Polyguard System Documentation

Version 1.0.11

Table of Contents

Executive Summary

The modern hiring process is under siege. What once relied on in-person interactions and trusted referrals has evolved into a high-velocity, remote-first system — and with that shift has come a surge in deception. “Job fraud” has emerged as a systemic threat, where candidates misrepresent their identity, outsource interviews to third parties, or leverage AI tools to convincingly impersonate qualified professionals. Interview-as-a-Service platforms and malicious impersonation techniques are now widespread, blurring the lines between legitimate applicants and synthetic fraudsters.

For staffing firms and recruiters, the cost isn’t just reputational — it’s operational and financial. Time is wasted vetting candidates who don’t exist, interviewers are misled, client trust is eroded, and in too many cases, impersonators make it through to placement — triggering contractual penalties, regulatory headaches, and the loss of critical business relationships. These errors aren’t just human; they’re systemic, exacerbated by brittle verification workflows and an overreliance on screenshots, spreadsheets, and good faith.

Beneath the surface lies a quieter crisis: the normalization of unsafe behaviors. Candidates are routinely asked to share sensitive personal data through insecure channels, often with minimal verification or safeguards. This not only creates risk for the recruiter and the employer — it sets up jobseekers to become victims of fraud themselves. In the rush to screen faster, we’re training users to trust blindly — and in doing so, we’ve opened a new front in the battle for digital identity.

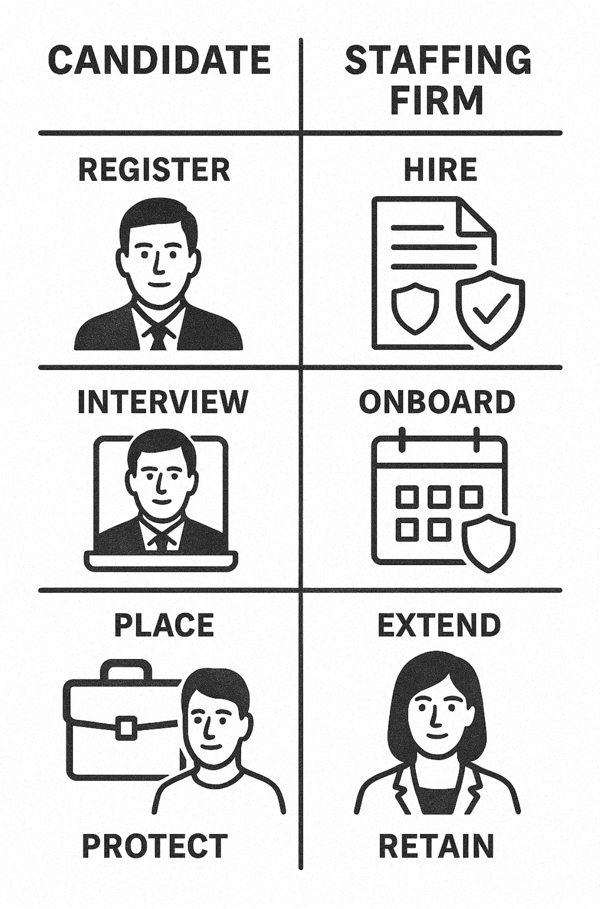
Solution: Continuous Mobile Identity Verification

Polyguard solves this growing crisis with a simple but powerful idea: **trust must travel with the candidate**.

By leveraging the secure enclaves and biometric sensors already embedded in modern smartphones, Polyguard enables **continuous mobile identity verification** — verifying who someone is once, safely and thoroughly, and then **brokering that verified identity** across the hiring process. No more reinventing trust for every call, every screen share, every document.

The Polyguard System pairs tamperproof mobile clients with advanced AI-driven biometric and document analysis, anchored by cryptographic proof. Once verified, candidates can seamlessly join interviews, submit credentials, and engage with recruiters — all while maintaining a persistent, high-confidence identity state. And because Polyguard’s trust layer extends **beyond the hiring process**, verified individuals can continue using the platform **throughout their employment**, enabling secure onboarding, compliance check-ins, and ongoing access to sensitive systems — without sacrificing privacy or introducing friction. The result is a faster, safer, and more respectful experience for everyone involved: less fraud, less friction, and dramatically higher trust.

Target Use Cases and Users



Polyguard Secure Meetings is designed for organizations that operate in **high-trust, high-risk hiring environments** — where the cost of impersonation, fraud, or compliance failure is significant.

Primary Users:

- **Recruiters & Talent Acquisition Teams**
  Prevent synthetic candidates from advancing through the funnel, while streamlining identity verification at scale.

- **IT & Security Leaders**
  Integrate verified identities into broader compliance and access control frameworks, especially in regulated or sensitive industries.

- **Consultants and Employees**
  Avoid hassle and protect your privacy while meeting workplace requirements, by sharing secure Polyguard tokens instead of raw ID documents.

Core Use Cases:

- **Remote Interview Verification**
  Authenticate candidates before and during video interviews using live biometric and document validation.

- **Staffing Partner Assurance**
  Offer clients verifiable proof of identity for all placed candidates, reducing liability and building trust.

- **Ongoing Identity Proofing for Remote Workers**
  Extend verification beyond background checks — to onboarding, compliance check-ins, and access control for remote or contract workers.

Whether you're screening thousands of applicants or staffing critical roles on short notice, Polyguard provides the **invisible infrastructure of trust** needed to move faster, without sacrificing security.

Key Benefits of the Polyguard Approach

- **Stop Fraud Before It Starts**
  Detect and block impersonators *before* they enter your hiring pipeline — not after the damage is done.

- **Verify Once, Trust Everywhere**
  Eliminate repetitive, error-prone identity checks with persistent, cryptographically anchored trust.

- **Faster, Safer Hiring**
  Accelerate screening and placement without sacrificing security, accuracy, or candidate experience.

- **Enterprise-Grade Privacy & Compliance**
  Meet SOC 2, GDPR, and FCRA standards with end-to-end encryption, audit trails, and data minimization.

- **Restore Confidence with Clients**
  Offer verifiable proof that every candidate is who they claim to be — and keep it that way through their employment.

- **Designed for the Real World**
  Mobile-first, recruiter-friendly, and built to scale across thousands of candidates and interviews.

Key Differentiators

Polyguard is the only solution designed from the ground up for **real-time, recruiter-driven identity verification** — before, during, and after interviews — with an infrastructure-level approach to trust that goes far beyond a one-time ID check. We bring cryptographically-secure proofs to bear within existing workflows (video interviews, phone calls and remote logins), where they save time and increase the trust of all parties.

Capability	Polyguard	Competitors
In-Meeting Verification	✅ (Zoom & Teams app integration)	❌
Continuous Identity Proofing	✅ (Reusable across lifecycle)	❌ (One-time only)

Trust Protocol (cryptographic)	✅ (Tamper-proof device + biometric)	⚠️ (Limited or missing)
Recruiter & Admin Tools	✅ (Admin dashboard + mobile UX)	⚠️ (Often developer-focused APIs)
White-Label + Workflow Control	✅ (OAuth, branding, alerting)	⚠️ (Limited or missing)
Mobile-First + Human-Centric	✅ (Built for candidates & recruiters)	⚠️ (Built for banks or apps)
Post-Hire Use Cases Supported	✅ (Onboarding, compliance)	❌ (Pre-hire only)

Modern Pricing Model

Polyguard's standard pricing is centered around a straightforward **monthly per-seat model**, ideal for recruiters, staffing teams, and hiring managers who need continuous access to secure identity verification.

Each active recruiter seat includes:

- Unlimited secure meeting creation
- Full access to the admin dashboard and invite workflows
- Real-time identity verification and audit trail access

For organizations with variable hiring volumes, we also offer **usage-based bundles**, priced per verified candidate or meeting — a flexible option for seasonal demand, distributed teams, or pilot deployments.

For larger teams or long-term partnerships, we provide **custom Enterprise agreements**, which can include:

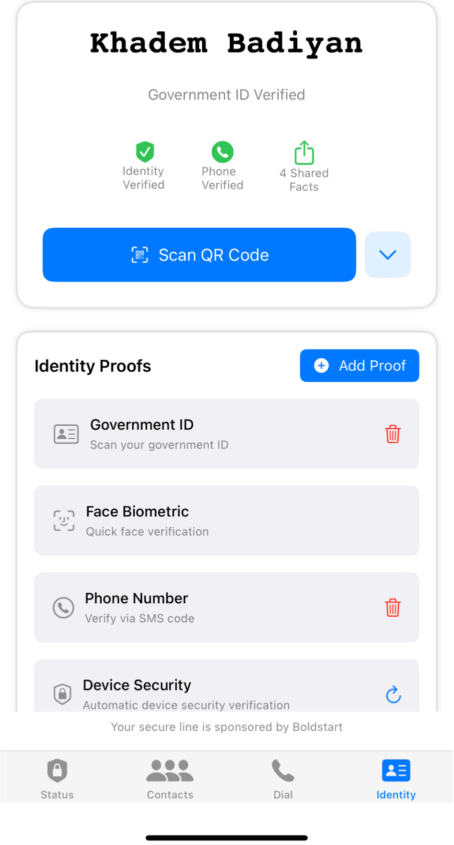
- Volume-based pricing
- Dedicated support and onboarding
- Integration assistance
- Enhanced SLAs and compliance commitments

Whether you're scaling across a region or running targeted verification programs, our pricing is designed to align with your operations — and grow with you.

**Across all Polyguard commercial models, there is no charge for use of the mobile app.

Polyguard Key Technology

Personal Credential Store



Khadem Badiyan

Government ID Verified

Each user's verified identity is securely stored on their own mobile device using a **personal credential store** architecture. This approach prioritizes privacy and minimizes centralized risk by ensuring that sensitive identity data never needs to be aggregated in the cloud.

Key Technical Details:

- **Local Storage with Hardware-Backed Encryption:**
 Identity proofs — including biometric data, verified documents, and associated metadata — are encrypted and stored locally on the user's device. Each credential is encrypted using a **unique key** that is generated and securely stored within the device's **hardware enclave** (e.g., Apple Secure Enclave or Android TEE).

- **Application-Scoped Access Control:**
 These encryption keys are **bound to the Polyguard application**, meaning they cannot be accessed by other apps, the operating system, or even Polyguard's own cloud services. Only the authenticated Polyguard app instance running on the original device can decrypt and use these credentials.

- **No Central Aggregation:**
 Unlike traditional identity providers that store personal data in centralized databases — creating attractive targets for attackers — Polyguard avoids aggregating user identity data in the cloud. This reduces the risk of large-scale breaches and ensures that **each user remains in control** of their own verified identity.

By combining secure local storage with application-scoped cryptographic protections, Polyguard significantly raises the standard for privacy and data security in identity verification.

Device Tamper-Proofing with Hardware Attestation

Polyguard employs Apple's App Attest framework to ensure the integrity of its mobile application and the authenticity of the devices on which it operates. This integration provides a robust mechanism to detect and prevent unauthorized modifications and usage.

How it works:

- **Secure Key Generation:** During user registration, the Polyguard app generates a unique cryptographic key pair within the device's Secure Enclave. This key is inaccessible to the application itself, safeguarding it against extraction or misuse.

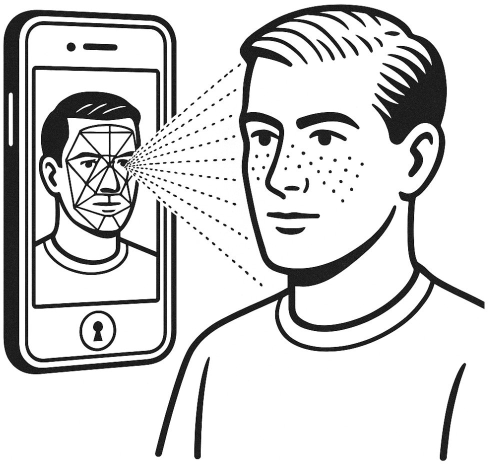
- **App Integrity Verification:** The app creates an attestation that includes a hash of its binary and other relevant data. This attestation is signed by Apple, confirming that the app is genuine and unaltered.

- **Device Authenticity Assurance:** The attestation process also verifies that the app is running on a legitimate Apple device. This step is crucial in preventing the use of emulators or jailbroken devices that could compromise security.

- **Payload Validation:** For each critical operation, the app generates assertions that are cryptographically signed using the attested key. These assertions ensure that the data sent to Polyguard's servers has not been tampered with during transit.

By leveraging App Attest, Polyguard adds an additional layer of security, ensuring that only authentic, unmodified applications on genuine devices can interact with its services. This approach significantly reduces the risk of fraud and unauthorized access.

AI-Strong Biometric Verification



Polyguard’s biometric verification system is built to withstand the latest advances in synthetic media and presentation attacks. By leveraging **3D sensing capabilities** in modern smartphones and combining them with secure execution environments, Polyguard ensures that biometric authentication is both accurate and resilient to spoofing.

Core Technologies and Protections:

- **3D Depth Sensing (LIDAR / Time-of-Flight):** Polyguard uses the smartphone’s front-facing depth sensor to capture a three-dimensional scan of the user’s face. This confirms the presence of a real human subject, rather than a flat image or a video replay. Devices with **Apple FaceID** or equivalent **Android 3D sensing hardware** are fully supported.

- **On-Device Validation:** All biometric capture and liveness detection is performed on the device itself. Combined with Polyguard’s **device tamper-proofing**, this prevents external manipulation or injection of synthetic video streams via virtual cameras or emulators.

- **Liveness & Anti-Spoofing Checks:**
  The biometric engine actively detects signs of spoofing attempts, including photo presentation, screen replays, and 2D masks. Depth cues, motion parallax, and illumination changes are evaluated in real time to confirm a live subject.

- **Cryptographic Binding:**
  A successful facial verification is cryptographically bound to the session and device context, ensuring that verified identity cannot be reused or replayed in a different environment.

By combining **hardware-enforced integrity** with **AI-driven biometric analysis**, Polyguard ensures that biometric identity verification is not only convenient, but also resistant to modern impersonation tactics — including deepfakes, photo attacks, and avatar-based fraud.

Document Proofing

> “There are more than 1 billion ePassports issued currently, by 174 countries as of December 2024.”

Polyguard combines third-party intelligence with in-house verification capabilities to deliver rigorous, globally scalable document proofing.

We integrate with **Veriff**, a best-in-class identity verification provider, to support a broad array of documents from across the globe. At the same time, for the most secure and tamper-resistant document types — such as **ePassports** and **RealIDs** — Polyguard performs **direct, on-device verification** using the smartphone’s **NFC chip**. This allows us to read **cryptographically signed data** embedded within the document’s secure chip, ensuring both the **authenticity of the document** and a **high-confidence match to the individual’s biometrics and biographical information**.

Coverage and Capabilities

- **Countries Supported:**
  Identity documents from over **230 countries and territories** are accepted and validated through our integration with Veriff.

- **Document Types Supported:**
  Over **12,000 unique government-issued identity documents**, including:
  - National ID cards
  - Passports and ePassports
  - Driver’s licenses

- Residence permits
- Travel visas

- **High-Assurance Document Verification (NFC):** For NFC-enabled IDs like **ePassports** and **RealIDs**, Polyguard performs secure element reading directly from the embedded chip — verifying both the digital signature and the biometric match without relying on third-party services.

Fraud Scoring by Document Type

Different document types carry different levels of inherent trust. A government-issued passport with embedded cryptographic data offers significantly stronger verification guarantees than a physical driver's license or photo upload. Polyguard's system automatically adjusts **fraud risk scores** based on document type, issuance country, and real-time verification confidence — enabling more accurate, context-aware decisions across hiring and onboarding workflows.

Business Records Affidavits

Polyguard ensures that each identity verification is supported by a legally admissible **Business Records Affidavit**, providing a robust foundation for compliance and legal defensibility.

A Business Records Affidavit is a sworn statement by the custodian of records affirming the authenticity and accuracy of business records. In legal proceedings, such affidavits are commonly used to admit business records into evidence without requiring the custodian to testify in person.

Key Features:

- **Immutable Audit Logs:** Each secure meeting generates a cryptographically signed audit log, detailing the identity verification process, including methods used, timestamps, and outcomes.

- **Affidavit Generation:** These audit logs are used to create Business Records Affidavits, which are signed by the custodian of records and notarized, affirming the records' authenticity.

- **Legal Admissibility:** The affidavits comply with legal standards for admitting business records into evidence, facilitating their acceptance in court proceedings.

- **Accessibility:** Affidavits are readily available through the Polyguard dashboard, linked directly to the corresponding audit logs for ease of retrieval.

By providing Business Records Affidavits, Polyguard offers clients a reliable means to demonstrate the integrity of identity verification processes, supporting legal compliance and enhancing trust in the system's security measures.

Location Proofing

- Polyguard captures coarse-grained location signals to provide additional context and strengthen identity verification without compromising user privacy.
- Location data is collected through multiple channels, including GSM network information, GPS readings, Wi-Fi SSID signatures, and IP address analysis. These signals are gathered both at the device level — via the tamper-evident mobile client — and at the network layer to ensure consistency and authenticity.
- Importantly, all location data is collected in compliance with applicable privacy regulations (such as GDPR and CCPA). Only the minimum necessary information is captured, avoiding precise tracking while still enabling effective fraud detection and proof of presence.
- Location proofing supports anomaly detection (e.g., impossible travel scenarios, unexpected geo-patterns) and reinforces trust decisions in a privacy-conscious manner.

Certainty Scoring

Polyguard is not a detection platform. In the synthetic age, where the line between real and artificial identities is increasingly blurred, we operate with a "default deny" posture toward any unverified identity.

Rather than relying on outdated fraud scoring models that attempt to detect anomalies after the fact, Polyguard provides a **certainty score** — a measure of how strongly a user's identity has been verified based on cryptographic proofs and real-time biometrics.

Certainty scoring incorporates multiple independent signals, including:

- Type and quality of the identity document presented
- Results from document and identity proofing
- Number and pattern of repeat identity proofing attempts
- Validation against trusted third-party databases
- Real-time facial biometric match distance and liveness results
- Hardware attestation status, including repeat device certification attempts
- Continuity of location signals across interactions

The certainty score provides administrators with clear, actionable insight into the trustworthiness of each verified participant — enabling confident decisions without relying on subjective or probabilistic fraud models.

Fine-Grained Trust Protocol

In today’s dynamic threat landscape, trust must be adaptive. Every organization — and every role within it — faces distinct risks. Polyguard’s fine-grained trust protocol extends traditional scoped authorization by introducing **context-aware proof requirements** that can be customized per role, per event, or per verification workflow.

Administrators, recruiters, and security analysts can easily define **adaptive trust policies** that specify exactly what proofs are required based on the sensitivity of the interaction and the threat environment.

Configurable parameters include:

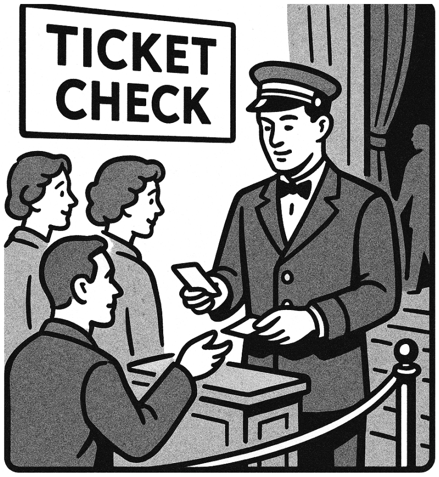
- Setting minimum certainty score thresholds for identity acceptance
- Restricting verified participants to specific geographic regions based on location proofing data
- Excluding lower-trust identity document types from approval flows

This architecture allows organizations to dynamically align identity verification policies with operational risk — providing strong, role-specific protection against synthetic, impersonated, or compromised identities.

User Guide

Overview: Secure Meetings

Polyguard Secure Meetings provides an end-to-end system for verifying candidate identity before, during, and after virtual interviews. This guide outlines the steps recruiters, candidates, and administrators need to follow to ensure seamless identity verification and secure meeting participation.



Components & System Requirements

All users of the Polyguard System use a mobile application to verify and share identity proofs. Talent management team members can create verified meetings or request ad-hoc identity verifications through the web-based Administrative Dashboard, or directly within the interface of their Video Conferencing application.

Mobile Client App	Candidate-facing app for identity verification and secure meeting participation	Apple iPhone 10 or newer (running iOS 17.0+), Android (see supported device list)
Admin Dashboard	Recruiter/admin-facing portal for managing meeting invitations and viewing audit records	Web-based, compatible with Zoom, Chrome, Edge, Safari
Video Conferencing Integration	Embedded apps for Zoom and Microsoft Teams that enable review of real-time identity verification within the meeting interface	Zoom (5.15+), Teams (All platforms)

Workflows

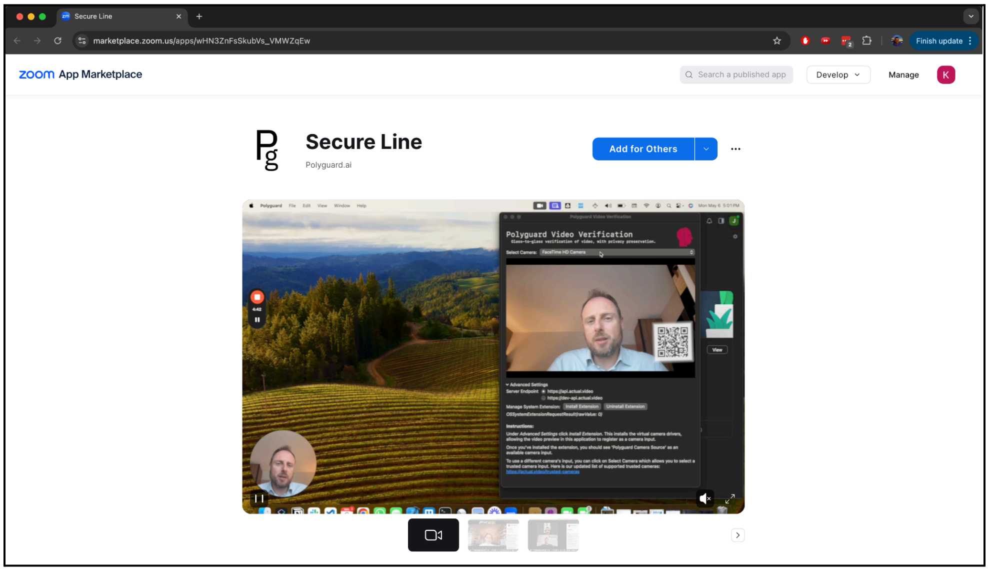
Before individual team members can use Polyguard within Zoom or Teams, the application must first be installed by an account administrator.

To install Polyguard in your Zoom Workspace:

1. Navigate to the Polyguard application in the Zoom App Marketplace.

2. Click **"Add for Others"** and accept the requested permissions.

   These permissions allow Polyguard to create meetings and maintain complete audit logs, including verified participant attendance.



Select Camera: FaceTime HD Camera

Advanced Settings

Server Endpoint ● https://api.actual.video
○ https://dev-api.actual.video

Manage System Extension: Install Extension Uninstall Extension

OSSystemExtensionRequestResult(rawValue: 0)

Instructions:

Under *Advanced Settings* click *Install Extension*. This installs the virtual camera drivers, allowing the video preview in this application to register as a camera input.

Once you've installed the extension, you should see 'Polyguard Camera Source' as an available camera input.

To use a different camera's input, you can click on Select Camera which allows you to select a trusted camera input. Here is our updated list of supported trusted cameras: https://actual.video/trusted-cameras

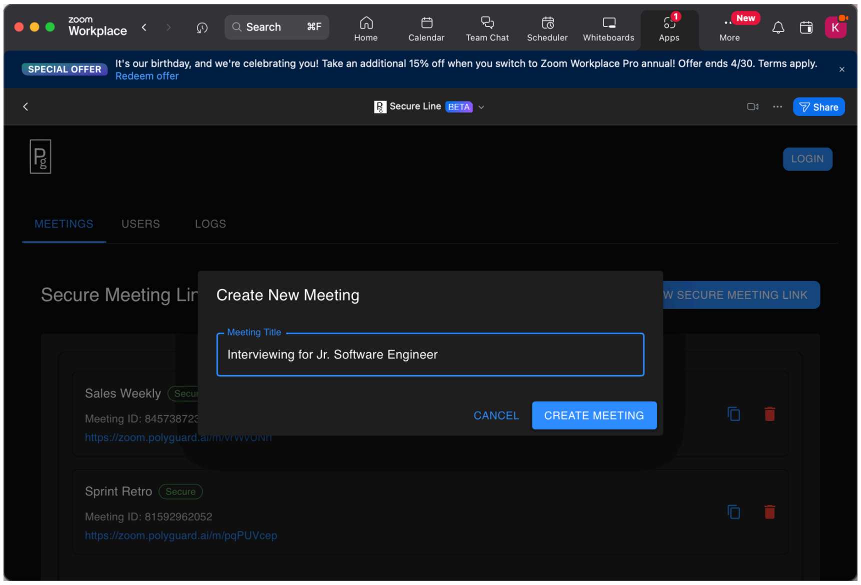
Meeting Creation

To create a Secured Meeting in Zoom:

1. Press **"+ Create New Secure Meeting Link"** to generate a new Polyguard Secured Meeting.

2. Configure the meeting permissions:

    - Set verification requirements, such as document proofing, biometric checks, or verified location.



It's our birthday, and we're celebrating you! Take an additional 15% off when you switch to Zoom Workplace Pro annual! Offer ends 4/30. Terms apply.

Secure Meeting Lin

Create New Meeting

Meeting Title: Interviewing for Jr. Software Engineer

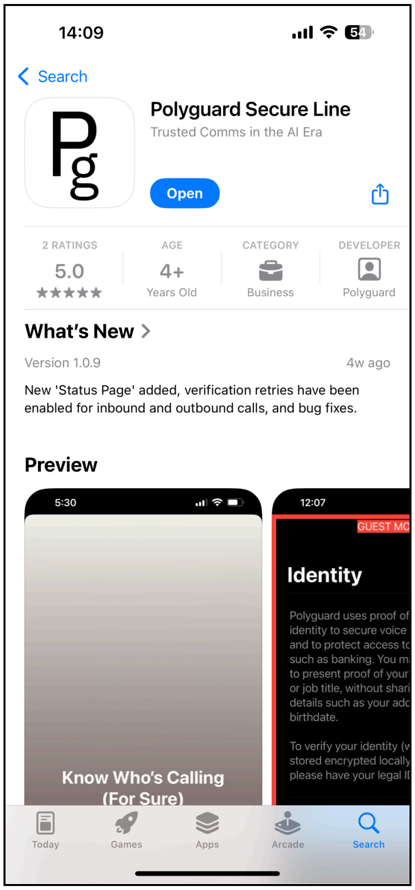
Sales Weekly Secu
Meeting ID: 845738723
https://zoom.polyguard.ai/m/vrWVUNn

Sprint Retro Secure
Meeting ID: 81592962052
https://zoom.polyguard.ai/m/pqPUVcep

Candidate Identity Verification

Mobile App Installation:

- Candidates receive a secure link via email or SMS.
- The link directs them to the App Store or Google Play to download the Polyguard mobile app.



14:09

< Search

Polyguard Secure Line

Trusted Comms in the AI Era

Open

2 RATINGS	AGE	CATEGORY	DEVELOPER
5.0 ★★★★★	4+ Years Old	Business	Polyguard

What's New >

Version 1.0.9 4w ago

New 'Status Page' added, verification retries have been enabled for inbound and outbound calls, and bug fixes.

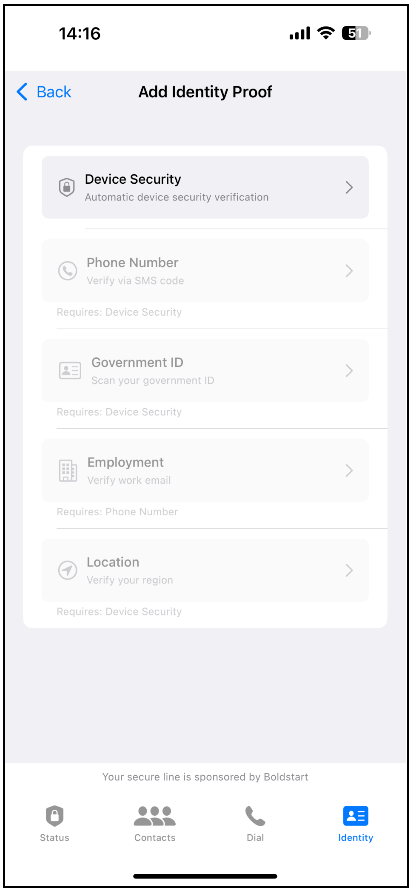
Preview

Know Who's Calling (For Sure)

Identity

Polyguard uses proof of identity to secure voice and to protect access to such as banking. You m to present proof of your or job title, without shari details such as your add birthdate.

To verify your identity (v stored encrypted locally please have your legal II



14:16

< Back Add Identity Proof

Device Security — Automatic device security verification

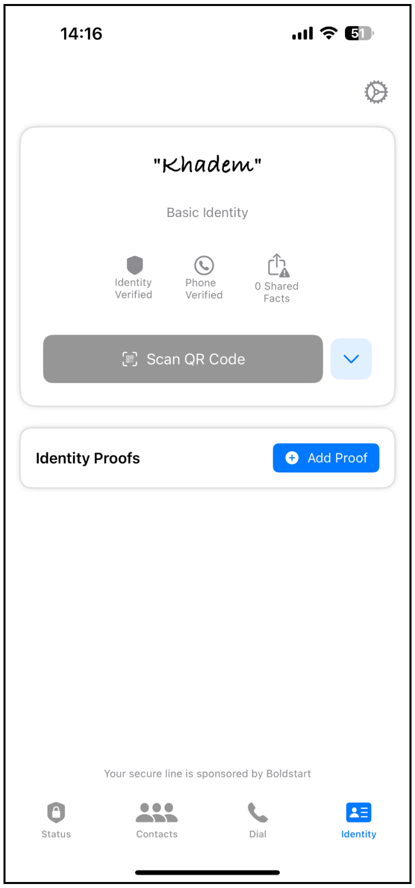
Phone Number — Verify via SMS code — Requires: Device Security

Government ID — Scan your government ID — Requires: Device Security

Employment — Verify work email — Requires: Phone Number

Location — Verify your region — Requires: Device Security

Your secure line is sponsored by Boldstart



14:16

"Khadem"

Basic Identity

Identity Verified

Phone Verified

0 Shared Facts

Scan QR Code

Identity Proofs

Add Proof

Your secure line is sponsored by Boldstart

Identity Verification Steps:

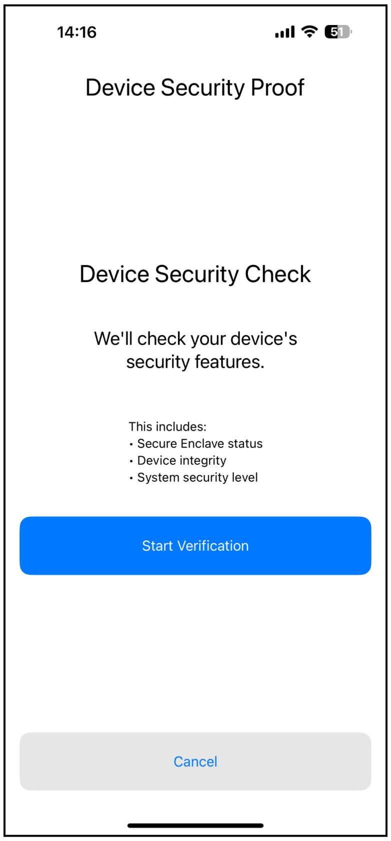
1. **Device Integrity Check**
   Ensure the candidate’s device meets security and tamperproofing requirements.

2. **Phone Number Verification**
   Confirm the candidate’s phone number through a one-time SMS verification code.

3. **Biometric Verification**
   Perform a facial scan with liveness detection to verify the candidate’s identity.

4. **Document Proofing**
   Capture and validate a government-issued ID, using NFC reading if available.

Upon successful completion of these steps, candidates receive confirmation and are authorized to join secured meetings, or provide ad-hoc identity verification proofs.



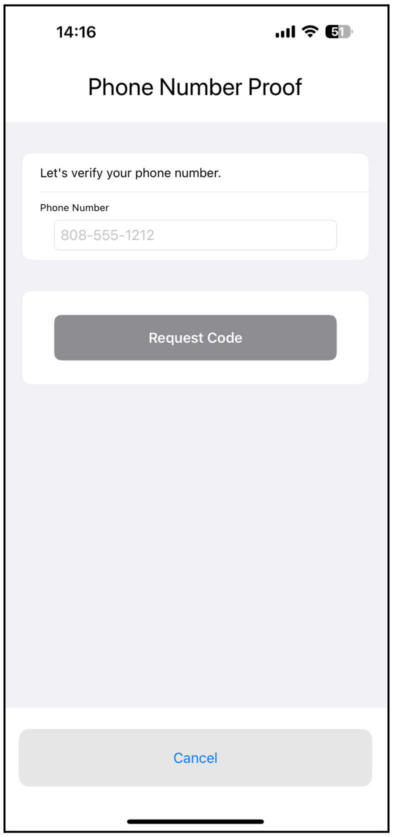
14:16

Device Security Proof

Device Security Check

We'll check your device's security features.

This includes:
- Secure Enclave status
- Device integrity
- System security level

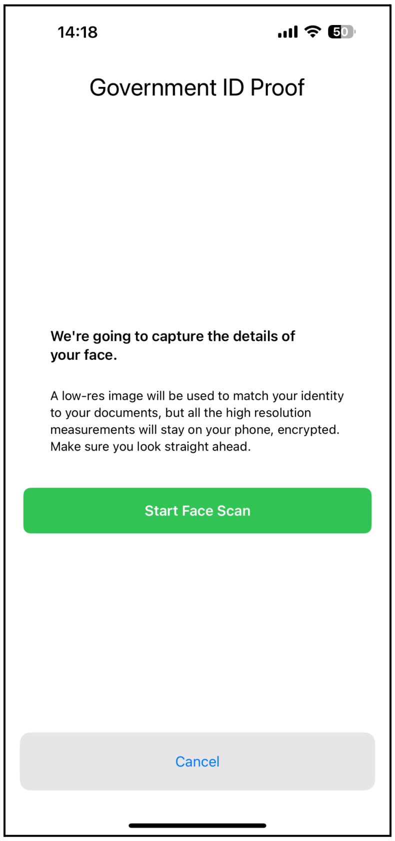


14:16

Phone Number Proof

Let's verify your phone number.

Phone Number: 808-555-1212



14:18

Government ID Proof

We're going to capture the details of your face.

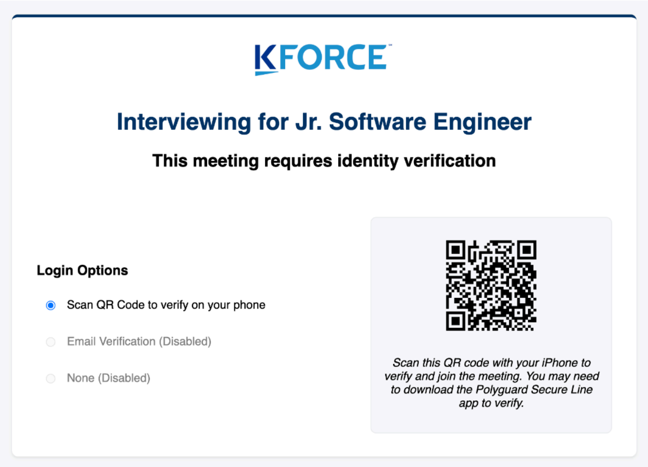
A low-res image will be used to match your identity to your documents, but all the high resolution measurements will stay on your phone, encrypted. Make sure you look straight ahead.

Joining a Secured Meeting

- Candidates access the secured meeting link by either:
  – Visiting the link on their mobile device, or
  – Scanning the QR code displayed on their desktop or laptop via the Polyguard Secure Redirect Link.

- Upon access, Polyguard performs a quick, real-time biometric liveness check of the candidate;

- Verified candidates are automatically granted access and redirected into the meeting (Zoom or Teams) on their device; recruiters are notified of each candidate's verified status within the meeting interface.



KFORCE

Interviewing for Jr. Software Engineer

This meeting requires identity verification

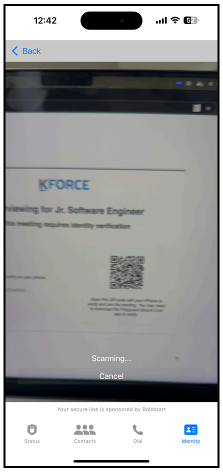
Login Options

● Scan QR Code to verify on your phone

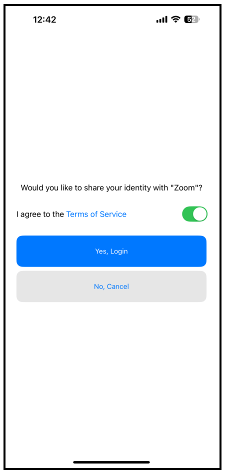
○ Email Verification (Disabled)

○ None (Disabled)

Scan this QR code with your iPhone to verify and join the meeting. You may need to download the Polyguard Secure Line app to verify.



Your secure line is sponsored by Boldstart



Would you like to share your identity with "Zoom"?

I agree to the Terms of Service

Reviewing Verification Records

Admin Dashboard Features:

- View upcoming secured meetings and the list of invited candidates.
- Monitor each candidate's verification status and assigned grade (A–F).
- Access immutable audit logs for every meeting, including:
  - Verification methods used (biometrics, document proofing, phone number verification)
  - Timestamps for each verification event
  - Fraud certainty scoring for each participant

Export Options:

- Generate **Business Records Affidavits** to support client audits or internal compliance reviews.
- Download **Meeting Verification Summaries** as PDFs for reporting or archival purposes.

Support Model

We offer **multiple support options** to meet diverse client needs globally, including **24/7 multilingual coverage**, **geo-distributed support teams**, and **scalable engagement models** — all tailored to your licensing framework.

- 24/7/365 availability with guaranteed SLA adherence
- Multilingual capabilities across critical regions
- Geo-distributed teams for "Follow-the-Sun" support
- Data privacy, compliance (e.g., SOC 2, GDPR, ISO 27001) aligned
- Flexible resource allocation (full-time, part-time, and variable models)
- Implementation resources, including setup, testing and training, to meet the desired go-live date agreed upon
- Access to support across multiple channels including phone, email, chat and online knowledge base

Tiered Support Options

Option 1: Standard Support Model

- **Coverage:** Business hours (9-5 local timezone)
- **Languages:** English primary, additional languages on-demand
- **Scope:**
    - Incident Response
      (Critical: P1/P2 during working hours, 2 hour response SLA)
      (Standard: P3/P4 during working hours, 4 hour response SLA)
    - Basic onboarding assistance
    - Light account management (ticket handling, knowledge base access)
- **Geo Availability:** Americas, EMEA, APAC regions (regional focus)

Option 2: Dedicated Support Model (24/7/365)

- **Coverage:** Full global coverage, including holidays
- **Languages:** English, Spanish, Hindi (other languages available)
- **Scope:**
    - Real-time critical incident management (P1–P4)
    - Dedicated Customer Success Manager (CSM)
    - Quarterly Business Reviews (QBRs)
    - Onboarding, compliance support, and security posture reviews
- **Geo Availability:** ***Follow-the-Sun global team*** (coverage: North America, Europe, Asia)

Option 3: Flexible Support Model

- **Coverage:** Flexible — tailored to peaks in demand or specific seasons
- **Languages:** Multilingual team available on-demand
- **Scope:**
  - Elastic scaling based on business events (e.g., product launches, audits, threat advisories)
  - Support resource pool that scales up/down as needed
  - AI-driven triage to prioritize and route incidents efficiently
- **Geo Availability:** Elastic — assigned based on need and workload

Capability	Standard	Dedicated	Flexible
Incident Response SLA	4 hours (business hours)	30 min – 1 hour (24/7)	Based on demand
Languages Supported	English + Optional	Multilingual standard	Multilingual on-demand
Onboarding Support	Limited	Full lifecycle onboarding	Available as needed
Customer Success Manager (CSM)	Yes (shared resource)	Yes (Dedicated)	Yes (shared resource)
Compliance and Audit Assistance	Minimal	Full support	Available as needed

Geo and Language Coverage

- **Americas:** English, Spanish, Portuguese
- **EMEA:** English, French, German, Arabic
- **APAC:** English, Mandarin, Japanese, Korean, Hindi

*All critical support functions operate on a **Follow-the-Sun model** ensuring zero downtime coverage.*

Mobile Client User Support

All users of the Polyguard Mobile application have access to standard application support.

Mobile Support Access Points

Polyguard Mobile App users can access support through:

- **In-App Support Center:** Direct from the Polyguard app menu
- **Live Chat:** 24/7 multilingual support embedded in app
- **Help Articles:** Mobile-optimized FAQs and troubleshooting guides
- **Phone Support:** Click-to-call feature inside the app
- **Email Ticketing:** Auto-fill form submissions routed to tiered support teams

Mobile Support Workflow Overview

Stage	Action	Platform Behavior	Escalation Path
Issue Encountered	User identifies an issue or question within the mobile app	"Need Help?" button available on all screens	N/A
Self-Service Attempt	User can browse FAQs, common issues, and quick troubleshooting tips	Dynamic knowledge base suggestions	N/A
Live Chat Initiated	User connects to AI-powered chatbot or human agent	In-app messaging panel	AI agent escalates to human if no resolution in 5 min
Ticket Created	If not resolved, support ticket automatically generated	Pre-populated with device info, app version, user ID	Assigned to Tier 1 mobile support specialist
Initial Triage	Tier 1 specialist assesses ticket and resolves or escalates	80% of issues resolved at Tier 1	Tier 2 escalated for technical/development investigation
Tier 2 Escalation	Advanced issues (e.g., app crashes, data sync failures)	Development/Engineering support	Ticket handoff with full context
Resolution Provided	User receives solution via chat, email, or app notification	Update confirmation or workaround steps provided	Escalation to Customer Success if unresolved
Follow-Up	24-hour automated check-in to confirm satisfaction	Quick survey or reopen option if needed	Customer Success Manager engagement if re-opened

System Status Alerting and RCA Policy

- Any system user can sign up for system status alerts.
- We provide RCA's on all incidents and provide follow up to all support related interactions.

Example RCA Incident Response Flow

Stage	Action	Timeline	Responsible Team
Detection	Monitor identifies system degradation	T=0 min	Monitoring/AI Ops
Notification	System alert auto-triggers status alert to subscribers	T=0–15 min	Infrastructure Support
Containment	Initial triage and mitigation steps taken	T=0–1 hr	Site Reliability Engineering (SRE)
Customer Communication	Preliminary notification sent to clients	T=0–2 hr	Support Desk
Root Cause Investigation	Detailed technical analysis begins	T=0–48 hr	Incident Response Team
RCA Report Issued	RCA delivered to impacted clients	T=72 hr max	Security/Engineering
Remediation Validation	Fix verified, and status page updated	T=5 business days	Quality Assurance
Follow-Up	CSM outreach with closure summary and lessons learned	Post-resolution	Customer Success

Professional Services

Typical Implementation Services & Timeline

Phase	Activity	Duration	Description
Lead Time	Resource Alignment	2–4 weeks	Internal team preparation, resource assignment, and kickoff scheduling
Kick-Off	Project Kick-Off Meeting	1-3 days	Define project goals, timelines, stakeholders, and success criteria (onsite or remote)
Train-the-Trainer	Core Team Enablement	1 week	Intensive training sessions for key client trainers (onsite or remote)
Integration	Authentication (AuthN) / Authorization (AuthZ)	3–5 weeks	Secure integration into existing IAM (Identity and Access Management) systems including SSO, MFA, and Role-Based Access Control (RBAC)
Installation	Solution Deployment	2–4 weeks	Installation of software agents, cloud connectors, configuration of monitoring rules and alerts
Monitoring	Usage and Support Incident Monitoring	First 90 Days and Ongoing	CSM engagement, health score monitoring, incident response tracking and adoption KPI’s tracking

Available Supporting Services

Service	Description
Training (Onsite and Remote)	Comprehensive administrator, SOC analyst, and end-user training packages; Available both in-person and virtually
Onboarding Services	Personalized onboarding plan including environment assessment, documentation hand-off, and first 90-day support alignment
Integration Engineering Services	Hands-on technical consultants to assist in complex integrations, API development, and customization requests
Professional Services Project Management	Dedicated Project Manager (PM) assigned to ensure on-time delivery and manage communication, risks, and escalations

Additional Integration and White-Labeling

Logo and Theming
The candidate experience for Polyguard-verified meetings can be fully customized to reflect your brand. Customers may configure logos, brand colors, fonts, and domain names to create a seamless and familiar experience.

Customized Terms of Service
Candidates are required to accept terms and conditions of service (via clickwrap) when joining identity-verified meetings. These terms can be customized at the customer level — or even tailored for specific meetings — to reflect unique legal or operational requirements.

Roles-Based Access Control (RBAC)
While small businesses and agencies may use the out-of-the-box authentication model, larger enterprises typically prefer fine-grained roles-based access control. Polyguard supports integration with Microsoft Entra ID, Google Workspaces, and any OAuth 2.0–compatible Identity Provider (IdP), allowing your IT team to map appropriate roles and scoped privileges across the platform.

Customer-Managed Encryption Keys
All non-repudiable audit logs are encrypted at rest. For customers with heightened security requirements, Polyguard supports the use of customer-provided encryption keys via AWS KMS or equivalent key management systems.

Event Alerting and Webhook Integration
To enable integrated workflows, especially within Talent Management Systems (TMS) or Applicant Tracking Systems (ATS), Polyguard can deliver real-time webhook events for key candidate milestones, including invitation acceptance and identity verification completion.

Single-Tenant Deployments
For enterprises operating in highly regulated sectors such as defense, intelligence, or critical infrastructure, Polyguard can be deployed as a dedicated single-tenant environment. These environments may be managed by the customer’s IT team or supported by Polyguard’s operations team, depending on customer preference.

System Operations and Security Practices

Polyguard's platform is designed and operated with a security-first mindset, ensuring resilience, scalability, data protection, and regulatory compliance at every layer of the system.

Scale and Performance

Polyguard's infrastructure is architected for high concurrency and global distribution. Our current production environment supports:

- **Total Load:** Elastic scaling to support millions of verification events daily, with peak load tested beyond projected client growth scenarios.

- **Concurrent Sessions:** Up to 10,000 simultaneous identity verification sessions per region.

System capacity planning is proactive, with auto-scaling and redundancy across multiple availability zones to ensure consistent performance under load.

Data Residency and Retention

Polyguard offers flexible data residency options to align with client jurisdictional requirements. Core infrastructure supports data residency in the United States, Canada, and the European Union, with expansion to other regions on request.

All customer data is subject to strict retention policies:

- Identity verification session data is retained for a **default period of one year** unless otherwise specified by the client.
- Clients may request shorter or longer retention windows, including immediate data deletion upon verification outcome.

No biometric templates are stored centrally — all biometric data remains secured within the user's mobile device.

Encryption and Data Protection

Data is encrypted in transit and at rest using strong, modern encryption standards:

- **In Transit:** TLS 1.3 with forward secrecy
- **At Rest:** AES-256 encryption across all storage layers

- **Key Management:** Customer-specific encryption keys are supported via integrated Key Management Service (KMS) options

Sensitive operations, including biometric analysis and document proofing, are performed in secure, ephemeral processing environments to minimize data exposure risks.

Data Sanitization

Polyguard follows industry best practices for secure data sanitization and disposal, including:

- Cryptographic erasure of storage volumes
- Verification of secure wipe processes on media retirement
- Automated deletion workflows based on retention schedules and client policies

We maintain alignment with NIST SP 800-88 guidelines for media sanitization.

Business Continuity and Disaster Recovery (BC/DR)

Polyguard maintains a comprehensive BC/DR plan that is reviewed and tested semi-annually. Key elements include:

- **RTO (Recovery Time Objective):** 4 hours
- **RPO (Recovery Point Objective):** 5 minutes
- **Multi-region failover:** Active-active architecture across geographically separate data centers
- **Incident Response Integration:** Seamless escalation from system events to security incident response playbooks

All critical systems have defined recovery priorities, and customer communications are integrated into our incident management process to ensure transparency in the event of major disruptions.

Regulatory Compliance

At Polyguard, regulatory compliance is a core pillar of our approach to security, privacy, and trust. Although we are an early-stage company, we have prioritized building a robust governance, risk, and compliance (GRC) program from the outset, and have engaged a leading cybersecurity firm (see attachments) to conduct a formal GRC assessment in 2025. Our commitment is to not only meet but exceed the standards expected by our enterprise customers and regulatory bodies.

Data Protection and Privacy

Polyguard's systems and processes are designed to align with major data privacy regulations, including the California Consumer Privacy Act (CCPA) and the European Union's General Data Protection Regulation (GDPR). We implement data minimization, user consent management, access controls, and encryption of data at rest and in transit, in line with these frameworks.

Security Standards and Certifications

We are actively working toward a SOC 2 Type II certification and follow best practices aligned with the American Institute of CPAs (AICPA) Trust Services Criteria. Our technical and operational controls also reflect guidance from the National Institute of Standards and Technology (NIST), particularly the NIST 800-63 Digital Identity Guidelines, which are foundational to our identity verification processes.

While formal certifications are underway, we have implemented controls and internal audits consistent with these standards, and maintain comprehensive documentation to support future attestation.

Identity and Anti-Fraud Regulations

Polyguard's identity verification solutions are built to align with the Fair Credit Reporting Act (FCRA) where applicable, and we have designed our technology stack with compliance to industry-specific requirements such as the Cybersecurity Maturity Model Certification (CMMC) in mind. Our identity proofing protocols and fraud prevention measures adhere closely to emerging best practices for secure and verifiable digital identities.

Audit and Reporting

Polyguard maintains detailed operational logs and audit trails to support customer compliance requirements. Our platform can produce reporting necessary for regulatory audits and internal reviews, including access history, identity verification events, and data residency assurances.

Ongoing Monitoring and Adaptation

We recognize that the regulatory landscape continues to evolve, particularly in the areas of artificial intelligence, biometrics, and digital trust. Polyguard is committed to continuous monitoring of relevant legal and regulatory changes, and we proactively update our processes and policies to ensure ongoing compliance as standards develop.

Product Roadmap

Our product roadmap is designed to continuously enhance the security, usability, and reach of our identity verification platform — enabling recruiters and staffing firms to operate with greater confidence and efficiency. We are building the trust infrastructure for the future of digital work.

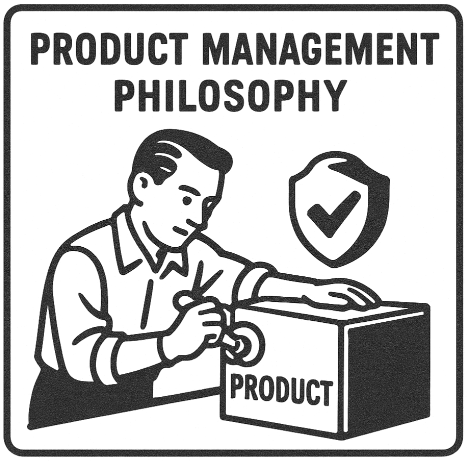
Product Management Philosophy

Our product strategy is grounded in three principles:

- **Customer-Centric Innovation**: We prioritize features that solve real problems for our users and clients.

- **Secure by Design**: Every product enhancement strengthens our core promise of trusted, verified interactions.

- **Continuous Improvement**: We deliver frequent, incremental updates to maximize value and responsiveness.



Focus Themes

Our roadmap is organized around three focus areas — who, where, and what:

- **Who Can Use This**: Expanding device and language accessibility to serve a global, mobile, and diverse workforce.

- **Where They Can Use It**: Deepening integrations with the collaboration tools staffing firms already rely on, and improving the ease of embedded and on-demand verifications.

- **What It Integrates With**: Enhancing compatibility with major conferencing and ATS platforms to streamline workflows.

Roadmap Highlights

(*Timeline are estimates only, and subject to change*)

- **Basic Teams Integration** *(Q2 2025)*
  Enable candidates to verify identity when joining Microsoft Teams meetings (at parity with existing Zoom Workspace integration).

- **Deeper Teams Integration** *(Q3 2025)*
  Allow recruiters to access candidate identity verification details directly within the Teams meeting interface, and to request ad-hoc verification during an existing meeting.

- **Android Client Release** *(Q3 2025)*
  Extend full mobile identity verification capabilities to a majority of Android devices, in addition to iOS.

- **Localization** *(Q4 2025)*
  Translate all candidate-facing and recruiter-facing screens into Hindi, Spanish, and Portuguese to support global adoption.

- **Embedded eSignature for Candidate Consent** *(Q4 2025)*
  Upgrade click-through Terms of Service to an embedded eSignature workflow for stronger legal compliance and better candidate experience.

- **Analytics Module** *(Q4 2025)*
  Provide admins and recruiters with dashboards showing usage metrics, adoption rates, verification success rates, and actionable insights.

Appendices

Android Device Compatibility

We rely on the Google Play Integrity hardware attestation to ensure that Polyguard verifications are not compromised through jailbroken operating systems or the injection of virtual cameras. This limits our mobile app support to target android device types that pass “MEETS_STRONG_INTEGRITY” thresholds:

Eligible Devices

- Most recent Google Pixel phones (e.g., Pixel 6, 7, 8 series) running official, up-to-date firmware with a locked bootloader.
- Recent Samsung Galaxy flagship devices (e.g., Galaxy S22, S23, S24, Note 20, Z Fold/Flip series) with official firmware, Play Protect certification, and a locked bootloader.
- Other major OEMs' flagships (e.g., OnePlus, Xiaomi, Sony, Oppo) that are Play Protect certified, running unmodified stock firmware, and with a locked bootloader.

Ineligible Devices

- Devices with an unlocked bootloader or any form of root access.
- Devices running custom ROMs (e.g., LineageOS, GrapheneOS, CalyxOS)-even if signed or supporting hardware attestation.
- Devices with outdated security patches or missing vendor updates.
- Devices with revoked or broken hardware key stores (e.g., certain ASUS ROG models after key revocation)1.
- Devices not Play Protect certified (including many imported or region-unlocked models).

POLYGUARD VERIFIED MEETING AFFIDAVIT

Meeting Audit Report - Downloaded: 2025-04-13T14:00:11Z

Meeting Information

Platform: Zoom Workspace

Title: Polyguard Q1 2025 Board Meeting

Scheduled Date & Time: April 13, 2025 – 2:00 PM ES

Scheduled Duration: 45 minutes

Meeting Host: Joshua McKenty (joshua-25777)

Created by: Joshua McKenty (joshua-25777)

Organization: Polyguard, Inc.

🔐 Verification Summary

All attendees were verified in real-time via Polyguard Secure Line (PSL) using biometric facial authentication and government-issued ID. Each verified participant generated a self-signed affidavit upon entry, cryptographically bound to their identity token.

- Verification Proofs included:

  Hardware Attestation (Apple AppAttest key exchange)
  Facial biometrics (on-device)
  Document Proofing (via proofing partner)
  Phone Number (OTP via SMS)

- Private Key Handling: Zero-trust; attestations signed locally by attendee with a key stored encrypted in the hardware enclave of their mobile device.
- Tamper-Proof Logs: Stored securely with meeting metadata hash: **9fae3c7b...b2849d**

📄 Meeting Integrity Attestation

This document confirms that the listed attendees were live participants verified by PSL at time of entry and that no other individuals joined this session.

Meeting Hash: PGM-20250413-QIR0421

✅ Verified Attendance

Name	*Affiliation*	*Poly ID*	*Entry*	*Exit*
Joshua McKenty	Polyguard, Inc.	joshua-25777	1:57 PM	2:48 PM
Khadem Badiyan	Polyguard, Inc.	khadem-51899	1:59 PM	2:48 PM
Ed Sim	boldstart vc	ed-14556	2:00 PM	2:45 PM

📄 Participant Identity Attestation

Joshua McKenty (joshua-25777)

- **Hardware**: AppAttest Public KeyId: b3epu8dP4Lv98gExzxadIyCIKk8nvgZ21t2GlmV60cU=
- **Phone Number**: Twilio Verification: VEf95e6e62c77179eeaecb53a839b2eff9
- **Document**: *Veriff Session ID:* eae66e14-2642-4201-ae34-7a1b85ba7e9f
- **Biometric**: *PSL FaceAnalyzer Build 1.0.10*, Certainty: 94.773%

Khadem Badiyan (khadem-51899)

- **Hardware**: AppAttest Public KeyId: 6uN+u84HtjbGFtkksVTqrHDLpuWzOjffxF35Rjzw8V4=
- **Phone Number**: Twilio Verification: VEd36fd9840aafca1fd0312c2ce176a267
- **Document**: *Veriff Session ID:* 88a3bcdb-c18f-4997-b297-5f64ad9d062e
- **Biometric**: *PSL FaceAnalyzer Build 1.0.10*, Certainty: 97.451%

Ed Sim (ed-14556)

- **Hardware**: AppAttest Public KeyId: USrOKftreRdZ7Nq5yELsGNzRIQyXNvjgHDL2WWrdFso=
- **Phone Number**: Twilio Verification: VE596938d26e772cbac2afb11507feb16c
- **Document**: *Veriff Session ID:* 50a3ed32-67a8-455f-9596-eb4ec24ead83
- **Biometric**: *PSL FaceAnalyzer Build 1.0.10*, Certainty: 96.11%