



G-Cloud 15 iProov Biometric Solution Suite: Remote Facial, Fingerprint, Palm Verification and Authentication with Liveness Detection

Service Overview

The iProov Biometric Solution Suite is a cloud-hosted service for remote identity verification using facial, fingerprint, and palm biometrics. It supports biometric capture, matching, and liveness detection, combined with document and database verification. These capabilities enable secure remote onboarding and authentication, allowing citizens to access government services via smartphones, web applications, or kiosks with high usability and unwavering security.

iProov specialises in advanced liveness detection to protect against presentation attacks, injection attacks, and deepfake-based fraud. This capability is strengthened by the iProov Security Operations Centre (iSOC), which continuously monitors, detects, and responds to emerging threats, delivering rapid and ongoing algorithmic updates.

iProov supports flexible deployment models, offering standalone SDKs or a complete end-to-end platform. The platform also enables a transition to decentralised identity models through verifiable credentials, which can be issued directly to citizens' smartphones for privacy-preserving data storage and multi-factor authentication.

iProov has been recognised as a 'Leader' in the KuppingerCole Compass for Identity Verification and included in the Gartner Innovation Insight for Biometric Authentication. iProov serves some of the world's most security-conscious organisations, including the Australian Taxation Office, GovTech Singapore, UBS, the UK Home Office, and the US Department of Homeland Security.

Core Components

Facial Verification

iProov offers two facial verification experiences with distinct liveness detection technologies designed for different risk profiles.

Express Liveness® provides fast verification for standard risk scenarios. Users simply align their face within an on-screen oval for near-instant multi-frame capture. The system analyses proprietary signals from the user, device, and imagery to detect presentation, injection, and deepfake attacks.

Dynamic Liveness® delivers mission-critical protection for high-risk scenarios. During capture, the device screen is illuminated with Flashmark® technology. The light reflection on the user's face is verified to confirm the user is authenticating in real time. Unlike active challenge responses, like a head turn, this passive challenge requires no action from the user and delivers high performance regardless of physical or cognitive capability. Dynamic Liveness delivers the highest level of protection against presentation, injection, and deepfake attacks.



iProov Dynamic Liveness UX: Multi-frame capture with passive challenge response via Flashmark

iProov Express Liveness UX: Multi-frame capture

Fingerprint Verification

iProov enables the remote, contactless capture of fingerprints using non-specialized devices with a rear-facing camera, such as a smartphone or tablet. This eliminates the need for individuals to visit physical locations for in-person fingerprint checks, expanding the reach of government services and removing administrative and logistical burdens.

Individuals simply align their hands in the designated positions shown on the screen to capture their four fingers and their thumb. The images are instantly analysed with multi-frame liveness technology for signs of spoofs presented to the camera, such as photos, finger moulds, or artificial fingertips. Images of the captured prints are returned to the relying party and optionally verified against a source database.



Palm Verification

iProov enables the remote, contactless capture of a person's palm using non-specialized devices with a rear-facing camera, such as a smartphone or tablet, or a computer device with a camera. Individuals can remotely enrol by capturing their palm and can then enjoy fast, contactless authentication for logical and physical access to services on any device.

The user is instructed to capture their palm using the device's rear-facing camera. Visual, on-screen cues assist in the correct alignment of their palm. The imagery is analysed with advanced multi-frame liveness detection technology to detect spoofs, such as a photo or an artificial palm presented to the camera. An image of the captured palm can be returned to the relying party if required.



Document Verification

Document Capture & OCR: Fast, reliable document capture with Optical Character Recognition (OCR) extracts data from thousands of government-issued IDs, including passports, national ID cards, and driving licences. The service accurately captures personal data and Machine Readable Zone (MRZ) information, streamlining data entry and improving user experience.

NFC-Based Document Verification: Fully automated verification of NFC-enabled identity documents such as ePassports, national eIDs, and residence permits. Users simply tap their document on a smartphone to securely extract and cryptographically validate chip data in real time. Embedded biometric data (e.g. facial images or fingerprints) can be matched against live capture to detect forgery or manipulation.

Document Liveness: For documents without electronic chips, automated liveness checks verify authenticity, with optional manual review for added assurance. Using advanced machine learning, the service analyses document security features, images, MRZs, and barcodes to detect tampering, forgery, and expired or invalid documents.

Database Integration: iProov integrates seamlessly with government-owned and trusted third-party databases to validate identity data, delivering a high level of assurance and a robust, end-to-end identity verification solution.



OCR Document Capture



NFC Verification

Cybersecurity Service

The solution is underpinned by the iProov Security Operations Centre (iSOC), an intelligence-led cybersecurity capability that protects customers against rapidly evolving threats. iSOC unifies world-class scientists, threat intelligence analysts, and ethical hackers in a continuous security loop: the team discovers new threats, validates them in controlled environments, and deploys defences to production before customers are impacted.

Proactive Threat Intelligence

iSOC continuously researches emerging attack vectors and translates findings into algorithmic updates for the core AI system. The Threat Intelligence Team tracks sophisticated adversaries, analyses their tools and tactics, and converts real-world signals into actionable defences. These insights feed directly to science teams, enabling rapid, data-driven platform hardening that protects customers ahead of new attack waves.

Reactive Defense & Rapid Response

iSOC provides real-time monitoring, detection, and response capabilities. Suspicious activity is detected quickly, investigated by specialist analysts, and neutralised through seamless cloud updates that strengthen customer deployments without service disruption or impact to end-user experience.

Core Services:

- **Ongoing monitoring:** Machine learning models continuously analyze production traffic to identify attack patterns, such as similar images submitted in rapid succession across multiple attempts
- **Incident response:** Suspicious events are triaged by the Threat Intelligence Team, who block repeat threat actors and implement new mitigations to reduce future risk
- **Threat hunting:** Experts proactively search for hidden or emerging vulnerabilities, applying expertise and creative techniques to uncover scenarios that evade standard controls
- **Red teaming:** Ethical hackers simulate sophisticated adversary techniques to identify and remediate security gaps before they can be exploited
- **Threat intelligence:** Analysts monitor underground channels and adversarial communities to track evolving tools, techniques, and procedures (TTPs), ensuring the platform anticipates real-world attacks

This integrated approach ensures iProov biometric systems remain resilient, continuously updated, and prepared for next-generation threats.

Integration & Deployment

The cloud-based service is consumed via SDKs for Web, iOS, and Android, or hosted web journeys via OpenID Connect (OIDC).

Algorithmic updates are deployed automatically to the cloud with no customer action or specialised expertise required.

Complete integration documentation and API specifications are maintained at <https://docs.iproov.com/>.

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

Facial Biometrics Technology Certifications (applicable 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.
- Conforms with ISO 19795 and ISO 30107 standards for biometric testing.
- Conforms to Web Content Accessibility Guidelines (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
- US DHS commissioned extensive testing by an external Red Team. Advanced techniques were employed to spoof the system, yet iProov effectively blocked them. "The iProov authentication process was robust against digital impersonation techniques."

- Verified by the UK, Singapore, and Australian Governments as part of their National Due Diligence.

Company Certifications and Audits:

- Compliant with the requirements of the Cyber Essentials scheme.
- SOC 2 Type II, ISO 9001, CSA Star Attestation
- 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.

Reference Customers

- **NHS** - as part of the NHS App; iProov provides strong face biometric verification to onboard citizens in the UK to the NHS digital mobile app. Using the iProov solution, citizens are able to register for the NHS App using a web SDK and are then able to verify themselves in real time with the image on their national ID document.
- **The Home Office** - the EU Settled Status scheme utilised iProov to assure the genuine presence of remote users and verified that the applicant was the rightful holder of the validated ID document. Over 5 million EU citizens have successfully used the service to apply for permanent residency status. It facilitated a safe, secure, and convenient process with over 85% of applicants utilising the digital channel.
- **Government Digital Service (GDS)** - GDS improved access to government services with GOV.UK One Login Programme, replacing the inefficient legacy system - GovDoc Verify. This new federated identity scheme utilises iProov's Remote Onboarding Solution, featuring Dynamic Liveness, NFC, and OCR capabilities, and hybrid check options. It simplifies and streamlines online access for over 11 million users, enabling inclusion, safeguarding citizens, and potentially saving £700 million over three years.
- **Generic Identity Verification Service (GIDV)** - the UK Home Office awarded iProov partner Entrust a two-year contract to provide a biometric immigration solution. The GIDV solution consists of document verification, facial biometric enrollment using Dynamic and Express Liveness, identity capture, and professional services. It supports the UK Electronic Travel Authorisation (ETA) scheme, facilitating travel for 30-40 million non-UK citizens annually for purposes such as tourism, transit, business visits, and short-term study. The GIDV solution aligns with the UK's broader digitalisation agenda, enhancing accessibility, convenience, and inclusivity in service provision.

Data Backup, Restore, and Disaster Recovery

iProov services are hosted on enterprise cloud platforms, which are available in all operating regions in the world. The platforms have two distinct elements: Database services and Compute services.

- iProov uses secure databases to store a small set of artefacts which are required for iProov to provide the service. These databases are regional, with resilience sets in a separate, but similar data centre, each with a scheduled backup which runs in minimum two hour intervals. This ensures data recovery within standard operating process times and ensures coverage and recoverability against potential outages.
- Database restoration mechanisms are tested at least annually in production conditions. The process is adapted within iProov's own test environments.
- Compute services are augmented with other standard platform security and functions to enable customer access and associated transactional functionality.
- Restoration of the Compute platform is carried out through an automated platform build process which is used to reinstate the Compute services and associated configuration, both peripheral and core.
- In the case of Database Recovery, iProov will first restore the compute platform then attach the databases. Once this has completed, a database snapshot is used to reinstate the platform to pre-outage operation.

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. There are exceptions for fraudulent attempts to breach the service, data for a non-genuine actor can be retrieved and analysed by specialist teams working from the UK.

iProov is looking 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, including Crown-Hosting.