




Technical and Operational Specification: Gemini Verification System – GOPHORA

1. Purpose of the System

The verification system aims to guarantee the reliability and authenticity of all providers offering opportunities (services, classes, missions, or hobbies) within the GOPHORA ecosystem.

This is achieved through integration with the Gemini API, which analyzes the provider’s data and returns a Trust Score (0–100) with a short reason explaining the result.

The score determines an automatic traffic-light decision flow:

-  Automatically approved
-  Sent for review
-  Automatically rejected

2. Verification Levels

The system recognizes three provider levels, each with different data sources and verification criteria:

Level	Provider Type	Main Data Sources	Evaluation Method
Level 1 – Institutional	Registered companies with their own website and domain.	Website content, corporate email, domain age, internal reviews.	Business verification through web and registration analysis.
Level 2 – Professional (Freelancer)	Freelancers or instructors with an active online presence.	Social media, online portfolio, account age, engagement rate.	Digital reputation verification.
Level 3 – New Talent	New users without established online presence.	Video introduction, personal description, references, or early user reviews.	Authenticity and motivation verification.

3. General Verification Process

User registers and selects provider type (company, freelancer, or new talent).

System automatically collects data based on the provider's level.

Data is formatted in JSON and sent to the Gemini API.

Gemini analyzes the data and returns:

Trust score (0–100)

reason (short explanation)

System applies the traffic-light logic to make an automatic decision.

Result is stored in the database and the provider is notified.

User can view their status and receive personalized improvement suggestions.

4. Example of Data Structure (JSON format)

```
{
  "provider_id": "UUID",
  "provider_name": "string",
  "provider_type": "institutional | professional | new_talent",
  "data_sources": {
    "website_url": "string | null",
    "email": "string | null",
    "domain_age": "number | null",
    "social_profiles": [
      {
        "platform": "instagram | linkedin | youtube | behance",
        "url": "string",
        "account_age": "number | null",
        "followers": "number | null",
        "engagement_rate": "number | null"
      }
    ],
    "video_intro_url": "string | null",
    "user_description": "string | null",
    "user_reviews": [
      {
        "reviewer_id": "UUID",
        "rating": "number (1-5)",
        "comment": "string"
      }
    ]
  }
}
```

```

},
"system_metadata":{
  "submission_date": "timestamp",
  "collected_by": "system|admin"
}
}

```

5. Required Variables per Level

<i>Variable</i>	<i>Level 1</i>	<i>Level 2</i>	<i>Level 3</i>	<i>Description</i>
Website_Url	✓	✗	✗	Official website URL.
Email	✓	✓	✓ (optional)	Email type (corporate or generic).
Domain_Age	✓	✗	✗	Domain age in years.
Social_Profiles	✗	✓	✓ (if available)	Publicly accessible social media profiles.
Account_Age	✗	✓	✓	Account age in years.
Followers	✗	✓	✓ (if relevant)	Estimated real followers.
Engagement_Rate	✗	✓	✗	Average interaction rate.
Video_Intro_Url	✗	✗	✓	Short introduction video.
User_Description	✓	✓	✓	Short personal or professional description.
User_Reviews	✓	✓	✓	Internal or previous student reviews.

6. Example of Internal Verification Endpoint

Endpoint: POST /api/verification/gemini

Description: Sends provider data to Gemini and returns the Trust Score and reason.

Headers:

Content-Type: application/json

Authorization: Bearer <GEMINI_API_KEY>

Response Example:

```
{
  "provider_id": "UUID",
  "trust_score": 86,
  "reason": "Consistent professional portfolio, verified email, and 4 years of domain activity.",
  "recommendation": "approve"
}
```

7. Traffic-Light Decision Flow

<i>Trust Score Range</i>	<i>Automatic Action</i>	<i>Provider Status</i>	<i>Human Review</i>
≥ 85	Auto-approved	verified	Not required
40 – 84	Sent for review	pending_review	Required (quick check)
< 40	Automatically rejected	denied	Not required

UX Recommendation:

Users should receive automatic notifications with personalized feedback, e.g.:

- “Add an introduction video to improve your verification score.”
- “Connect your professional Instagram account to boost your trust level.”

8. Base Prompt for Gemini API

You are an expert digital verification analyst for a human opportunity platform.

Based on the data provided, analyze the legitimacy and trustworthiness of this provider.

Return a Trust Score (0–100) and a short reason for your score.

9. Specific Considerations per Level

Level 1 – Institutional

- Validate that the email domain matches the website domain.
- Check for professional tone and complete sections (“About”, “Contact”).
- If the website times out, log the error and trigger manual review.
- Allow score recalculation when domain or website data changes.

Level 2 – Professional (Freelancer)

- Require at least one active social profile (6+ months old).
- Include content consistency metrics (regular posts, genuine comments).
- Gemini should analyze visual and textual coherence with the declared service.
- Prioritize portfolio platforms like Behance, YouTube, or LinkedIn if available.

Level 3 – New Talent

- Provide Gemini with the description text and video URL.
- Gemini should evaluate tone, authenticity, and coherence.
- Require at least one internal review or reference to complete verification.
- After three positive user reviews, automatically trigger re-verification (possible level upgrade).

10. Technical Recommendations

Store all verification results (`trust_score`, `reason`, `timestamp`, `provider_type`) in the database.

Add field `verification_source` = "`gemini_v1`" | "`manual_review`" | "`hybrid`".


Cache results for 24 hours to avoid redundant API calls.


Create a `verification_log` table for incomplete or failed API responses.


Implement a “Re-verify” button on the provider dashboard.

11. Recommended User Experience (UX)

Display verification badge:

 AI Verified – Institutional Level

 AI Verified – Professional Level

 AI Verified – Explorer Level

Show the Trust Score and a short “Verified by Gemini” line.

Include a “How to improve your verification” section with specific tips.

Allow re-verification every 60 days.

12. Expected Benefits

<i>Benefit</i>	<i>Description</i>
<i>Consistency</i>	All providers, regardless of type, are evaluated using the same AI.
<i>Inclusion</i>	Individuals without legal registration can still be verified.
<i>Scalability</i>	New verification levels or data types can be added easily.
<i>Security</i>	Reduces fake accounts and unverified providers.
<i>Efficiency</i>	Combines automated verification (Gemini) with selective human review.

Implementation Guide GOPHORA

User Verification System

Objective

To implement a smart and scalable **user verification system** integrated with the **Gemini API**, which evaluates the legitimacy and trustworthiness of providers within the GOPHORA ecosystem.

The system assigns each provider a **Trust Score (0–100)** and performs **automatic actions** based on that score (traffic light logic: approve, review, or reject).

1. User Classification

- Ask the user to select their provider type during registration:
 - **Company / Institution**
 - **Independent Professional / Freelancer**
 - **New Talent / Explorer**
- Automatically assign the verification level according to the selected type.
- Allow level upgrade later (e.g., from *Explorer* to *Professional*).

2. Basic Data Collection

- Provider name.
- Email (check if corporate or generic).
- Website URL (if applicable).
- Country and city.
- Short biography or description.
- Type of service, class, or opportunity offered.

3. Data Requirements by Level

Level 1 – Company / Institution

- Validate if the email domain matches the website domain.
- Analyze website content (professional tone, structure, and completeness).
- Check domain age (preferably >1 year).
- Confirm presence of essential pages: *About Us*, *Contact*, *Team*.
- Detect generic templates or unoriginal content.

Level 2 – Independent Professional / Freelancer

- Require at least one active professional social media account (Instagram, LinkedIn, YouTube, Behance).

- Validate:
 - Account age (minimum 6 months).
 - Posting frequency and engagement rate.
 - Genuine comments and followers.
 - Content coherence with declared service.
- Request portfolio or previous work links.
- Gather internal or external reviews if available.

Level 3 – New Talent / Explorer

- Require a short introduction video (30–60 seconds).
- Request self-description and motivation text.
- Allow one personal or community reference.
- Enable trust growth based on early reviews and activity within GOPHORA.
- Trigger automatic re-verification after three positive internal reviews.

4. Data Transmission to Gemini API

- Format all collected data into a structured JSON object.
- Send via POST `/api/verification/gemini`.
- Include authentication headers:
 - Content-Type: `application/json`
 - Authorization: `Bearer <GEMINI_API_KEY>`
- Store Gemini’s response containing:
 - `trust_score` (0–100)
 - `reason` (short text)

5. Decision Flow (Traffic Light Logic)




<i>Trust Score</i>	<i>Automatic Action</i>	<i>Status</i>	<i>Human Review</i>
≥ 85	Auto-approved	verified	Not required
40–84	Pending review	pending_review	Required (quick)
< 40	Auto-rejected	denied	Not required

- Send notification to admin for “pending review” cases.
- For rejections, display personalized improvement suggestions.

6. Database Storage and Logs

- Save the following fields in the verification table:
 - `provider_id`
 - `trust_score`
 - `reason`
 - `verification_source` (“gemini_v1” or “manual_review”)
 - `timestamp`
- Keep an error log (`verification_log`) for incomplete or failed API calls.
- Cache results for 24 hours to prevent duplicate API requests.

7. User Experience

- Display visible verification badges:
 -  *AI Verified – Institutional Level*
 -  *AI Verified – Professional Level*
 -  *AI Verified – Explorer Level*
- Show Trust Score and short reason (“Verified by Gemini – 86%”).
- Provide automatic improvement tips based on Gemini’s reason.
- Allow re-verification after profile updates.

8. Notifications

- Send automatic email or in-app message with the result:
 - **Approved:** “Your profile has been successfully verified.”
 - **In Review:** “Your profile is currently being reviewed by our verification team.”
 - **Rejected:** “Your profile did not meet the minimum verification requirements. Please review the improvement suggestions.”
- Notify admin for users flagged as “pending review.”

9. Admin Dashboard Requirements

- Display all providers with their Trust Scores.
- Filter by verification status (verified, pending_review, denied).
- Include “Re-verify with Gemini” button.
- Show verification history (past scores, timestamps).
- Allow manual override with admin notes for auditing.

10. Technical and Security Recommendations

- Recalculate verification automatically every 60–90 days.
- Include internal user ratings as part of future Trust Score adjustments.
- Add field `version_model` to track Gemini version used.
- Protect API keys using environment variables.
- Ensure all endpoints use HTTPS and respect rate limits.
- Allow users to request data deletion (GDPR compliance).

11. Transparency and Learning

- Display to each user what data was analyzed for verification.
- Offer insight on how to improve their Trust Score.
- Use human-reviewed cases to fine-tune future Gemini evaluations.
- Maintain version history of prompts and parameters used.

12. Expected Results

- Faster verification of new providers.
- Increased trust among users and partners.
- Scalable AI integration across all provider types.
- Inclusive verification for informal or new talents.
- Transparent, auditable, and secure process.