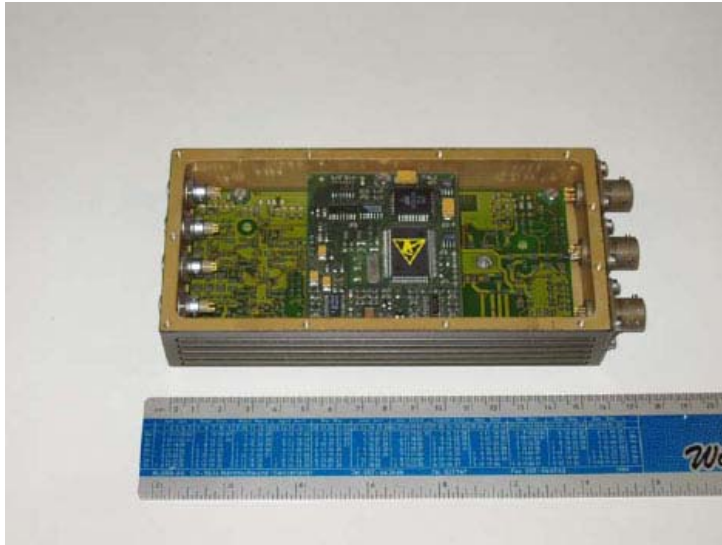


Voice Data Encryption AT Crypt One



Example: Customised Add-on Unit

- AT Crypt One-01 Add-on Unit for voice and data encryption
- AT Crypt One-02 Encryption Board for radio integration
- AT Crypt-03 Handset with integrated voice encryption

Add-on Unit Features

- Voice and Data encryption
- Remote Commands
- Universal Radio Interface
- MIL and STANAG waveforms
- Custom defined waveforms and protocols
- Applicable up to MACH-2 platforms
- Protected Over-the-Air re-programming and key exchange.

Very high security

- Evaluated AES encryption algorithm
- Interoperability with other systems
- Automatic resynchronisation
- Adaptive channel equalisation
- Excellent speaker recognition
- User exchangeable key generator
- Customised encryption algorithm
- No political considerations

We offer new Voice and Data Encryption Module AT Crypt One for highly secure voice and data communication over analog narrow-band radio channels. Complex digital signal processing techniques in conjunction with state-of-the-art encryption techniques ensures excellent speaker recognition with highest security.

The AT CRYPT ONE is a high security voice encryption system which is mainly used for authorities, governmental agencies, police and military or paramilitary. AES encryption algorithm providing the highest security needed for such user groups. From a practical standpoint, it is not susceptible to attack by eaves-droppers, etc. or by using current crypto analytical methods. Customised encryption algorithms or number generators can be integrated if required.

The AT Crypt One Voice Encryption System can be implemented into *already existing* radio networks for end-to-end encryption without the necessity of changing radio communication infrastructures. The AT Crypt One system guarantees a secure and economic solution for high security applications without compromise.

The AT Crypt One is compatible with complex radio networks, such as multiple repeaters and simulcast systems. No wider bandwidth is needed for encrypted mode. For relay operation, no special repeater is required.

User defined encryption algorithms and addressing schemes can be integrated. Different waveforms according to STANAG or MIL can be downloaded for interoperability. The user can select standard waveform and protocol custom defined or standardised procedures by local settings to ensure interoperability between different user groups. This flexibility is given by using modern FPGA technologies. The AT Crypt One can be used for V/UHF

as well as for HF SSB radio channels. Channel typical behaviours like fading and Doppler effects are compensated automatically. MACH2 versions for airborne platforms are available.

The high security encryption technique applied for the AT Crypt One is not affected by any political considerations. This leads to a very high level of security, an absolute must for military theatre deployment, for special police task force units or other governmental security organs.

AT Crypt One-01 Add-on units

to be connected to existing tactical radios.

AT Crypt One-02 Module versions

can be retrofitted in already existing radios.

AT Crypt One-03 Handsets

with integrated voice encryption to be connected to most commonly used tactical radios.

Technical specifications

Ciphering Technique:	AES-128/256 in conjunction with RSA and DH authentication process using integrated high security Smart Cards for authentication and remote key exchange.
Cryptographic data:	Key length up to 256 bits
Key storage	10 selectable communication keys stored in battery buffered encrypted key banks containing up to 250 keys.
Key Loading	Key-fill Device or with protected Smart-Card Reader or over the air, highly secured by RSA-1024 and DH protocol.
Key and Parameter generation:	Menu driven process with Crypto Management System or with Key Programming Unit.
Operating mode:	- Voice - Data - Remote Commands
Emergency:	Local or remote emergency erase/kill
Coding delay (Voice):	Low end to end delay
Mode control (Voice):	Clear/Encrypted: Clear voice over-ride; Automatic reception of encrypted signal.
OTAR	Key selection (10 out of 250 key) over air using highly protected commands.
Synchronisation	Automatic re-synchronisation after channel disturbance, Late-entry techniques
Transmission channel requirements:	Bandwidth: 250 - 3000 Hz, adaptable Automatic link-offset compensation
Audio Interface:	H-189/250/350 handsets
Communication interface:	Universal radio interface
Data Interface:	USB, V.24 (RS232)

Diagnostics:	BITE Fail safe operation
Environmental conditions:	MIL-STD-810F
Temperature:	Operating: -20 to +60°C (extended temperature range on request) Storage -40 to +85°C
Humidity:	95% RH (+60°C), non-condensing

Tightness:	Submersible to 1 meter
Vibration:	1 g/5 to 200 Hz random
Shock:	25 g/11 ms
EMI	Within MIL-STD-461B, Class A3
Power requirements:	9 to 36 VDC
Power consumption:	3.5 W
Size and weight:	160 x 32 x 75 mm; weight 0.6 kg
Options:	../010 Anti-Spoofing
	../020 Selective Call (Analog or Digital Ident)
	../030 Local keypad entry and LCD display
	../040 Remote access to database (RADIS System)
	../050 Remote Commands
	../090 Various customised Interfaces, e.g. digitised video
	../110 Key Programming Unit
	../120 Smart Card Reader
	../130 Protected Over-the-Air programming
	../140 Encrypted GPS information
	../150 Frequency Hopping

Voice Encryption | Data Encryptor | HF VHF Military Tactical Radios

<http://hf-encryption.at-communication.com/en/at/voice-encryption-unit.html>