

WHITEPAPER

Vertrouwen aan de lijn

Hoe telefoonfraude het fundament van organisatiecommunicatie ondermijnt

en waarom gegarandeerde nummeridentiteit de nieuwe standaard wordt

Voor bestuurders en compliance-verantwoordelijken in de

financiële sector · zorgsector · overheid

Gepubliceerd door Jan Niessen

Trusted Voice B.V.

Stadhuisplein 10, Eindhoven · www.trustedvoice.eu

April 2026

1 Managementsamenvatting

Vertrouwen in telefonische communicatie erodeert. Het publieke telefonienetwerk verifieert niet wie belt, en criminelen gebruiken die architecturale kwetsbaarheid op industriële schaal. Voor organisaties in financiële dienstverlening, zorg en overheid is dit niet langer een veiligheidsincident. Het is een compliance-, reputatie- en continuïteitsvraagstuk.

Caller ID spoofing (het vervalsen van het telefoonnummer dat op het display van de ontvanger verschijnt) is uitgegroeid tot een van de meest schadelijke vormen van fraude in Europa. Criminelen misbruiken nummers van banken, ziekenhuizen en overheidsinstanties om burgers en medewerkers te misleiden. Het resultaat is financiële schade, reputatieschade en een snel erosief vertrouwen in telefonische communicatie.

Het probleem is bovendien niet stabiel. Generatieve AI heeft fraude goedkoop en schaalbaar gemaakt: deepfake-stemmen, geautomatiseerde spoofing-infrastructuur en industriële social engineering zijn binnen handbereik gekomen van netwerken die voorheen alleen opportunistisch opereerden. Europol bestempelt caller ID spoofing als een Europese veiligheidsprioriteit met een jaarlijkse schade van circa **€ 850 miljoen**.

De oorzaak ligt in de architectuur. Het publieke telefonienetwerk (PSTN) is decennia geleden gebouwd zonder authenticatiemechanisme. Iedere aangesloten carrier kan elk willekeurig nummer meesturen, en het netwerk accepteert dit zonder verificatie. Moderne reactieve maatregelen, zoals STIR/SHAKEN of klantgedreven verificatie in bank-apps, mitigeren symptomen maar adresseren de onderliggende kwetsbaarheid niet.

De Europese wetgever reageert. De Digital Networks Act (januari 2026) verplicht telecomaanhouders tot geharmoniseerde maatregelen tegen CLI-spoofing. De Cyberbeveiligingswet (NIS2-implementatie, voorjaar 2026) maakt veilige communicatie voor vitale sectoren een wettelijke zorgplicht. DORA en AVG doen daar aanvullende eisen bij. Samen vormen ze een regulatorisch momentum waarin **aantoonbaar veilige communicatie** verschuift van best practice naar harde verplichting.

Trusted Voice lost dit op aan de bron. Niet door filtering achteraf, maar door elk uitgaand gesprek cryptografisch te verifiëren binnen een gesloten, telecomgrade netwerk dat volledig los staat van de publieke infrastructuur. Spoofing is daarbinnen technisch onmogelijk.

KERN VAN DIT WHITEPAPER

Het publieke telefonienetwerk maakt spoofing structureel mogelijk. Dit is niet oplosbaar binnen de bestaande infrastructuur.

Wet- en regelgeving (DNA, NIS2, DORA, AVG) dwingt organisaties tot aantoonbaar veilige communicatie, inclusief persoonlijke aansprakelijkheid van bestuurders.

AI versnelt de dreiging: deepfakes en geautomatiseerde spoofing zetten elke reactieve verdediging onder druk.

Trusted Voice biedt gegarandeerde nummeridentiteit via een gesloten, geauthenticeerd netwerk, aantoonbaar compliant en zonder klantfrictie.

Organisaties die nu handelen lopen voor op regelgeving en bouwen een aantoonbaar compliance-dossier op.

2 Het probleem: telefoonfraude als vertrouwenscrisis

Drie scenario's die dagelijks plaatsvinden

Onderstaande situaties zijn geen theoretische risico's. Ze spelen zich dagelijks af in Nederland en in de rest van Europa.

SCENARIO 1. FINANCIËLE SECTOR

Een bankklant ontvangt een telefoontje. Het nummer op zijn display is identiek aan het nummer op zijn bankpas.

Een vriendelijke 'medewerker' vraagt hem een transactie te bevestigen of zijn betaalpas te beschermen.

De klant vertrouwt het nummer en volgt de instructies op.

De bank heeft niemand gebeld. Het was een fraudeur.

SCENARIO 2. ZORGSECTOR

Een patiënt ontvangt een terugbelverzoek van wat lijkt op de polikliniek van zijn ziekenhuis.

De beller vraagt hem zijn BSN-nummer en verzekeringsgegevens te bevestigen 'voor de administratie'.

De patiënt geeft de informatie, want het nummer klopt.

Het ziekenhuis heeft niet gebeld. De gegevens zijn in handen van criminelen.

SCENARIO 3. OVERHEID

Een burger ontvangt een oproep van 'de gemeente' over een achterstallige belasting.

Er wordt druk uitgeoefend: direct betalen, anders volgen juridische stappen.

Het nummer is het officiële nummer van de gemeente.

De gemeente heeft niet gebeld. De burger heeft geld overgemaakt aan een criminele organisatie.

De omvang van het probleem in cijfers

€ 850M

Wereldwijde jaarlijkse schade door caller ID spoofing (Europol, 2025)

44.500

Meldingen van telefoonfraude in Nederland in de eerste helft van 2025 (Fraudehelpdesk)

€ 26,8M

Financiële schade in Nederland in de eerste zes maanden van 2025 (Fraudehelpdesk)

64%

Aandeel van fraudemeldingen dat verloopt via telefoon of sms (Europol)

Achter deze cijfers gaan persoonlijke drama's schuil: ouderen die spaargeld kwijtraken, patiënten wier medische gegevens worden misbruikt, burgers die het vertrouwen in overheidscontact verliezen. Voor organisaties heeft dit een directe keerzijde: de reputatieschade van *'jullie nummer is misbruikt'* is aanzienlijk en structureel, ook al heeft de organisatie zelf technisch niets misdaan.

AI maakt spoofing schaalbaar

De dreiging is niet statisch. Waar caller ID spoofing tien jaar geleden vooral een opportunistische tactiek was, is het inmiddels een geautomatiseerd crimineel verdienmodel. Generatieve AI verlaagt de drempel drastisch: stemmen van bekenden of medewerkers kunnen op basis van enkele seconden audio worden nageemaakt, scripts worden gepersonaliseerd met publiek beschikbare data, en deepfake-technologie maakt realistische one-to-one misleiding mogelijk op schaal.

Spoofing exploiteert kwetsbaarheden in het publieke telefonienetwerk.

Caller ID spoofing wordt gebruikt om vertrouwde organisaties en personen te imiteren.

AI-deepfakes zetten slachtoffers op het verkeerde been en ontfutselen gevoelige informatie.

Verkregen informatie wordt gebruikt om fraude en financiële diefstal uit te voeren.

Het resultaat: aanvallen worden goedkoper, sneller en gericht. Reactieve afweer, gebaseerd op patroonherkenning en klantalertheid, schaal niet mee.

3 Waarom dit nu urgent is: het regulatoire momentum

Voor organisaties in de financiële sector, zorg en overheid is caller ID spoofing niet alleen een veiligheidskwestie. Het is een compliancevraagstuk dat snel concreter wordt. De wet- en regelgeving beweegt zich in snel tempo in de richting van aantoonbaar veilige communicatie.

Digital Networks Act (DNA): EU, januari 2026

Op 21 januari 2026 publiceerde de Europese Commissie haar voorstel voor de Digital Networks Act, de meest ingrijpende herziening van het Europese telecomrecht in jaren. Als Verordening is de DNA rechtstreeks van toepassing in alle 27 lidstaten, zonder nationale omzetting. De DNA introduceert geharmoniseerde maatregelen tegen CLI-spoofing (calling line spoofing vgl. caller ID spoofing), phishing, smishing en vishing. BEREC (het Europese regelgeversorgaan) wordt belast met richtlijnen voor technische en juridische maatregelen om eindgebruikers effectief te beschermen. De Commissie krijgt bovendien expliciete bevoegdheid aanvullende maatregelen te nemen.

Cyberbeveiligingswet / NIS2: voorjaar 2026

De Cyberbeveiligingswet, de Nederlandse implementatie van de Europese NIS2-richtlijn, treedt in werking in het voorjaar van 2026. Voor organisaties in vitale sectoren (waaronder financiële dienstverlening, gezondheidszorg en overheid) wordt digitale weerbaarheid een wettelijke zorgplicht. Bestuurders worden persoonlijk verantwoordelijk. **Communicatiebeveiliging valt expliciet binnen de reikwijdte van NIS2.**

DORA: Digital Operational Resilience Act

DORA stelt voor financiële instellingen eisen aan de operationele weerbaarheid van digitale systemen en communicatieprocessen. De betrouwbaarheid van uitgaande communicatiekanalen valt onder de reikwijdte van DORA-compliance. Trusted Voice is operationeel ontworpen binnen een dedicated netwerk dat gecontroleerde routing en veerkrachtige communicatieprocessen borgt.

Europol: spoofing als Europese veiligheidsprioriteit

In oktober 2025 publiceerde Europol een position paper over caller ID spoofing, gebaseerd op input van 23 EU-lidstaten. De conclusie: de bestaande situatie is niet langer houdbaar voor de Europese openbare veiligheid. Europol roept op tot EU-brede technische standaarden en een neutraal internationaal traceback-systeem.

REGULATOIRE TIJDLIJN

Okt. 2025	Europol position paper: caller ID spoofing als Europese veiligheidsprioriteit
Jan. 2026	Digital Networks Act voorgesteld: geharmoniseerde maatregelen CLI-spoofing
Voorjaar 2026	Cyberbeveiligingswet (NIS2) van kracht: communicatiebeveiliging als zorgplicht
2026+	BEREC-richtlijnen voor anti-spoofingmaatregelen verwacht
2027 tot 2028	DNA van kracht na goedkeuring Parlement en Raad

De vraag is niet óf regulering op dit terrein komt, maar hoe snel, en of uw organisatie dan al klaar is.

4 Hoe caller ID spoofing werkt, en waarom het zo moeilijk te bestrijden is

Het publieke telefonienetwerk: gebouwd zonder identiteitscheck

Het PSTN is decennia geleden ontworpen met één doel: gesprekken tot stand brengen. Authenticatie van de beller was geen vereiste. Sindsdien is de wereld volledig veranderd, maar de basisarchitectuur van het telefonienetwerk niet.

Wanneer een gesprek wordt opgebouwd, stuurt de beller een nummerreeks mee als Calling Line Identification (CLI). Het netwerk toont dit nummer bij de ontvanger. Er is geen enkel verificatieproces. Iedere carrier wereldwijd kan ieder nummer meesturen, en het netwerk accepteert dit. De opkomst van VoIP heeft dit verder vergemakkelijkt: veel platformen laten gebruikers hun eigen caller ID instellen zonder strikte validatie.

Waarom bestaande maatregelen onvoldoende zijn

- STIR/SHAKEN werkt alleen op specifieke IP-gebaseerde netwerksegmenten. Zodra een gesprek via legacy-apparatuur of internationale routes loopt, wordt authenticatie-informatie verwijderd. In Europa is de implementatie ver achtergebleven.
- Filtering en blocklists kunnen patronen herkennen maar kunnen de caller ID zelf niet authenticeren. Nieuwe nummers en technieken omzeilen filters continu.
- Klantgerichte verificatie ('check de oproep' in een bank-app) is reactief en plaatst de bewijslast bij de eindgebruiker. Er is geen authenticatie aan de bron.
- Nummer-blokkering door carriers is een achtervolgingsspel: criminelen wisselen voortdurend van nummer.

De conclusie is hard maar onvermijdelijk: zolang het PSTN nummers accepteert zonder verificatie, zal spoofing mogelijk blijven. De kwetsbaarheid zit in de architectuur van het netwerk zelf, en die is niet te repareren binnen de bestaande infrastructuur.

5 De drie sectoren die het hardst geraakt worden

Financiële sector: reputatie, aansprakelijkheid en klantvertrouwen

Banken en financiële instellingen zijn het meest gefrekwenteerde doelwit van caller ID spoofing. Hun nummers zijn bekend, hun naamsbekendheid is groot en de financiële motivatie voor criminelen is direct.

De impact is meervoudig. Naast directe klantschade draagt de bank de reputatieschade: *'jullie nummer is misbruikt om mijn moeder op te lichten'* beschadigt de relatie blijvend, ook al heeft de bank technisch niets misdaan. Callcenters worden overspoeld met bezorgde klanten die vragen of een gesprek echt was.

Onder PSD2/PSD3 en de discussie over zorgplicht bij betaalfraude groeit de druk op banken om aantoonbaar actie te ondernemen. DNB en AFM kijken met toenemende aandacht naar de kwaliteit van klantcommunicatieprocessen.

Vraag voor uw organisatie: *weet u vandaag zeker dat elk uitgaand klantgesprek van uw instelling aantoonbaar authentiek is?*

Zorgsector: patiëntveiligheid en AVG-compliance

In de zorgsector raakt spoofing aan iets fundamenteelers dan geld: patiëntveiligheid en medische vertrouwelijkheid. Zorgverleners bellen patiënten met gevoelige informatie over uitslagen, medicatie, behandelplannen en psychische begeleiding.

Wanneer een fraudeur een zorginstelling nabootst zijn de risico's direct. Patiënten kunnen medicatie-instructies van een fraudeur opvolgen. BSN-nummers en medische informatie worden ontfoetseld. In GGZ-context kunnen kwetsbare patiënten worden gemanipuleerd door iemand die zich voordoeft als behandelaar.

De AVG stelt hoge eisen aan de beveiliging van bijzondere persoonsgegevens, waaronder gezondheidsgegevens. NIS2 maakt communicatiebeveiliging expliciet onderdeel van de wettelijke zorgplicht voor zorginstellingen. Bestuurders worden persoonlijk verantwoordelijk.

Vraag voor uw organisatie: *kunt u garanderen dat wanneer uw polikliniek een patiënt belt, die patiënt zeker weet dat het uw organisatie is?*

Overheid: burgersvertrouwen en institutionele geloofwaardigheid

Overheidsinstanties worden het meest nagebootst bij caller ID spoofing. De Belastingdienst, DUO, gemeenten en de politie: hun nummers zijn openbaar en hun gezag maakt burgers ontvankelijk voor druk. Criminelen spelen hierop in met urgentie en dreiging.

De schade is tweeledig: financiële schade bij burgers én institutionele schade bij de overheid zelf. Burgers die overheidsoproepen structureel wantrouwen, negeren meldingen. Dit ondermijnt de uitvoerbaarheid van overheidstaken direct.

De Wet Modernisering Elektronisch Bestuurlijk Verkeer (Wmebv, van kracht per 1 januari 2026) maakt veilige digitale communicatie met burgers tot een wettelijk recht. De beleidsgeest is eenduidig: de overheid moet aantoonbaar veilig communiceren. Spoofing van overheidsnummers staat hier haaks op.

Vraag voor uw organisatie: *weten burgers zeker dat wanneer uw organisatie belt, het ook echt uw organisatie is?*

6 Wat een structurele oplossing vereist

Gegeven de fundamentele kwetsbaarheid van het publieke telefonienetwerk zijn er vijf eisen waaraan een echte oplossing moet voldoen.

1. **Authenticatie aan de bron, niet filtering achteraf**

De enige manier om spoofing structureel uit te sluiten is het verifiëren van de belleridentiteit vóórdat het gesprek het netwerk ingaat. Filtering achteraf is per definitie reactief.

2. **Onafhankelijkheid van het publieke netwerk**

Zolang communicatie via het PSTN loopt, is het blootgesteld aan de architecturale kwetsbaarheid van dat netwerk. Een echte oplossing opereert in een gesloten omgeving los van de publieke infrastructuur.

3. **Gesloten toegang met gecontroleerde identiteit**

Toegang tot het netwerk moet beperkt zijn tot geverifieerde deelnemers. In een gesloten netwerk is elke deelnemer bekend en geverifieerd. Anonieme toegang bestaat niet.

4. **Bewijsbaarheid en audittrail voor compliance**

Organisaties moeten kunnen aantonen dat hun communicatie veilig is. Een volledige audittrail van elk gesprek (wie heeft wanneer gebeld, geverifieerd door het netwerk) is een compliance-vereiste.

5. **Schaalbaarheid zonder klantfrictie**

Een oplossing die aanpassingen vereist aan de kant van de ontvanger zal nooit op schaal werken. De oplossing moet transparant zijn voor de ontvanger: het gesprek komt aan als een normaal telefoongesprek, maar dan geverifieerd.

7 Gegarandeerde nummeridentiteit: Trusted Voice

Trusted Voice is gebouwd rondom een enkelvoudige overtuiging: elke organisatie verdient de zekerheid dat haar bellers zijn wie ze zeggen te zijn, en haar ontvangers die zekerheid ook.

Hoe het werkt

Trusted Voice opereert als een gesloten, telecomgrade netwerk volledig los van de publieke telefonie-infrastructuur. Elke deelnemer (elke medewerker, elk systeem dat namens de organisatie belt) is geverifieerd en geauthenticeerd bij toegang tot het netwerk.

Wanneer een gesprek wordt opgebouwd, verifieert Trusted Voice encrypted of de beller is wie hij claimt te zijn, vóórdat het gesprek wordt doorgezet. Een gesprek dat deze verificatie niet doorstaat, wordt niet geaccepteerd. Er is geen tussenliggende stap waarop een fraudeur zich kan plaatsen.

Het Trusted Network. Architectuur op hoofdlijnen

Klanten via bank-app

CIAM-geverifieerd
(customer identity provider)

Trusted Private Network

Telecomgrade voice
cryptografisch geverifieerd

Medewerkers op kantoor of remote

IAM/IGA-verbonden
(enterprise identity)

Het Trusted Network koppelt CIAM-geverifieerde klanten en IAM/IGA-verbonden medewerkers via een gesloten voice-netwerk. Het publieke PSTN ligt buiten het pad; authenticatie is ingebakken in het netwerk zelf.

Waarom dit fundamenteel anders is

- Elke uitgaande oproep is encrypted geverifieerd voor verbinding.
- Toegang tot het netwerk vereist geauthentiseerde identiteit.
- Geen afhankelijkheid van het publieke netwerk of diens kwetsbaarheden.
- Volledige audittrail van elk gesprek voor compliance-doeleinden.
- Geen aanpassingen vereist aan de kant van de ontvanger.
- API-integratie met bestaande systemen, geen app nodig bij de klant.

Vergelijking: publiek netwerk vs. Trusted Voice

Kenmerk	Publiek netwerk (PSTN)	Trusted Voice
Identiteit geverifieerd	Nee	Ja (encrypted)
Spoofing mogelijk	Ja, triviaal eenvoudig	Nee, technisch onmogelijk
NIS2 / DORA / AVG	Niet aantoonbaar	Aantoonbaar compliant
Audittrail	Nee	Ja, volledig gelogd
Klant hoeft geen verificatie te doen	Nee, vertrouwen ontbreekt	Ja, netwerk garandeert identiteit
Integratie	N.v.t.	API, geen app bij ontvanger

Technische eigenschappen

- Privacy-verhoogde belmiddelen met encrypted voice- en signaleringsverkeer.
- Ontworpen conform NIS2- en DORA-eisen (zie hoofdstuk 11 voor de artikelsgewijze mapping).
- Integratie met uw bestaande customer identity provider (CIAM).
- Integratie met uw IGA- en enterprise identity provider.
- SDK's voor private-label iOS- en Android-experiences bij organisaties die een in-app-ervaring verkiezen.

8 Benchmark: reactief versus proactief

Een vergelijking van de huidige Europese markt laat twee fundamenteel verschillende benaderingen zien. De meeste Europese banken leunen op reactieve mechanismen; wereldwijd tekent zich een verschuiving af richting proactieve oplossingen. Trusted Voice sluit aan bij de tweede categorie, en brengt deze naar Europa.

Reactieve oplossingen in Europese banken

Voorbeelden uit de markt zijn 'check je gesprek'-widgets in bank-apps, in-app-meldingen met de strekking *'u praat met een adviseur van uw bank'*, en hotlines die klanten vragen zelf terug te bellen. Deze oplossingen delen drie eigenschappen: de oproep loopt via het publieke netwerk, de klant moet zelf verifiëren in de app, en de verificatie is klantgedreven. Het resultaat is een extra stap voor de klant, frictie op het moment dat de klant iets wil gedaan krijgen, en een structurele afhankelijkheid van alertheid bij de eindgebruiker.

Proactieve oplossingen wereldwijd

In Singapore (OCBC), het Verenigd Koninkrijk (Revolut Audio) en enkele Aziatische markten vinden oproepen pre-verified plaats binnen de bankcontext zelf. De oproep is natively onderdeel van de bank-app, de klant ziet dat de organisatie geverifieerd is nog voordat hij opneemt, en er is geen extra handeling vereist. Minder frictie, meer vertrouwen, maar vandaag nog beperkt tot regionale implementaties en fragmentarisch ingericht.

WAT TRUSTED VOICE TOEVOEGT

Trusted Voice biedt een Europese, telecomgrade, cross-institutionele infrastructuur voor proactieve nummeridentiteit. Niet een feature binnen één bank-app, maar een gedeeld vertrouwensnetwerk waar meerdere organisaties op aansluiten, met behoud van hun eigen klantbeleving via API of SDK.

9 Waarde per stakeholder

De impact van aantoonbaar veilige communicatie verschilt per stakeholder. Drie perspectieven maken dat concreet.

Klanten, patiënten, burgers

Probleem → Onzekerheid of een binnenkomende oproep daadwerkelijk afkomstig is van de organisatie. Dit leidt tot verlies van vertrouwen, het negeren van legitieme oproepen en grotere blootstelling aan fraude.

Waarde → Heldere, realtime verificatie dat de oproep authentiek is. Vertrouwen hersteld, ervaring eenvoudiger en veiliger.

Medewerkers en callcenter-operators

Probleem → Tijdverlies aan het verifiëren van klanten, het bewijzen van de eigen legitimiteit, en het omleiden naar secundaire kanalen vanwege wantrouwen op het voice-kanaal.

Waarde → Wederzijds vertrouwen voordat het gesprek begint. Minder frictie, snellere en effectievere klantinteracties.

De organisatie zelf

Probleem → Oplopende financiële schade, toezichthoudersdruk en reputatieschade door spoofing-gedreven fraude en dalend klantvertrouwen in het voice-kanaal.

Waarde → Proactieve fraudepreventie, sterker compliance-dossier en een voice-kanaal dat klantvertrouwen versterkt in plaats van ondermijnt.

10 Implementatie: eenvoudiger dan verwacht

Een van de meest gehoorde bezwaren bij het bespreken van een nieuwe communicatie-infrastructuur is de veronderstelde complexiteit van implementatie. In de praktijk is het tegendeel waar.

Geen aanpassingen bij de ontvanger

De ontvanger (de klant van de bank, de patiënt van het ziekenhuis, de burger) hoeft niets te doen. Geen app te installeren, geen account aan te maken, geen gedragsverandering. Het gesprek komt aan op een regulier telefoonnummer, maar dan geverifieerd.

Integratie via API

Trusted Voice sluit aan op bestaande systemen via een eenvoudige API-integratie. Callcentersoftware, CRM-systemen en communicatieplatformen kunnen worden gekoppeld zonder infrastructurele herziening. De implementatietijd is weken, geen maanden.

Optionele in-app-beleving via SDK

Organisaties die een proactieve, in-app-beleving willen aanbieden (bijvoorbeeld een duidelijke, zichtbare verificatie van de oproep binnen hun mobiele applicatie) kunnen hiervoor de Trusted Voice SDK inzetten. In-app caller-identificatie werkt aan beide zijden, integreert met de bestaande klantbeleving, voorziet in call-ratings, opnames en transcripties, en biedt duidelijke visuele indicatie dat de beller is geverifieerd.

Het implementatiepad

1. Intakegesprek

Analyse van huidige communicatieprocessen en spoofingrisico's. Vaststellen van de kritieke belstromen (klant, backoffice, callcenter).

2. Technische inventarisatie

Koppeling met bestaande systemen (CRM, callcenter, identity provider) in kaart brengen en scope afbakenen.

3. Pilotimplementatie

Selecte groep medewerkers of afdeling bellen volledig geverifieerd. Kwalitatieve en kwantitatieve evaluatie.

4. Uitrol

Organisatiebrede implementatie met ondersteuning vanuit Trusted Voice en change-management voor medewerkers en klantbeleving.

5. Live

Elk uitgaand gesprek geverifieerd. Audittrail actief. Compliance aantoonbaar richting toezichthouder en bestuur.

11 Compliance by design: DORA en NIS2 artikelsgewijs

Trusted Voice is ontworpen zodat de architectuur zelf voldoet aan de centrale eisen die DORA en NIS2 stellen aan ICT-risicomanagement en communicatiebeveiliging. Onderstaand een artikelsgewijze mapping die u kunt meenemen in uw compliance-dossier.

1. Encryptie (voice + signalering)

DORA

Art. 9(2). Verplicht ICT-risicomaatregelen inclusief beleid, procedures en tools voor de veiligheid van netwerken en informatiesystemen. Encryptie is expliciet benoemd in de RTS/ITS-richtlijnen.

Art. 10(2)(d). Verplicht bescherming van data *in transit* en *at rest*.

NIS2

Art. 21(2)(a). Verplicht beleid op risicoanalyse en informatiesysteembeveiliging.

Art. 21(2)(e). Noemt expliciet het gebruik van encryptie.

2. Identiteitsbeheer en MFA

DORA

Art. 9(4)(a). Vereist sterke authenticatiemechanismen en toegangscontrole voor ICT-systemen.

Art. 10(1). Dekt het voorkomen van onrechtmatige toegang tot ICT-middelen.

NIS2

Art. 21(2)(b). Verplicht beleid op toegangscontrole en assetmanagement.

Art. 21(2)(g). Noemt expliciet multi-factor-authenticatie of continue authenticatie.

3. Realtime monitoring en alerts

DORA

Art. 10(2)(b). Vereist continue monitoring van ICT-systemen.

Art. 15(1). Verplicht detectie van afwijkende activiteiten en incidenten.

Art. 17. Vereist incidentclassificatie en rapportage.

NIS2

Art. 21(2)(c). Vereist incident handling-capaciteiten.

Art. 23. Legt strikte meldtermijnen op (24-uurs early warning).

4. Leveranciersverantwoordelijkheid

DORA

Art. 28. Volledig raamwerk voor ICT third-party risk management.

Art. 30. Contractuele eisen aan ICT-leveranciers.

Art. 31. Toezicht op kritieke ICT-third-party providers.

NIS2

Art. 21(2)(e). Vereist supply chain-beveiliging inclusief leveranciers en dienstverleners.

Art. 22. Expliciete verantwoordelijkheid voor risico's vanuit leveranciers.

De operationele architectuur van Trusted Voice sluit op elk van deze punten aan. Persoonsgegevens en gespreksmetadata worden behandeld conform AVG met strikte controle over elke interactie. Toegangs-, identiteitsvalidatie- en loggingprocessen volgen ISO 27001-principes voor veilige en auditeerbare operaties.

12 Conclusie: van reactief naar aantoonbaar veilig

Het publieke telefonienetwerk zal niet worden gerepareerd. De architecturale kwetsbaarheid die caller ID spoofing mogelijk maakt, is inherent aan de decennia-oude infrastructuur. Europol zegt het expliciet: de situatie is niet langer houdbaar voor de Europese openbare veiligheid.

Tegelijkertijd beweegt de wet- en regelgeving snel. De Digital Networks Act, de Cyberbeveiligingswet, DORA: ze sturen alle drie in dezelfde richting: communicatiebeveiliging is een aantoonbare verplichting, geen inspanningsverplichting.

Generatieve AI voegt een derde dimensie toe. Deepfakes en geautomatiseerde spoofing-infrastructuur zetten iedere reactieve afweer onder druk en verhogen de schaal waarop fraude kan worden uitgevoerd. Wachten op branche-brede filtering is geen strategie.

Organisaties die nu handelen doen drie dingen tegelijk: ze beschermen hun klanten, patiënten en burgers tegen een reëel en groeiend risico, ze verlagen reputatie- en bestuurdersaansprakelijkheid, en ze bouwen een compliance-dossier op dat vóór de curve ligt wanneer regelgeving bindend wordt.

Trusted Voice biedt de structurele oplossing: gegarandeerde nummeridentiteit, aan de bron, in een gesloten netwerk dat volledig los staat van de publieke infrastructuur. Geen filters. Geen reactieve maatregelen. Geen aanpassingen bij de ontvanger. Spoofing is technisch uitgesloten: niet bemoeilijkt, maar onmogelijk gemaakt.

“Vertrouwen mag nooit een vraagteken zijn. Verifieer elk gesprek voordat het begint.”

DE KEUZE DIE VOOR U LIGT

Wachten tot regelgeving bindend is, en dan achterlopen op de verwachtingen van toezichthouders, pers en klanten.

Nu handelen: uw communicatie aantoonbaar beveiligen, uw klanten beschermen, uw compliance-dossier opbouwen.

Elke maand die u wacht, groeit het risico. Elke maand die u handelt, groeit uw voorsprong.

13 Over Trusted Voice

Trusted Voice B.V. is een Europese tech-organisatie gespecialiseerd in veilige, geverifieerde spraakcommunicatie voor organisaties in de financiële sector, zorg en overheid. Wij opereren vanuit Eindhoven, met oprichters in Nederland en België, en werken aan een Europa waar elke organisatie kan garanderen dat haar bellers zijn wie ze zeggen te zijn.

Ons team combineert diepgaande expertise in identity, banking, telecom en cybersecurity. De oplossing is gebouwd door practitioners die de regulatoire, operationele en security-realiteit van Europese financiële instellingen begrijpen. Trusted Voice is commercieel beschikbaar en inzetbaar via API-integratie met bestaande communicatiesystemen, of via SDK voor organisaties die een in-app-beleving verkiezen.

Neem contact op

Website: www.trustedvoice.eu

Adres: Stadhuisplein 10, Eindhoven

Wilt u weten wat veilig bellen voor uw organisatie betekent? Wij denken graag met u mee, vrijblijvend en zonder verplichtingen.

© 2026 Trusted Voice B.V. Alle rechten voorbehouden.

Dit whitepaper is uitsluitend bedoeld voor informatieve doeleinden en gebaseerd op publiek beschikbare bronnen, waaronder publicaties van Europol, de Europese Commissie en de Fraudehelpdesk, en Trusted Voice eigen documentatie.