G-Cloud 15 iProov Verified Meetings™ Service Definition

Service Overview

iProov Verified Meetings is a module available for integration into leading video conferencing platforms. The technology is a cloud-hosted service that confirms whether remote individuals are real and genuinely present before and on demand during video conferencing calls. Built for security and usability, the solution protects against deepfake, injection, and presentation attacks.

iProov Verified Meetings is designed to continuously detect emerging threats and deliver real-time algorithmic updates using integrated cybersecurity service capabilities.

Core Technologies

iProov Verified Meetings includes two liveness technologies that can be evoked based on the risk level of the meeting, participants, and contextual signals:

Dynamic Liveness: Dynamic Liveness delivers mission-critical protection for high-risk scenarios. During capture, the device screen is illuminated with patented 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 pass rates regardless of physical or cognitive capability.

In-meeting liveness technology: During the call, the system discreetly captures and analyses multiple video frames to confirm that a participant is a real person, not a deepfake, presentation attack, or other spoof.

Use cases

Dynamic Liveness and in-meeting liveness can be used as follows:

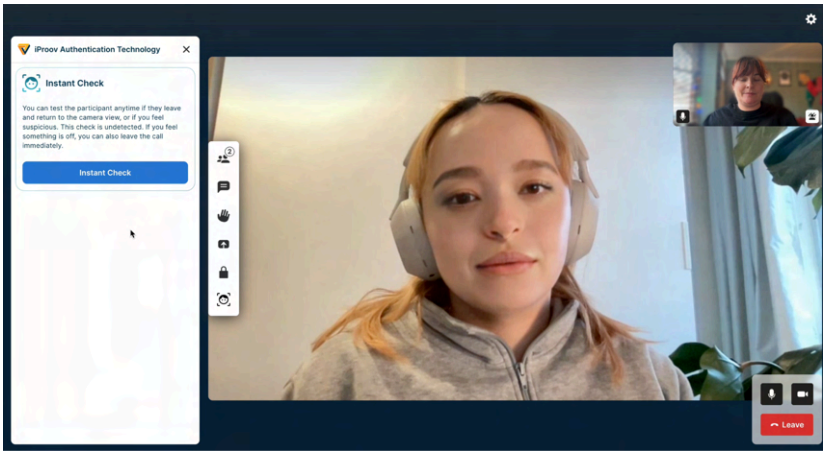
Before entry: For meetings with elevated risk (e.g., HMRC interviews under caution), hosts can request participants perform an iProov Dynamic Liveness check before entering the call.

During the call: In-meeting liveness detection allows hosts to discreetly verify participants during a live video session.

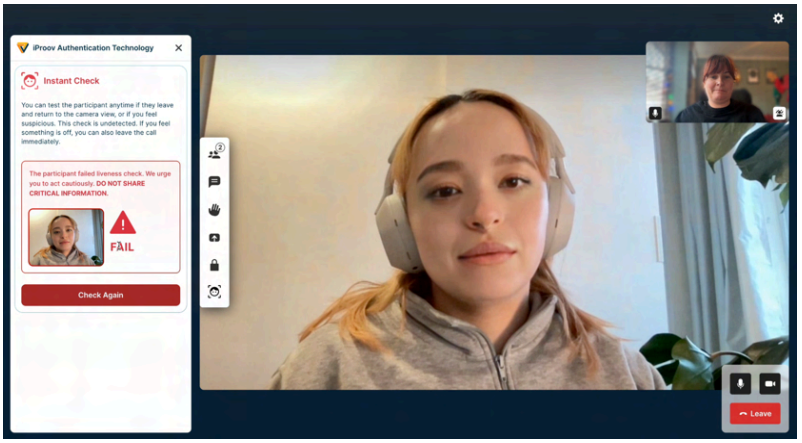
- The host can activate liveness checks throughout the call.

- Participants are not notified when a check is performed.
- When the system detects a spoof, the host is immediately notified and can decide whether to continue or terminate the session.

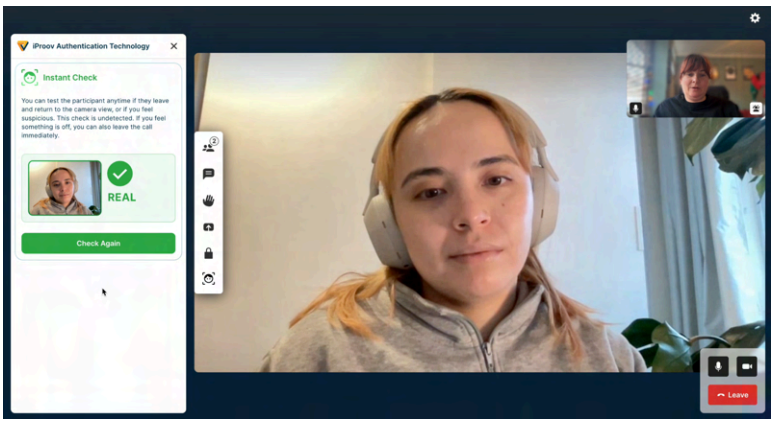
Step-up: If the host determines that additional assurance is needed, they can request the participant to perform a Dynamic Liveness check.



Host initiates a liveness check



Liveness technology detects a spoof.
The host is notified and cautioned.



In a separate scenario, liveness technology confirms the user is real.

User Experience & Accessibility

Dynamic Liveness is certified to meet Web Content Accessibility Guidelines (WCAG) 2.2 Level AA and Section 508 standards. It operates on most devices equipped with front-facing cameras, supporting over 21,000 device models globally.

Users complete verification with guided real-time feedback that enables optimal image capture on the first attempt. Auto-capture technology detects the optimal moment to begin the process, minimising user error and friction, whilst maximising first-time pass rates. The Flashmark illumination technology has been tested to conform with W3C WCAG 2.2 Level AA SC 2.3.1, ensuring safe operation for users with photosensitive epilepsy.

User Scenarios

Organisations can use iProov Verified Meetings across remote meetings and interviews. Examples of interactions that require elevated security include:

Remote government-to-citizen meetings: Government officials increasingly conduct remote video calls with citizens for high-stakes interactions such as tax interviews and Universal Credit eligibility checks. Deepfakes now evade human detection capabilities, allowing bad actors to impersonate legitimate individuals or use synthetic identities to infiltrate these meetings, creating a growing fraud surface with material financial and operational consequences.

Using real-time liveness detection, iProov Verified Meetings enables officials to identify spoofed participants and terminate potentially fraudulent interactions before harm occurs.

Remote job interviews: Remote hiring without in-person verification enables bad actors to spoof interviews with deepfake technology to obtain employment under false identities. These roles can be used to access internal systems or divert salaries to organised fraud or nation-state operations. North Korea's remote IT worker scheme alone is estimated to generate $250–600 million per year in employment fraud.

iProov Verified Meetings confirms human presence and detects deepfakes during remote interviews before candidates are granted employment, credentials, or system access.

Integration & Deployment

The cloud-based solution is available as a web integration into video conferencing platforms.

Changes to the user interface are released via plug-in updates. Algorithmic security 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/.

Cybersecurity Service

iProov Verified Meetings is underpinned by the iProov Security Operations Centre (iSOC), an intelligence-led cybersecurity capability that protects customers against rapidly evolving threats. iSOC unifies cybersecurity technology with 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.

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

Technology Certifications (applicable as relevant to product component):

- 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.
- WCAG 2.2 AA (2.1 and 2.0 inclusive)
- 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.

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 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 that 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 been 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 (MI), 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.