SECURE COMMUNICATIONS

TMSDEF

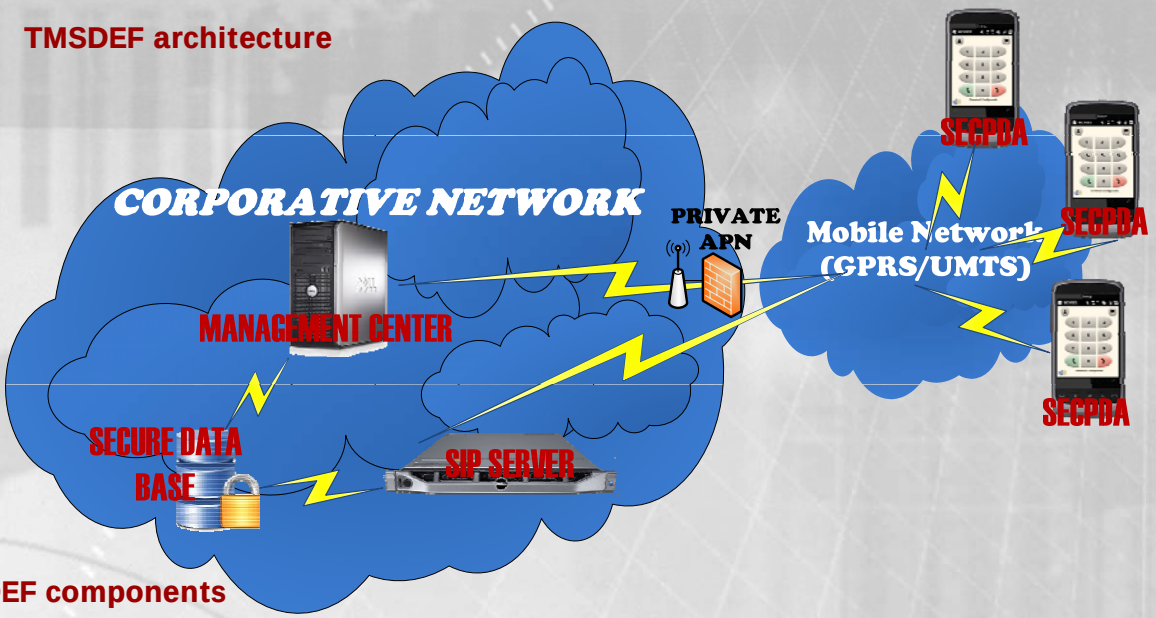
GENERAL DESCRIPTION

TMSDEF (Secure Mobile Device for Defense Agencies) is a secure communication system (voice and data) for smartphones over data networks. It is implemented using the secure protocol **SCIP** (Secure Communication Interoperability Protocol), which offers a point-to-point security channel between devices. The classification level of the system is up to NATO RESTRICTED.

NATO SCIP is an international standard for secure voice and data communications, which allows member countries to exchange classified information between heterogeneous systems.
It provides:

- **Network independent mechanism to establish and maintain a secure communication channel.**
- **Unique session key.**
- **X.509 certificates for authentication.**
- **Interoperability with other systems.**

TMSDEF architecture



TMSDEF components

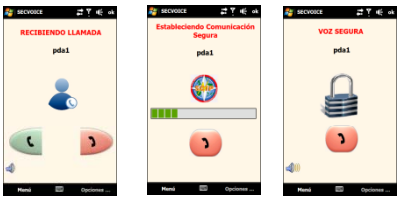
- **SECPDA: mobile device with secure voice software SECVOICE.**
- **SECSERVER**
  - **SipSecServer: SIP communication server.**
  - **Management Center: support and management of the system, mobile devices and cryptography information.**
  - **SecDatabase: secure database.**

Communication architecture

- **SIP (Session Initiation Protocol) signaling: IETF-defined protocol used for controlling communication sessions over the Internet Protocol (IP).**
- **Point-to-point RTP SCIP encrypted data streams.**
- **Call establishment: 3-4 s.**
- **Delay: 1-2 s.**
- **Vocoders: MELPe and G-729D**

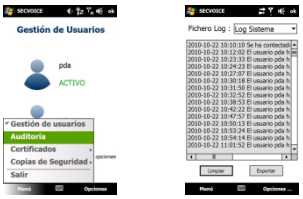
SECVOICE – User mode

- Secure voice calls over the SCIP protocol.
- User-friendly interface.
- Contact list with presence service.
- Call registry.
- System-integrated errors and missed calls notifications.
- Compatible with traditional mobile phone calls.
- Remote cryptography operations.
- Sensitive data zeroization mechanism.
- Software update functionality.



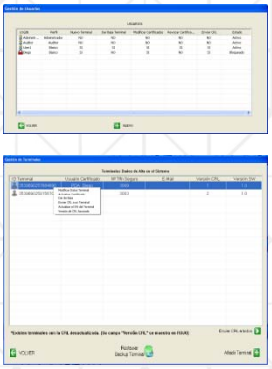
SECVOICE – Admin mode

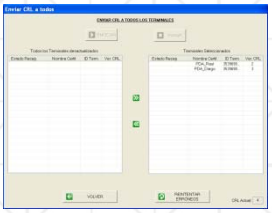
- Users management:
  - Block/unblock users.
  - Modify users login/password.
- Sip settings.
- Log functionality.
- Application data backup functionality.
- Sensitive data zeroization mechanism.
- Software update functionality.

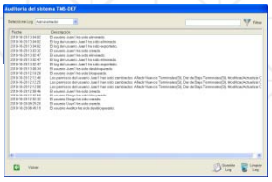


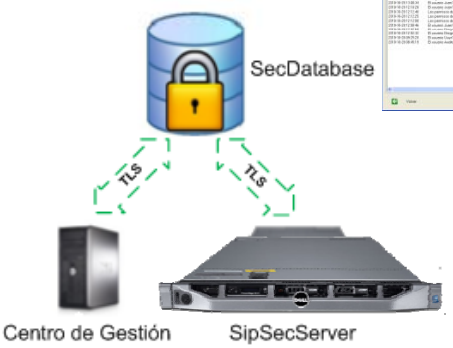
SECSERVER components

- Management Centre
  - Cryptography data management.
  - Users and mobile devices management.
  - Log functionality.
  - SipSecServer remote management.
  - SecDatabase remote connection via TLS.
  - Mobile devices remote connection using SCIP:
    - Remote zeroization.
    - Remote Certificates and CRL updates.
- SIPSecServer
  - SIP signaling.
  - DIGEST-MD5 authentication.
  - Presence service.
  - SecDatabase remote connection via TLS.
- SecDatabase
  - Directory server.
  - Security:
    - Encrypted data.
    - ACLs (Access Control Lists).
    - TLS secure connections.









OFICINAS CENTRALES:
Santa Leonor, 65 Edif. A 1ª Planta
Parque Empresarial Avalon
28037 Madrid, ESPAÑA
Teléfono: +34 916 617 161 Fax: +34 916 619 840

FABRICA:
Fudre, 18
13300 Valdepeñas
Ciudad Real, ESPAÑA
Teléfono: +34 926 347 830 Fax: +34 926 312 896

MINISTERIO DE DEFENSA

SECRETARÍA DE ESTADO DE DEFENSA

DIRECCIÓN GENERAL DE INFRAESTRUCTURA

SUBDIRECCIÓN GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES