iProov

G-Cloud 15 iProov Workforce Solution Suite Service Definition

Service Overview

The iProov Workforce Solution Suite is a cloud-based biometric service that enables organisations to reduce their exposure to AI-based identity threats and streamline operational access. The service delivers secure biometric verification and authentication across critical workforce processes, such as remote hiring and onboarding, account recovery, and authentication, including passwordless, multi-factor, and step-up use cases.

At the core of the service is iProov's advanced liveness detection technology, which delivers robust protection against presentation attacks, injection attacks, and AI-generated deepfakes. This technology is continuously monitored and updated by the iProov Security Operations Centre (iSOC), ensuring customers are protected as new attack techniques emerge globally - without requiring configuration changes or operational effort.

The service integrates seamlessly with existing identity and access management infrastructure, including all major IAM platforms, Microsoft Entra ID, and Windows Login. It can be deployed rapidly using OIDC-hosted journeys or native SDKs, allowing organisations to strengthen identity assurance without replacing existing systems.

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.

Technologies & Assurance Levels

Different workforce interactions carry different levels of identity risk. iProov provides the appropriate level of identity assurance for each interaction, balancing strong security with seamless user experiences conformant to Web Content Accessibility Guidelines (WCAG) 2.2 Level AA and the European Accessibility Act (EAA).

iProov Express Liveness®

iProov Express Liveness delivers fast, low-friction facial verification for standard-risk workforce scenarios. Users simply align their face within an on-screen oval for near-instant capture. The system analyses proprietary signals from the user, device, and imagery to detect presentation attacks, injection attacks, and AI-generated deepfakes

This approach enables rapid authentication for everyday access events while maintaining strong protection against common identity threats.

iProov Dynamic Liveness®

iProov Dynamic Liveness provides the highest level of biometric assurance for high-risk or sensitive workforce interactions. During capture, the device screen illuminates the user's face using iProov's patented Flashmark® technology. The unique light reflections are analysed to confirm the user is authenticating in real time.

Unlike active challenge-response methods, Dynamic Liveness is passive and accessible, requiring no specific movement or instruction from the user. This makes it suitable for diverse workforce populations while delivering robust protection against advanced presentation, injection, and deepfake attacks.

Workforce Identity Capabilities

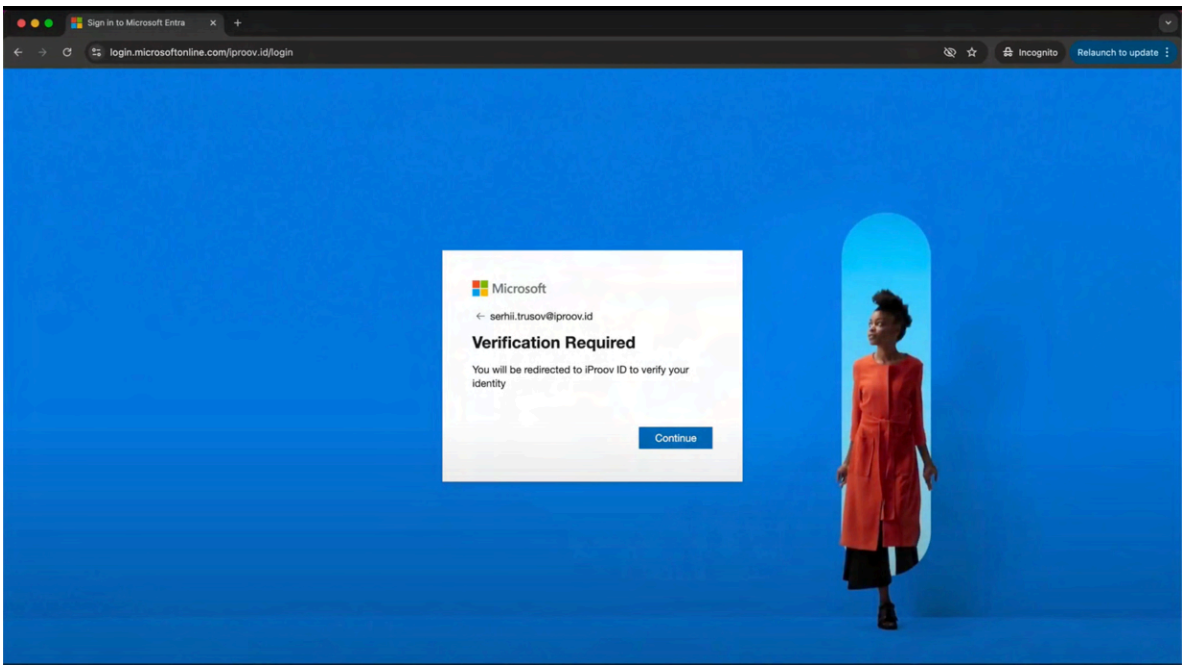
iProov Workforce Onboarding

iProov Workforce Onboarding enables organisations to remotely onboard employees and non-employees securely from anywhere in the world. New hires verify their identity using a government-issued identity document and a matching selfie, providing high assurance without requiring in-person checks or office visits.

This reduces onboarding delays, prevents impersonation and hiring fraud, and enables new workers to be productive from day one.

iProov Biometric MFA

iProov Biometric MFA provides phishing-resistant facial authentication as a second factor for OIDC-compliant web browsers and applications. It enables organisations to replace one-time passcodes and authenticator apps with a seamless biometric experience, mitigating social engineering and credential compromise while removing friction.



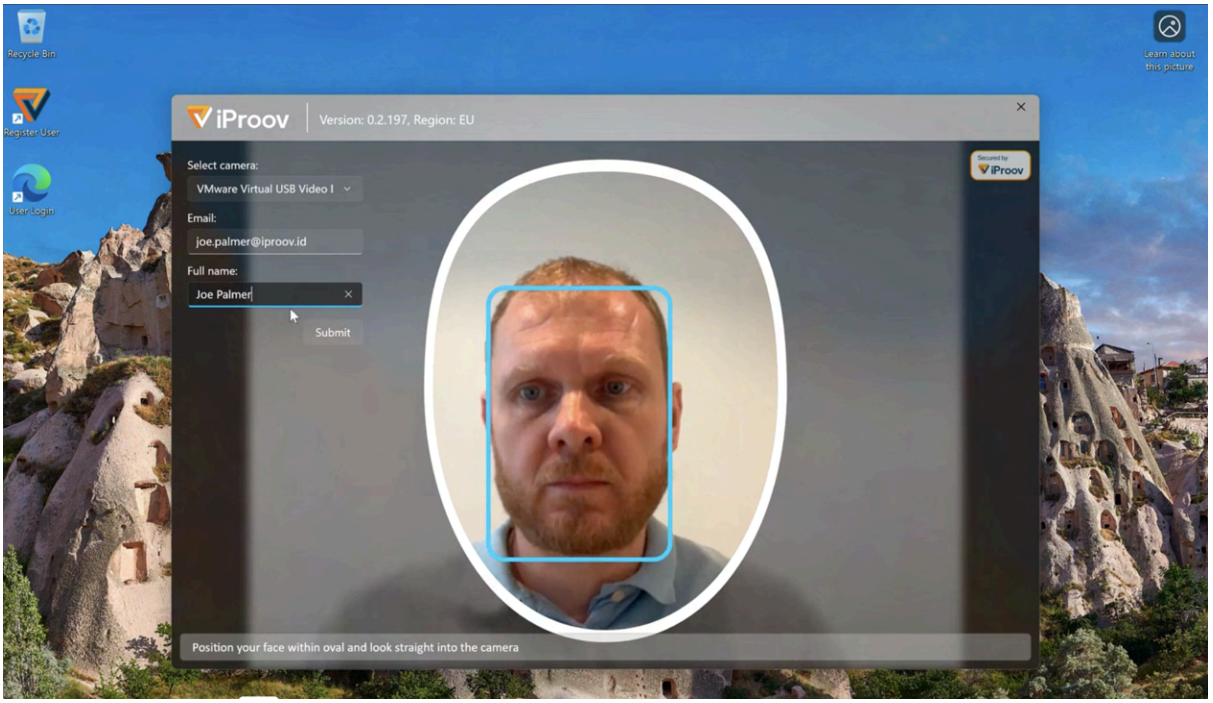
iProov Shared Device Authentication

iProov Shared Device Authentication enables frontline workers to access shared devices quickly and securely using their facial biometrics. Workers can sign in to Windows Login and Microsoft Entra ID without usernames or passwords, eliminating shared credentials and speeding up frontline operations. Certificates are also issued to the device for secure two-factor authentication.

Every authentication is verified to a real individual, improving accountability, supporting audit requirements, and reducing the risk associated with shared accounts across registers, kiosks, terminals, and other communal devices.

iProov Passwordless Windows Login

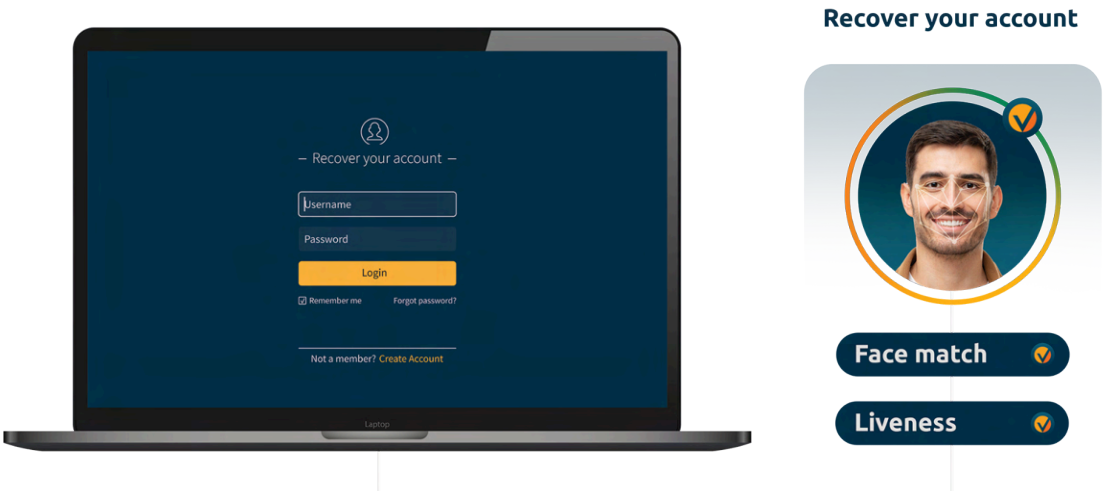
iProov Passwordless Windows Login enables organisations to remove passwords from Windows sign-in and let employees log in with their face. iProov combines facial verification with hardware-backed private keys to deliver strong two-factor authentication, improving security while making access effortless.



iProov Biometric Account Recovery

iProov Biometric Account Recovery enables workers to securely regain access to their accounts without contacting the help desk. Identity-verified facial biometrics provide high assurance while delivering a simple, device-independent recovery experience.

This capability reduces downtime, lowers support costs, and ensures secure recovery even when devices are lost, replaced, or unavailable.

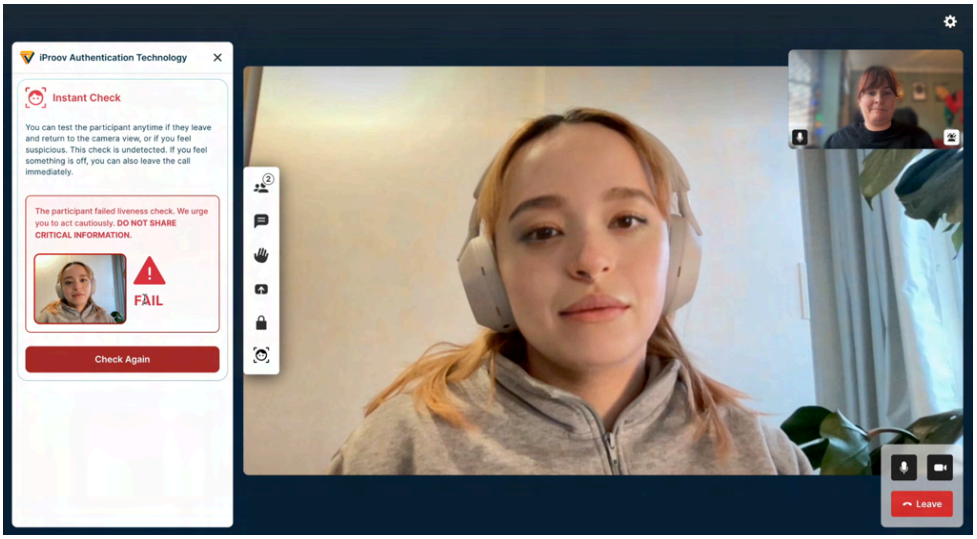


iProov Verified Meetings™

iProov Verified Meetings provides real-time deepfake detection for video conferencing, enabling organisations to strengthen trust and security in remote meetings. The service analyses live video sessions to confirm that participants are real and genuinely present during remote meetings, and not a deepfake, injection, or presentation attack. The check can be performed before the person is admitted to the meeting and then within the meeting, as determined by the host.

This protects organisations from deepfake-enabled impersonation and insider threats, such as CEO fraud, hiring fake workers, or giving malicious actors access to corporate information.

For more information, please see the **iProov Verified Meetings listing.**



iProov Physical Access

iProov Physical Access enables secure, seamless entry to restricted buildings without the need for cards, keys, or manual document checks. Users remotely enrol their facial or palm biometrics, which are verified against trusted identity credentials, and gain frictionless access to buildings, sites, and restricted areas. This replaces or works alongside existing physical access control solutions.

This helps organisations reduce access friction for employees and non-employees, improve operational efficiency, and maintain strong security controls across physical environments.

For more information, please refer to the **iProov Physical Access Solution Suite service listing.**

Cybersecurity Service

The service 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 Defence & 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 analyse 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 solution is consumed via native SDKs for Web, iOS, Android, and Windows Credential Provider, or hosted web journeys via OIDC.

Algorithmic updates are deployed automatically via 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 Biometric Technology Certifications (certification/audit profile as appropriate to relevant products):

- 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.
- 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.
- 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:

- iProov is compliant with the requirements of the Cyber Essentials scheme.
- iProov is compliant with SOC 2 Type II.
- iProov is certified under ISO 9001:2015.
- iProov is listed on the CSA STAR Registry at Level 1 (Self-Assessment) and Level 2 (Third-Party Certification).
- iProov is certified to ISO/IEC 27001:2013 Information Security Management System
- iProov complies with GDPR (EU) 2016/679
- iProov complies with iRAP (Information Security Registered Assessor Program) and IP3 (Identity Proofing Level Three) in Australia.

Data Backup, Restore, and Disaster Recovery

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

- iProov uses secure databases to store a small set of artifacts that 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 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.