ID-TRUSTER

Your customers can see that it really is *you*.

Every email, text, call and meeting from you can be checked in seconds, in a free app. The answer is signed with your key and checked against your own domain. Not against us.

FOR IT	Runs alongside your CRM, email and phone system. No inbound ports.
FOR LEGAL	Customer data stays with you, and every check is logged in your own database. You can document what you sent and what your customer checked.
FOR COMMUNICATIONS	Your customers see your verified name before they reply.

What it does

- **ID-Truster Messages.** Your emails and texts carry a trust code locked to one recipient. A copied code in a new message fails.
- **ID-Truster Calls.** When you call, the app shows who is calling. When your customer calls, they confirm in the app. A PIN ties the voice to the call.
- **ID-Truster Meetings.** Each participant confirms in the app and gives their own PIN. A recording cannot pass.
- A no from a customer or participant warns your company.

How it fits together

- One app for your customers, the ID-Truster service in the middle, and your own ClientDB.
- You host ClientDB, or run it in your own Supabase Cloud account. No company sees another company's data.
- Your ClientDB calls ID-Truster. You open no inbound ports.
- It runs beside your CRM, email, SMS and phone system.
- If ClientDB or ID-Truster is down, your own systems keep working.

Keys and signatures

- Two Ed25519 keys. One shows ID-Truster the call comes from your ClientDB. The other lets the app check that the answer comes from you.
- Both private keys stay in your ClientDB. They are never sent to ID-Truster.
- The public answer key sits in your own DNS, protected with DNSSEC.

Data

- Only the verification signal moves through ID-Truster. Emails, texts and calls never do.
- ID-Truster passes each signal on and deletes it right away.
- Personal data in ClientDB is stored as an HMAC and encrypted.
- Of the user data ID-Truster stores, the only thing it can read is the email address a user signs in with.

Your responsibility

- Protect ClientDB at the same level as your DNS and your mail server.
- Anyone who can call your ClientDB can speak as your company in the app.

Getting started

- Start with one product. Turn Calls, Messages and Meetings on or off one by one.
- Easy to try, and easy to stop. Your emails, texts, calls and meetings go on as before.
- Internal use on your own domain needs no company verification.
- To reach customers and partners, your company is verified first. Your auditor, bank or lawyer, public registers, and two letters.
- ID-Truster runs on Supabase Cloud in the EU, in Frankfurt. Tested before every release. The report is available under NDA.