

TRAMIGO

TRACKING & CONNECTIVITY



TRAMIGO MCPTT COMPLETE SOLUTION

info@tramigo.com

THE FIRST COMPLETE MCPTT ECOSYSTEM

Built and designed for demanding environments, the high-performance Tramigo Mission-Critical-Push-To-Talk (MCPTT) device is the latest technology of combined hardware, software and connectivity solutions.

HARDWARE

Robust easy to use hardware



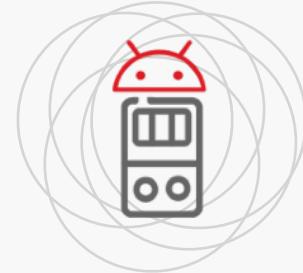
DUAL SIM

Comes with Tramigo eSIM and local plastic SIM option



ANDROID SOFTWARE

Android-based high-performance PTT software



WEB-ADMIN

MCPTT Enterprise Web-admin license



CONTROL CENTER

PC software for Command and Control Center



DISPATCHER APP

Tramigo App based Mobile Dispatcher



+358 50 475 46 06



info@tramigo.com

TRAMIGO

HOW WE DEFINE MCPTT

THE LOWEST LATENCY
& MOUTH TO EAR



HIGH AUDIO
QUALITY



ENCRYPTION AS256
DATA SECURITY



MULTI-NETWORK
CONNECTIVITY



MISSION CRITICAL PUSH-TO-TALK

M C P T T C O M P L E T E S O L U T I O N

KEY BENEFITS

Improved controlled communication results in higher performance and cost savings



HIGHEST VOICE QUALITY



ENCRYPTED COMMUNICATION



RELIABLE & SECURE



EXTREMELY SCALABLE SOLUTION



UNLIMITED REGIONAL COVERAGE



MULTI-NETWORK CONNECTIVITY



+358 50 475 46 06



info@tramigo.com

TRAMIGO

MCPTT-SUPERIOR VOICE QUALITY

- Server's internal latency <50ms
- Delay in LTE-network: 300-600 milliseconds
- Delays in 3G network:
 - First call: ~ 2 seconds:
 - Subsequent calls: ~1 second
- Delays in 2G (GPRS) network: (from "mouth to ear")
 - First call: ~3 seconds
 - Subsequent calls: ~2 seconds

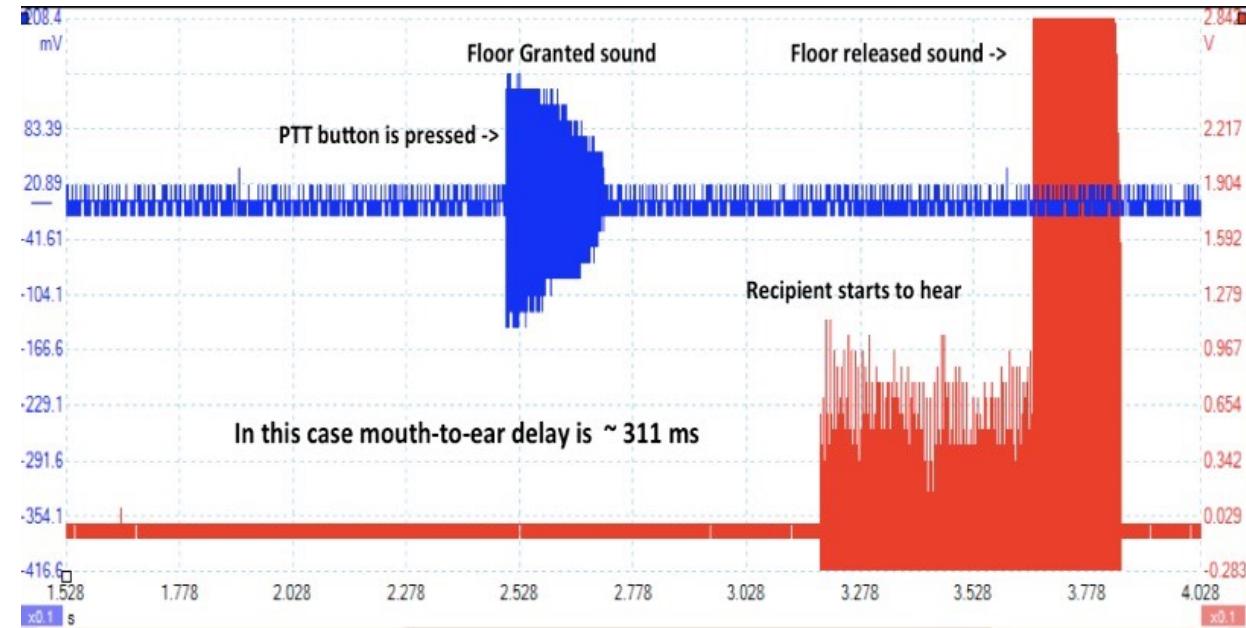


Image above: measurements in LTE-network, from mouth to ear in *LTE-network: 300-600ms

Delays over Wifi are same level as over LTE

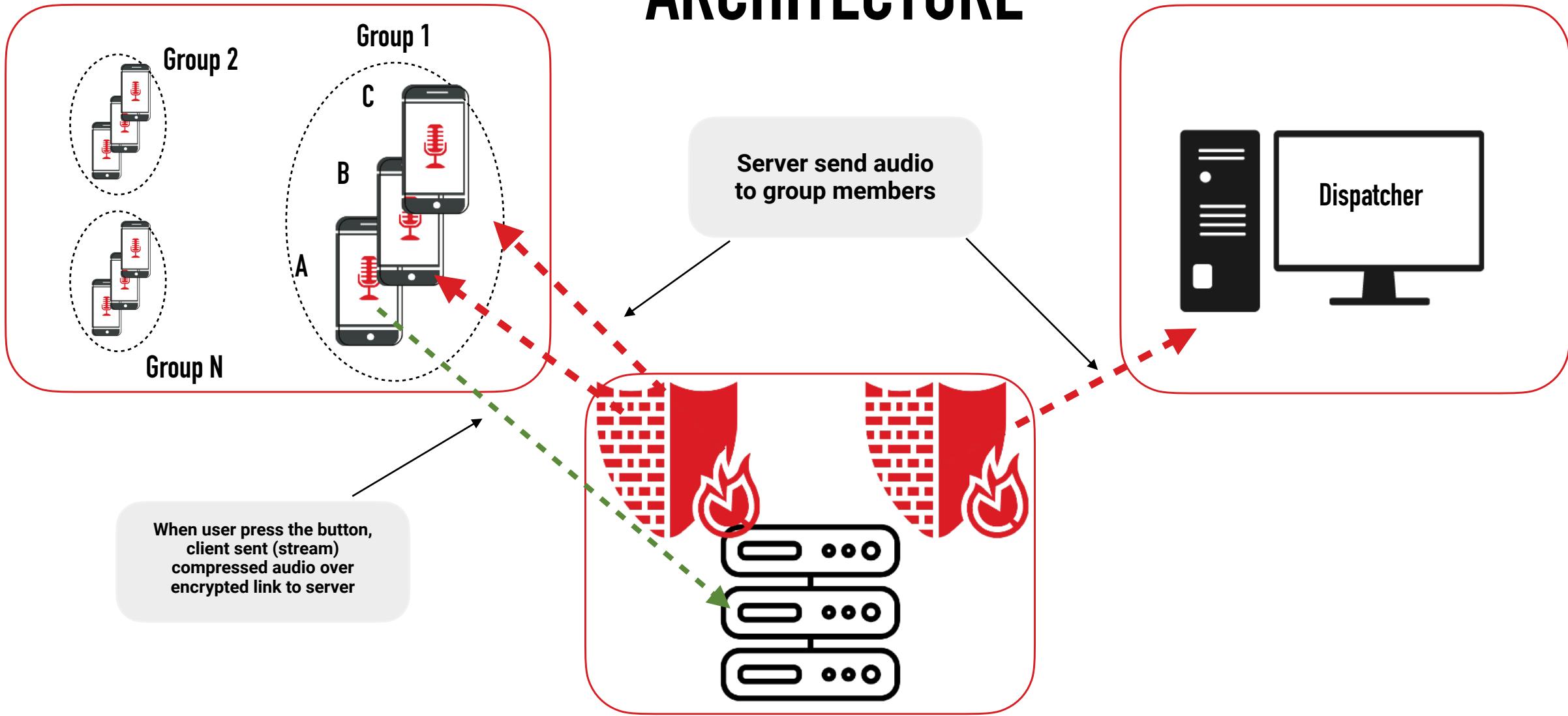
(Note that setup was non-ideal: no QoS and server outside of core-network which increase delay remarkably)

*Measured in Telia LTE-network in Finland, server located outside of core-network without QoS setup

ARCHITECTURE

MOBILE NETWORK

INTRANET / CONTROL ROOM



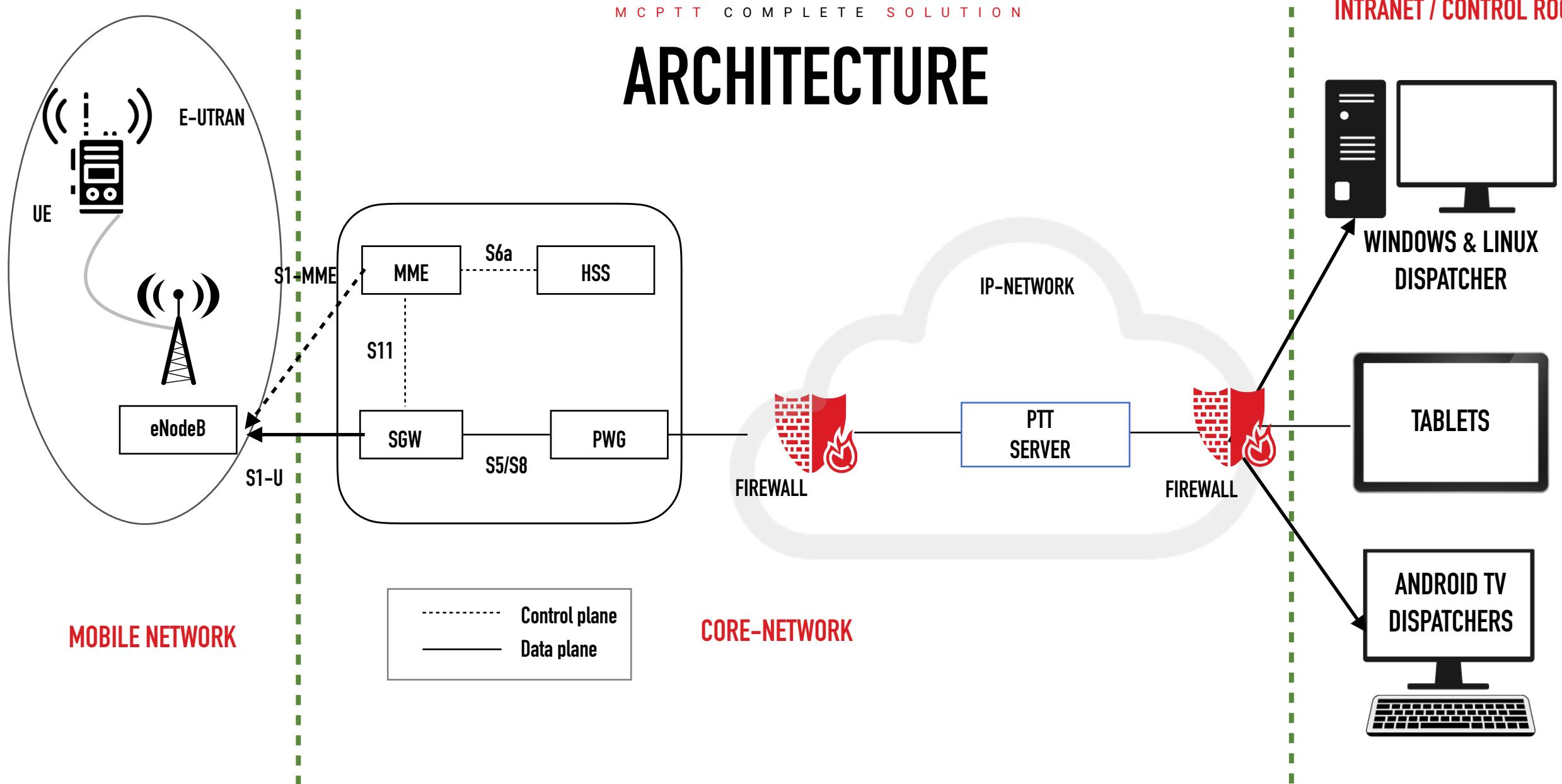
+358 50 475 46 06



info@tramigo.com

TRAMIGO

ARCHITECTURE



MCPTT-1 TECHNICAL DATA

Tramigo MCPTT-1 is a rugged device with an easy and simple interface.



TECHNICAL DATA

| | | | |
|-----------------------|-------------------|-----------------------------------------|---------------------|
| Model | G21 | Wi-Fi | Support 802.11b,g/n |
| GSM | Band 2/3/8 | Charging Mode | Micro USB |
| WCDMA | Band 1/5/8 | FM Radio | Yes |
| CDMA | Evdo Rev.A 800MHZ | Operating Temperature | -20°C ~ +50°C |
| TD-SCDMA | Band 34/39 | Waterproof / Dustproof Grade | IP54 |
| TDD-LTE | Band 38/39/40/41 | RAM | 512M |
| FDD-LTE | Band1/3 | ROM | 4G |
| Screen Size | 1.77 SPI | Project | MSM8909 |
| LCD Resolution | 128*160 | Switch Machine Animation | Custom |
| Bluetooth | Bluetooth 4.0 | Desktop Layout | Menu |
| GPS | Support | Physical Key Function Definition | Support |
| BeiDou | Support | Multipath MIC Switching | Yes |

MCPTT SALES PACKAGE

Sales package contains:

- MCPTT-1 device
- Standard accessories:
 - ▶ Antenna
 - ▶ Charger
 - ▶ Belt Clip
 - ▶ Battery

Optional accessories

- ▶ Desktop charger



+358 50 475 46 06



info@tramigo.com

TRAMIGO

MCPTT COMPLETE SOLUTION

SEAMLESS MULTI-NETWORK CONNECTIVITY

Tramigo multi-network connectivity ensures that your MCPTT device will always connect to the best available network in each country making the coverage better and stronger, especially in remote areas.



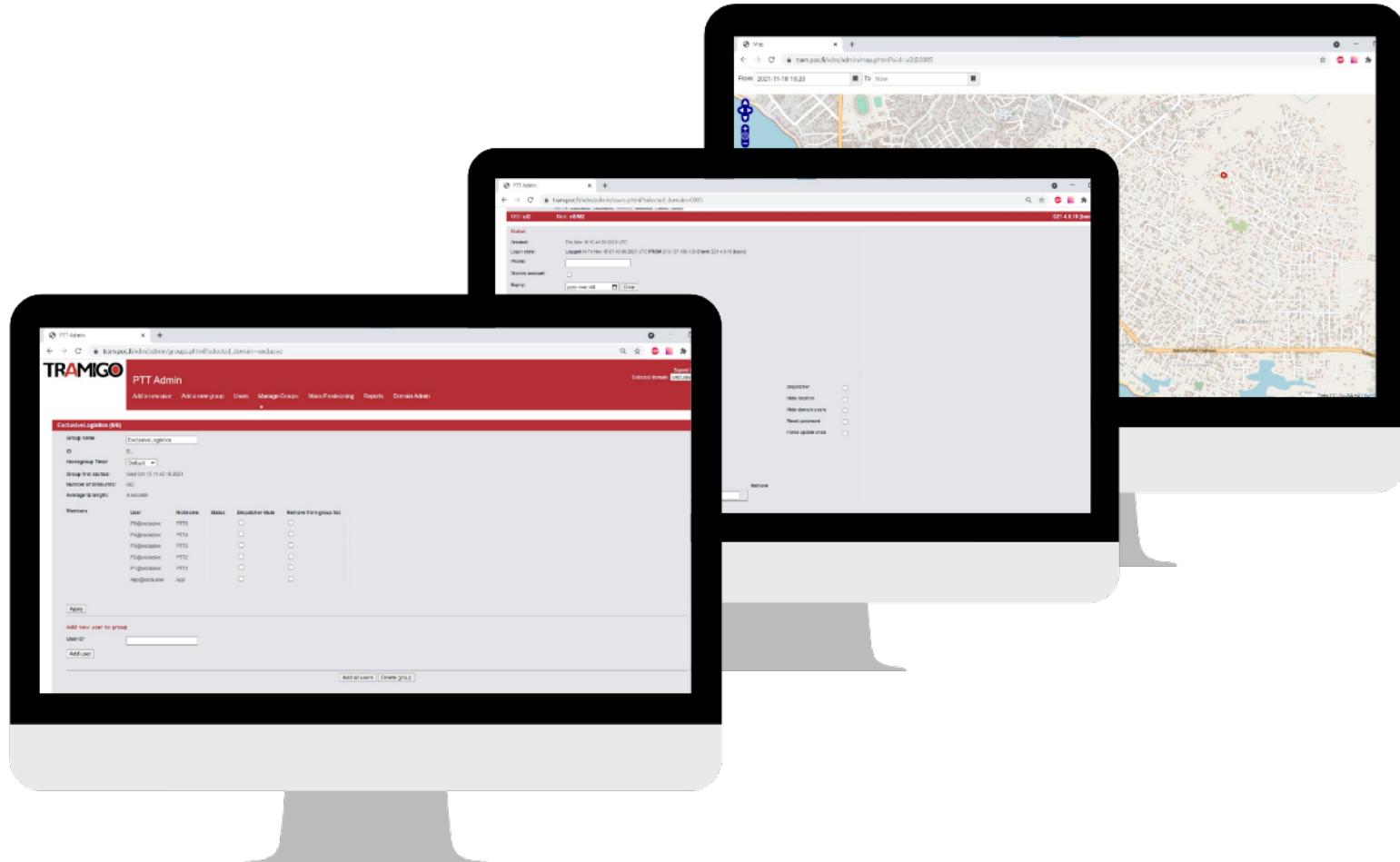
TRAMIGO MCPTT WORKS IN 4G, 3G, & 2G NETWORKS



MCPTT SOFTWARE SOLUTIONS

WEB-ADMIN

User friendly Web-Admin interface allows creating, adding and removing users and groups. Users and groups can be also created by uploading pre-filled excel file. All admin-functions are available over SOAP-protocol which allow to integrate PTT-management to company CRM and other business services.



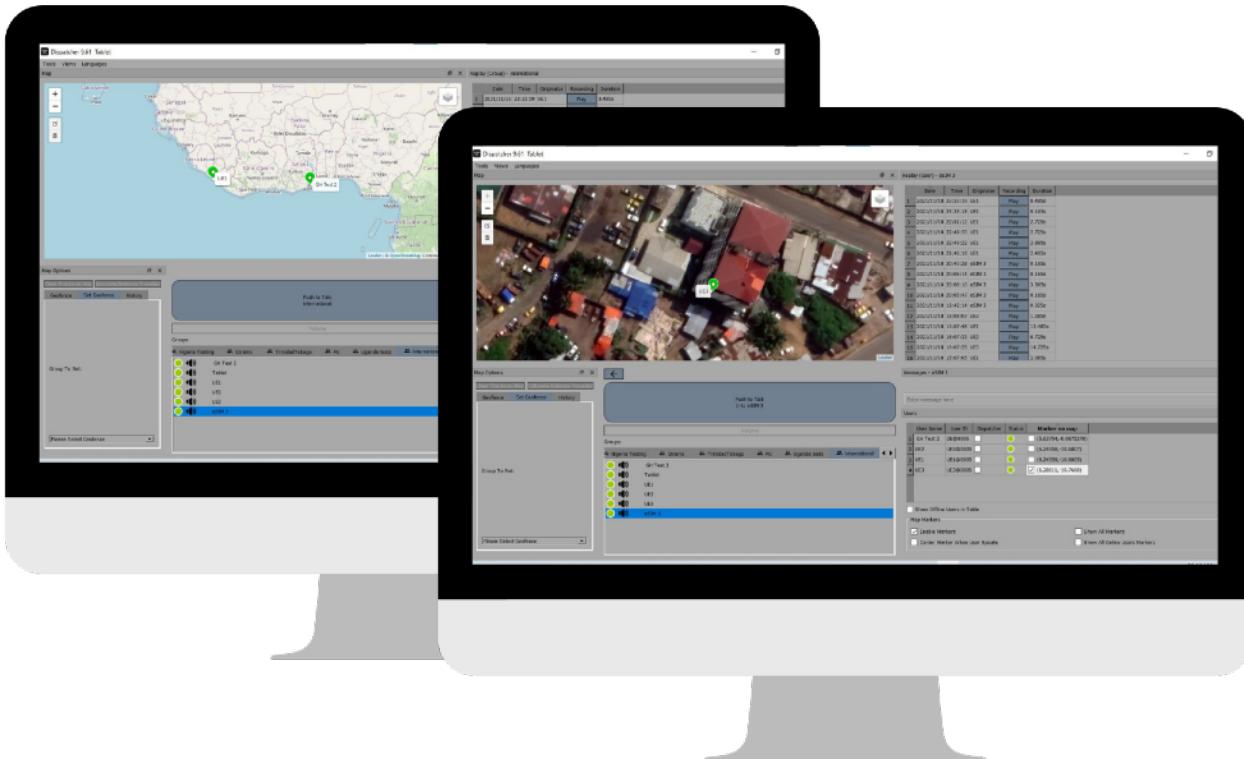
+358 50 475 46 06



info@tramigo.com

TRAMIGO

MCPTT SOFTWARE SOLUTIONS



CONTROL CENTER

The Windows PC MCPTT Control Center gives the possibility to monitor, track devices location, and communicate directly to devices. Audio in/out and text-input can be integrated using standard devices and connections, including wired and Bluetooth. Windows Dispatcher support 1-8 monitors allowing flexible scalability from entry-level single-display system to 8-screen video-wall.



+358 50 475 46 06



info@tramigo.com

TRAMIGO

MCPTT SOFTWARE SOLUTIONS

MCPTT-MOBILE APP DISPATCHER

Mobile App dispatcher is compatible with Android and designed to allow communication with small groups and control center and track devices location as well. Mobile app dispatcher also allows you to request for a call back from the devices.



PRIVACY FEATURES

Privacy is about strengthening the user's identity and data. One of the well-known privacy regulations is GDPR by the European Union (General Data Protection Regulation). To ensure intrinsic privacy and legislation compliance:

- PTT-service is role-based.
- Enduser's real identity is not stored in the PTT-system at all.
- Endpoints and groups are identified by numbers, and optionally referred to in user-interfaces by nicknames or screen names, for example, such as Radio 1 or Dispatcher.
- Endpoint is either a radio-like phone communicating over mobile data or Wi-Fi, or tablet or desktop-computer.
- Endpoint identification consists of two parts: user and domain. Although identifications can be freely chosen from any alphanumeric characters, the recommended naming convention is to use 5-digit user-id, 4-digit domain and 3-digit group ID. **For example, user with screen name Radio 1 may have id 12345@6789**
- Device location can be optionally reported to the back-end, where it is stored for tracking, but as handsets are identified by ID codes ,user's personal identity or location are not compromised. When application is uninstalled, all its data is removed as well.



+358 50 475 46 06



info@tramigo.com

TRAMIGO

SECURITY FEATURES

Tramigo ensures that all data used is safeguarded:

- All PTT-system data is encrypted at application-level between the client and the server, using TLS 1.2 with 2048 bit keys, and cipher configured. For example AES256, CHACHA20 or other per customer preferences. Both CHACHA20 and AES256 are considered as quantum-safe.
- The server is encrypted using open source encryption gnutls3
- User's passwords in the database are encrypted with bcrypt. CHACHA20, AES256 and bcrypt are considered as quantum-safe.

Available ciphers:

ECDHE-ECDSA-AES256-GCM-SHA384, ECDHE-RSA-AES256-GCM-SHA384, ECDHE-ECDSA-CHACHA20-POLY1305, ECDHE-RSA-CHACHA20-POLY1305, ECDHE-ECDSA-AES128-GCM-SHA256, ECDHE-RSA-AES128-GCM-SHA256, ECDHE-ECDSA-AES256-SHA384, ECDHE-RSA-AES256-SHA384, ECDHE-ECDSA-AES128-SHA256, ECDHE-RSA-AES128-SHA256