TEOREM

Secure voice and data system for:

- Mobile public networks (GSM/UMTS)
- Fixed public networks (PSTN, ISDN, VoIP)
- Military and governmental networks

High grade security:

- Red/black separation
- Tempest compliant
- Hardware crypto processor

Centralised online security management:

- Secure key and certificate management
- Secure remote management

TEOREM TELEPHONE CHARACTERISTICS

NETWORKS AND CONNECTIVITY

- GSM Quadri-band GSM, GPRS, EDGE, UMTS.
- Bluetooth wireless or USB cord link to PSTN, ISDN, or VoIP network access base.

FEATURES

- 2" 262000-colour TFT main screen.
- 1" 65000-colour STN security screen.
- Talk time up to 4 hours.
- Standby time up to 100 hours.

SERVICES

- STANAG 4591 (2.4 Kbps) and G.728 (16 Kbps) vocoders.
- 3000 phonebook entries.
- Phonebook synchronisation from a PC.
- Call list (dialled, received, missed calls).
- Built-in hands-free.
- Multilingual GUI.
- Clock, alarm, vibrating alert.
- Airplane mode (to disable the wireless features).

SECURITY

- High-grade encryption of voice and data.
- Strong user authentication with PIN code and token.
- Distant user cryptographic authentication.
- Indication of call: secure / regular phone calls.
- Trusted screen for call security level and distant user name display.
- TEMPEST AMSG 720B.
- Tamper-proof design.

FEATURES OF THE MANAGEMENT INFRASTRUCTURE

KEY GENERATION FACILITY

- Generation of all keys and user secrets from a hardware security module.
- Keys and certificates downloaded to equipment using DS-101 protocol.

CERTIFICATION FACILITY

- X.509 V3 certificate management.
- LDAP directory.
- Cross-certification (interconnection of certification authority).

REGISTRATION AND MANAGEMENT FACILITY

- Centralised management of more than 20,000 secure phones.
- Remote rekeying and security configuration.
- Remote telecom configuration.
- Remote software update.
- Remote zeroisation of compromised secure phone.
- Scalable and distributed management architecture.

THALES

TEOREM

Fixed and cellular secured telephony solution for Governmental and Defence use

THALES

Securing your future

TEOREM SECURE TELEPHONE

TEOREM

> **MOBILE PHONE USE**

> **CORDLESS PHONE USE**
> with PSTN, ISDN and VoIP networks access base

> **CORDED PHONE USE**
> with PSTN, ISDN and VoIP networks access base

> **DATA TRANSFERT FROM A PC**
> Encrypting Modem Function for supported networks

Main screen

USB port for PC or headset connection

Authentication hologram

Volume keys

Trusted screen: security level and user name display

John Matthews
Secured call
High grade

Secure / clear call indicator lights

Easy to use keyboard

Authentication token socket

Management Infrastructure

KEY GENERATION FACILITY
• Key Generation Station
• Initialisation Station

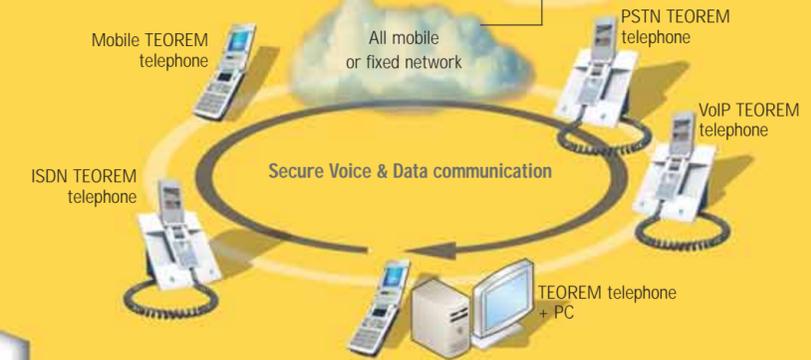Certification, publication and distribution of certificates

CERTIFICATION FACILITY
• Certification Authority
• Directory Station

Key generation and cryptographic initialisation of TEOREM telephones

REGISTRATION AND MANAGEMENT FACILITY
• Registration Authority
• Remote Management Station

User registration Management and supervision of TEOREM telephones

Mobile TEOREM telephone

All mobile or fixed network

PSTN TEOREM telephone

ISDN TEOREM telephone

Secure Voice & Data communication

VoIP TEOREM telephone

TEOREM telephone + PC

The Management Infrastructure facilitates and optimises use of TEOREM telephones.
It provides a large set of security and functional managing tools.
The Management Infrastructure is scalable in order to adapt the deployment of TEOREM telephones to the organisation.

KEY GENERATION FACILITY
• Key generation and management.
• Off-line red key handling.
• End-to-end black key distribution to TEOREM telephones.

CERTIFICATION FACILITY
• Certificate Lifecycle Management.
• Certificates made available in a directory.
• Cross-certification for interoperability with other organisations' TEOREM telephones.

REGISTRATION AND MANAGEMENT FACILITY
• Management and supervision of TEOREM telephones.
• Remote and automatic operations:
  - User registration.
  - Rekeying.
  - Supervision and zeroisation.
  - Distribution of compromised key list.
  - Phonebook distribution.
  - Non-sensitive software update.