e-Contact

Authenticated Institutional Communication

Concept Paper · Codelight OÜ · 2026

Executive Summary

In 2025, people in Estonia lost €29 million to phone fraud — three times the amount lost the year before. Every proposed response to date addresses symptoms: slower payments, awareness campaigns, call-blocking apps. None of them close the root cause.

The root cause is a structural asymmetry. Citizens must authenticate to institutions to access any digital service. Institutions face no equivalent requirement when contacting citizens. The citizen has no reliable signal to distinguish a legitimate institution from a scammer.

e-Contact closes that asymmetry. Institutions send authenticated contact requests through a verified digital channel. The citizen sees who is calling, why, and a verified callback number, and decides whether to respond. Once this channel exists and institutions adopt it, a single rule becomes enforceable: **any unsolicited phone call claiming to be from an institution is a scam.**

1. The Problem Is Structural

Estonia has authenticated citizen-to-institution contact for over 20 years. eID, Smart-ID, and Mobile-ID ensure that when a citizen accesses a digital service, their identity is verified cryptographically. The institution knows exactly who they are dealing with.

The reverse is not true. When an institution contacts a citizen by phone, there is no authentication mechanism. The caller asserts an identity. The citizen has no way to verify it. This asymmetry is the root cause of phone fraud. Scammers exploit it by impersonating banks, police, the Tax Board, and other trusted institutions. The technique works not because citizens are careless, but because the channel itself provides no authentication.

Current responses — payment cooling-off periods, awareness campaigns, AI-based call filters — are aimed at the wrong layer. They make fraud marginally harder to execute. They do not close the underlying vulnerability.

There is a further dimension: the problem now damages legitimate institutions too. People have become so wary of unknown numbers that couriers, doctors' offices, and law enforcement struggle to reach citizens by phone. The unauthenticated phone call is no longer working as a communication channel even when used legitimately. The system is broken for everyone.

2. The Solution: A Verified Channel and a New Rule

e-Contact is a platform through which institutions send verified contact requests to citizens. The institution authenticates, attaches a reason and a pre-registered callback number, and submits the request. The citizen receives a notification, reviews the verified details, and decides to call back,

defer, or decline. The institution never calls first. The citizen is always in control.

> Once institutions are on the platform, the following rule becomes enforceable and publicly communicable:
>
> **Any unsolicited phone call claiming to be from an institution is a scam.**
>
> This rule is binary, simple, and requires no technical knowledge from the citizen. It is the same structural shift Estonia made with the paper invoice (replaced by e-invoice), the paper signature (replaced by digital signature), and physical service counters (replaced by state portals).

3. How It Works

Contact flow

1. An institution employee authenticates via eID, Smart-ID, or Mobile-ID.
2. The employee submits a contact request: the citizen's personal code, the reason for contact, and a pre-registered callback number. Employees cannot enter arbitrary numbers.
3. The citizen receives the request through the e-Contact app or, if the app is not installed, via SMS with a secure link to a web view.
4. The citizen sees: verified institution name, verified employee name and role, reason for contact, and the callback number. The citizen calls back, defers, or declines.
5. Every action is logged in a tamper-evident audit trail.

Citizen notification: two channels

e-Contact app (primary)

- Push notification on the citizen's smartphone
- Full request detail, one tap to call back
- Request history visible to citizen

SMS fallback

- SMS from a verified sender: “[Institution] wishes to contact you”
- Secure link to a web view showing full verified request details
- Citizen calls back from the web view — no app required

The SMS fallback solves the adoption problem. Institutions can adopt e-Contact before every citizen has the app. The app grows organically as citizens encounter the web fallback.

Institution integration: two paths

Web dashboard — for smaller institutions (municipal offices, clinics, smaller agencies)

- No IT integration required
- Employees authenticate via eID or Smart-ID
- Contact requests submitted through web interface

API integration — for larger institutions (banks, utilities, police, Tax Board)

- Single authenticated endpoint
- Integrates into existing CRM or operational systems

- Delivery and response status available via webhook

4. Security

Verified institutions only. Onboarding requires a qualified digital signature from a person with signing authority, cross-checked against the Business Registry. Institution access is revocable immediately.

Verified callback numbers. Callback numbers are registered during institution onboarding. Employees cannot enter numbers outside this set. A compromised employee account cannot redirect citizens to a fraudulent line.

Citizens always initiate the call. e-Contact has no mechanism to connect a citizen to an unregistered number. The citizen calls back on a number they have inspected.

Data minimisation. Citizens are identified by personal code only. No address, email, or financial data is stored. Personal codes are encrypted at rest.

Immutable audit trail. All actions are written to an append-only log. No record can be modified or deleted, including by administrators.

Built on national identity infrastructure. Authentication uses eID, Smart-ID, Mobile-ID, and TARA. No new identity infrastructure is required.

5. Legal Basis and GDPR

The legal basis for processing is legitimate interest under GDPR Article 6(1)(f), specifically fraud prevention, aligned with Estonia's obligations under the Payment Services Directive.

- Only personal code, name, and device notification token are stored per citizen.
- Citizens may delete their account at any time.
- Audit logs are retained for seven years, consistent with Estonian financial communications requirements.
- A Data Processing Agreement is required with every institution prior to onboarding.
- Data breach notification to Andmekaitse Inspektsioon within 72 hours.

6. What This Is Not

e-Contact is not a messaging platform. Institutions send a structured contact request. Citizens respond with a phone call. There is no free-text messaging, no document exchange, no general communication.

e-Contact does not replace existing identity infrastructure. It builds on TARA, Smart-ID, eID, and the Business Registry.

e-Contact is not a consumer communication product. It is state infrastructure for institutional-to-citizen contact only.

e-Contact requires nothing from telecoms operators. It operates at the application layer. No carrier-level changes are needed.

7. Rollout

Phase 1 — Proof of Concept (3–4 weeks)

Working demonstration system: citizen mobile app, institution web dashboard, API integration, full audit trail, and a set of demo institutions using real Estonian registry codes. Authentication simulated for the PoC, designed for straightforward replacement with production TARA integration. Deliverable: a live, demonstrable system. Budget: under €10,000.

Phase 2 — Pilot

Production TARA authentication, security hardening, 3–5 real institutions, citizen app published to app stores, and integration documentation. A contract under €30,000 falls within direct procurement thresholds and requires no formal tender, enabling rapid commissioning once the concept is approved.

Phase 3 — National Standard

Following a successful pilot: legislation or regulation establishing e-Contact, or a compatible open standard, as the required channel for institutional citizen contact. Obligations applied to banks, utilities, police, and public authorities.

8. Why Now

Three conditions are aligned that have not been simultaneously true before:

- **Political urgency.** €29 million in losses in 2025, up threefold from the prior year, with sustained public and political attention. Decision-makers are under pressure to show structural progress, not another awareness campaign.
- **Infrastructure exists.** eID, Smart-ID, TARA, X-Road, and near-universal smartphone penetration mean e-Contact can be built on proven, trusted foundations. No new national infrastructure is required.
- **No competing proposal.** Current debate focuses on payment delays and call-filtering technology. Nobody is proposing to fix the authentication gap at the channel level. That gap is what e-Contact closes.

9. About Codelight

Codelight OÜ is a software development company and subsidiary of Avalanche Laboratory, which has a long track record of delivering Estonian public sector information systems. Codelight focuses on the efficient execution of complex small-to-medium software projects with high delivery capability.

Contact
Henri Parkja
Delivery Manager, Codelight OÜ
henri.parkja@codelight.eu
+372 559 411 04
www.codelight.eu