

SMART ROUTER WITH VPN SUPPORT

Advantage of integration

- Full integration of the technology into a smart router with VPN support
- Direct connection between the Router and the Tetrapol radio-terminal using a single cable
- All the safety factors (keys, certificates, settings) are transferred through the Tetrapol network
- Encryption and VPN management at the hardware device level
- Possibility to use the built-in GPS in the router for the AVL applications through Tetrapol without any other hardware
- Possibility to use several operators, alternatively or simultaneously
- Possibility to use satellite links (with added HW)
- Possibility to use Tetrapol data functions for backup connection
- Easy installation and setup
- Centralized device management
- Centralized license management

Mobile station

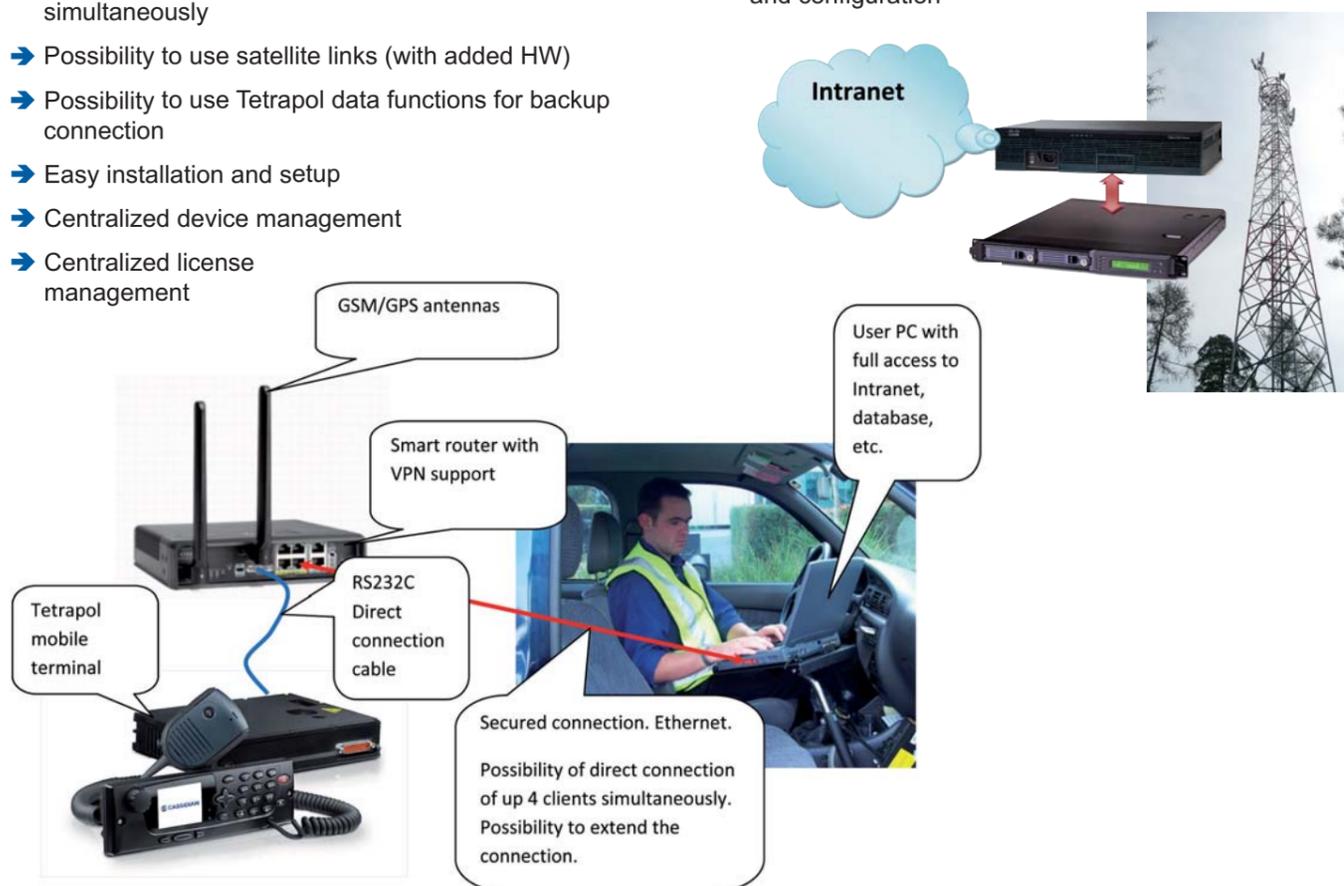
The mobile station consists of:

- Smart router with VPN support, equipped with GSM modems, GPS and the PMD application
- Tetrapol terminal
- Cable

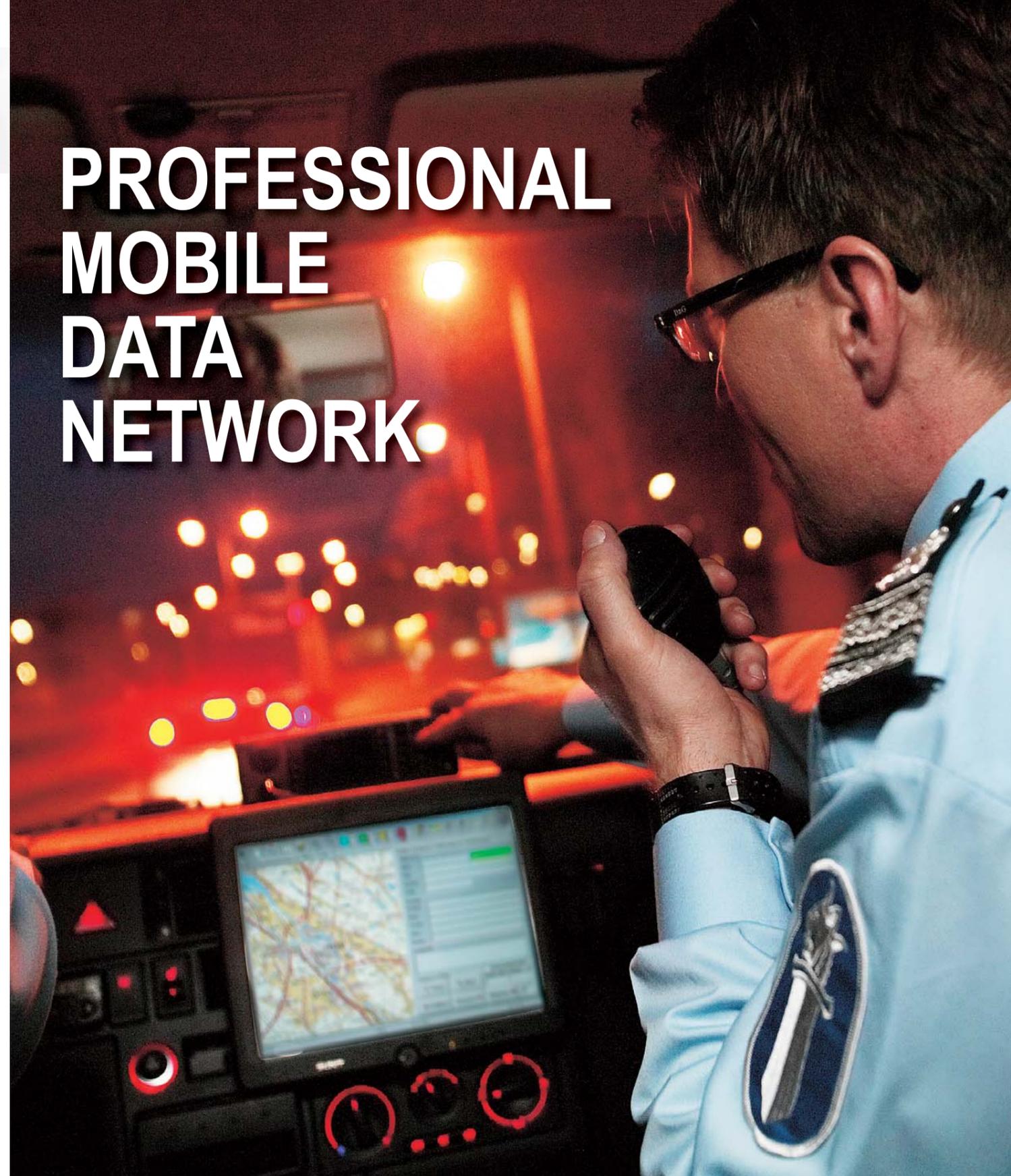
Central working station

The central working station consists of:

- Smart router with VPN support
- Server for maintenance of database licences, devices and configuration



PROFESSIONAL MOBILE DATA NETWORK



Professional mobile data Network

Communication for your safety

The PMD Network makes your intranet securely mobile

FEATURES

Advantage over existing solutions

- Possibility to establish new mobile data services with large data volume transmission support
- Possibility of full remote intranet access
- Noticeable acceleration of system responses to database queries
- Noticeable increase in overall capacity of mobile data services system
- Optimization and reduction of overall network traffic in the Tetrapol network
- Noticeable increase of overall system throughput (speed increase)
- Noticeable reduction of response time (waiting time to response)
- Reliable feedback (clear records (logs) of transmission requests, processing and results)

Supported applications for remote data access system

- Applications for large-volume tactical information transmissions, e.g. maps, site plan, photos, event descriptions etc.
- Continuous monitoring of terminal activities including operating status, data transmissions, and location
- Coordination and bulk distribution of information for large teams
- Direct remote intranet access

Solution attributes

- Data protection according to the Tetrapol network security level
- Transmission speed dependent on maximum allowed commercial mobile data transfer transmission speed (24 Mbit/s as of now)
- Full compatibility with Windows CE, Windows Mobile, Linux and Android platforms
- Full compatibility with the new MDT standard (Cassidian)
- Tested with all types of Tetrapol network terminals

Technology

This patented technology combines secured and broadband communication channels, creating a single secured broadband communication device.

- The system creates a secured virtual private network within the high-speed network environment
- All information related to the secure connection deployment, namely keys and certificates for VPN access, are transmitted by the Tetrapol network

The system is immune to broadband network drop-out (disaster, out of coverage, etc.). In this case, the system transmits all data over a secured channel, and/or allows a new query from the user with better accuracy and smaller data volume.

Solution

1. The remote client computer is connected to the gate via a standard network interface
2. At the time the first client application requires access to the intranet, the gateway sends a request to open the connection and to gain an access certificate through the Tetrapol network
3. A complementary gate, located in the intranet network, receives a request from the Tetrapol network and generates a single-way key for VPN connection
4. Keys, along with the relevant certificates, are transmitted through the Tetrapol network and forwarded to the remote gateway
5. The remote gateway opens a VPN connection
6. The client application has a full access to the intranet

Security

The validity of the single-way keys is limited. The keys are automatically updated via the Tetrapol network after their expiration.

In case of longer connection inactivity, the VPN network is automatically closed and the validity of the keys expires.

This architecture uses a secured and independent communication network for the transfer of keys and encryption management. It is absolutely impossible to break the security by attacking the encryption management. The encryption level entirely satisfies military requirements.

