TMS
TETRA MANAGEMENT SUITE

Product Data Sheet

MENTURA DIMO™ Mobile Device Management

- **Can you enforce the settings, policies and use of your smartphones?**
- **Do you know what was done to your data device while it was not in use?**
- **Do you know what SW is installed on it? Are you sure?**
- **Can you still trust it and let it access your sensitive data?**

The future of public safety communications is hybrid. We will continue to use narrowband (TETRA, P25) systems as mission critical voice, but organisations will increasingly employ smartphones, tablets and similar broadband data devices for field use. These devices will utilise both dedicated and commercial mobile networks for communications, and they will also need to be integrated in the same operations with narrowband systems.

Introduction of smartphone platforms creates new requirements for secure management of the devices. As the devices are by definition open platforms (just like the old systems are by definition closed and sealed), the device profiles, permissions, policies etc need to be centrally managed to protect the organisation from cyber-threats (varying from viruses, random hacking to advanced persistent threats).

The DIMO™ MDM is a solution from Mentura Group, which allows central management of all communication devices and user based security profiles of the organisation. DIMO™ allows you to keep your operations secure.

DIMO™ links a user to authorised devices and manages the device profiles centrally.

Benefits:

- Enforcement of device profiles, e.g. required applications, non-allowed applications, required security setting check etc.
- Control and limit of actions allowed for users (changing settings, installing apps etc.).
- Devices that are not compliant to the policies are not allowed to access sensitive data. (rooted or jail broken devices are not allowed access to data)
- User-device specific security policies (authorised user with specific settings active gets in).
- Remote lock and wipe of devices
- Central management of device inventory
- Possibility to pair smartphones with TETRA and P25 devices for user security.
- Management of SIM cards and devices
- Single Platform for managing both TETRA and 3G/4G devices with link to CRM and billing.
- Integrated with Mentura TNIB™ CRM platform.

Supported platforms:
Windows 2008 Server
Linux
Smartphone platforms:
IOS
Android (2.2-4.x). Samsung-A, HTC-A
Windows Mobile, 8

About Mentura Group
Mentura Group Ltd provides technology solutions that help PMR user organisations to improve the efficiency and security of their operations.

Mentura Group's customers include network operators, PMR user organisations and system integrators.

Mentura Group is a member of the TETRA and Critical Communications Association (TCCA).

Contact Information:
Mentura Group Oy
Keilaranta 1
02150 Espoo
Finland

TEL: +358 4244 801
FAX: +358 4244 80800
sales@menturagroup.com
www.menturagroup.com

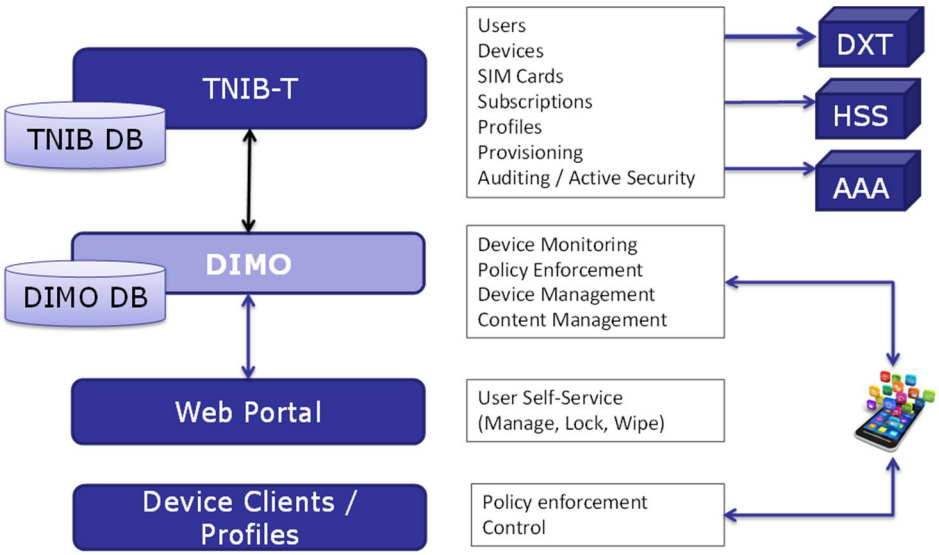
Doc id: 30283/8

mentura

TMS
TETRA MANAGEMENT SUITE

MENTURA DIMO™ Feature Summary

Feature	Details
Application Management	Inventory, install, configure, update, remove, start and stop applications, enterprise app market, black/whitelist for apps
Settings Management	Configure Access Points (3G, 4G, WiFi) and VPN, exchange account management, functionality restrictions.
Security Management	Device lock, selective wipe, support for antivirus SW, install certificates, root/jailbreak detection, data encryption, cross platform backup and restore.
Policy Management	Automated policy enforcement for required applications, certificates and security settings, device tagging, policy violation monitoring.
Monitoring and troubleshooting	Alerts, diagnostics, data usage counters, device auto-discovery, roaming control, remote control.
Delivery and integration	Scheduled, reoccurring and automatic tasks over-the-air, Exchange and Active Directory.
Platform Specifics	Prevent iCloud, extended Samsung Android Support, ActiveSync Tasks for WP, SCEP support for iOS.
Subscription management	Subscription alerting and disabling if SIM card removed from device, device status synch with subscription.



Used together with TNIB-T, DIMO provides an additional layer of security for professional organisations. SIM card and subscription management is linked to management of the device itself, detecting violations to security policy inside and outside of the dedicated network.

Smartphone Platforms Supported:

- Android (2.2 -> 4.x)
- HTC-A (Android enhanced support for HTC devices)
- Samsung-A (Android enhanced support for Samsung Devices)
- IOS MDM (IOS 4.0-8.x)
- WP8 (Windows Phone 8.x)
- Legacy support (available but not maintained):
  - S60 2nd,S80,UIQ2,UIQ3,Android 1.6-2.1,S60 3rd, S60 5th, Symbian 3, WM5, WM6, WP-EAS, iOS OTA

Doc id: 30283/8

TETRA