

Caller verification inside your AI voice workflow

Your voice platform handles the conversation. Proofcall checks the expected Microsoft account and returns a structured verification result. Begin with a test tenant and a complete call, including failed verification and human handoff.

Connection model

Use the HTTP API or remote MCP with an individual agent credential. The remote MCP endpoint uses Streamable HTTP at <https://app.proofcall.io/mcp>. Store credentials in your platform's secret store.

MCP tool	Purpose
proofcall_list_clients	Select the expected organisation.
proofcall_find_caller	Find the account and inspect available registered methods.
proofcall_start_verification	Start a request with the required action tier.
proofcall_send_link	Request delivery through a configured channel.
proofcall_wait_for_caller	Wait for the authentication state to change.
proofcall_submit_code	Submit the code the caller reads aloud.

Status checks and cancellation are also available. The handler cannot retrieve the caller's answer from the verification API. An MCP interface does not establish a tested partnership with any specific voice platform.

Integration pilot acceptance checklist

Successful verification

Confirm the account and tenant, requested action tier, completed result and handler attribution. Preserve the verification reference in the consuming workflow.

The sensitive action

The service performing the action must check the verification outcome and its own authorisation policy. Do not make a language model's conversational judgement the only gate.

Failure and human handoff

Test wrong identity, incorrect code, expired session, unavailable authentication and network failure. Use bounded waiting and retries. Failed or incomplete verification must not unlock the test action.

Voice and transcript handling

Ask for the separate Proofcall code only. Test recognition errors without guessing missing digits. Define code redaction and retention in the voice platform before using real caller data.

Operational fit

Measure integration effort, completion rate, elapsed time, retries and escalation. Agree who owns tenant setup, credential rotation, incident handling and recovery exceptions.

Pilot scope

Use a plan supporting agent credentials and MCP. Validate one chosen voice platform first. Start with a non-destructive test action, then agree the controls required before privileged production actions.

Explore the sequence at proofcall.io/for-ai-agents.