiple regions and may, in future, span multiple clouds. Critical components may also run on-premise to minimise disruption if public or private cloud services fail.

Configuration is stored as code, and we have minimised the steps required to provision new devices, with the ability to manage them remotely if needed.

We take regular backups of our remote platforms and, again, store configuration as code using modern tools to enable rapid execution of disaster recovery processes.

In case of needing to recover a full service platform and associated network connectivity, we aim to complete the process in under 3 hours.

## Support

Support of the iProov service is provided 24/7 throughout the year. iProov has a dedicated support team for customers to raise tickets and request support.

All processes relating to key components within the iProov platform are monitored with severity levels that trigger automatic alerts. Within the regional platform, processes are resilient with recovery automated for internal components.

Customers have three main mechanisms for reporting issues. If the customer is enrolled with iProov, “iPortal” tickets can be raised and tracked directly. iPortal is an online dashboard that enables organisations to manage their service and view results, reports, and performance. Customers may also raise tickets by email or by phone call. All of these methods result in the creation of a prioritised ticket in the iProov support platform.

Engineers will respond to tickets according to their severity and customers will be informed of actions and progress. For customers not using “iPortal”, the ticket updates will arrive through email.

## Service Parameters

iProov’s platform infrastructure has been designed to minimise maintenance downtime. In the rare event that downtime is required, this is notified to the customer with maximum advance notice and completed out of hours for the individual region.

## Technical Requirements

The minimum technical requirements are available on <https://docs.iproov.com/>.

## Outage and Maintenance Management

Maintenance of the platform is an ongoing process covered by a dedicated, in-house technical operations team. Tasks are identified, ticketed, executed, and reported as part of our standard operating procedures.

Automated tools monitor any outages and service downtime 24/7. Upon detection, the technical and operations teams are alerted. All alerts are dealt with immediately by on-call personnel with automatic escalation if not acknowledged within 5 minutes of receipt. This ensures contingency for on-call staff.

In the case of a Major Incident, the iProov MI process will be invoked. This process has provisions for engagement across the company with Commercial, Technical, and Senior Management coordination to ensure rapid communication and management of the issue.

## Hosting Options and Locations

iProov operates exclusively through cloud providers with a focus on Google Cloud Platform. Due to Data Governance regulations, and customer requirements, services will be hosted within the jurisdiction for the applicable data protection legislation for that region. The result of this is that iProov has platforms across the globe with data retention specific to the region.

iProov is planning to develop customised deployments of our service which can be deployed within customer premises. This is an early-day project but will eventually lead to multi-deployment options.