



AGT Launching Second Generation Tri-band CryptoPhone in the Middle East

Gulf market main target for mobile phone with trustworthy voice encryption based on published source platform

Dubai / Cairo -- June 2004. Advanced German Technology (AGT), a leading supplier of premier security products, solutions and services to the IT and telecommunications industries, today announced the launch of the second generation of encrypted published source-based GSM mobile phones in the Middle East and North Africa. The GSMK manufactured CryptoPhone 200 is the first end-to-end encrypted tri-band (900/1800/1900 MHz) phone based on published source code and can operate world-wide on any GSM network with data call facilities.

The CryptoPhone 200 is a response to the increased need for secure and trustworthy communications in an environment where wireless interception devices are inexpensive and common and often used in an unprincipled way. AGT Managing Director, Anas Chbib points out; "It is not only governments, police, military and security forces that have a need for secure communication, the private sector is finding out to its chagrin, that unscrupulous businessmen will do anything to gain even the slightest edge on their competitors."

With the proliferation of wireless communication systems, the market for encrypted communications devices has increased. Experience has shown that if the encryption is ineffective or weak, it is easily overcome. As the risk and cost of sensitive data in the wrong hands grows, the need for a dependable means to protect such information becomes vital.

The CryptoPhone comes with the securest algorithms available today - but it is not a bulky piece of hardware. It looks like any normal PDA mobile phone and accessories are easily available on the open market. CryptoPhone products that can place secure calls via ISDN or analog

landlines and satellite phone systems like Thuraya are also available.

The full source code of the CryptoPhone is published and can be reviewed independently to ensure there is no weak encryption and no backdoors. In contrast, "proprietary - algorithms" and encryption systems that are not fully verifiable by the buyer can contain weak encryption, backdoors and other defects.

Chbib stresses the importance of the published source code; "This is not a 'black-box' piece of equipment. No matter how high the overall quality of the device, if the code is not published and cannot be independently verified, the device simply is not secure. In Germany, there is no compulsory government intervention in the development and sales of security and encryption products."

The CryptoPhone 200 ensures voice communication privacy with the following specifications:

- Strongest and most secure algorithms available (AES256 and Twofish)
- 4096 bit Diffie-Hellman key exchange with SHA256 hash function.
- Readout-hash based key authentication.
- 256 bit effective session key length.
- Encryption session key is destroyed as soon as the call ends
- Source code available online for independent security assessments.
- Also supports unencrypted calls, unencrypted SMS, address book, calendar, etc
- Operates in any 900/1800/1900 GSM network that provides data call facilities.
- 150-hour standby time.
- Secured talk time up to three hours, thirty minutes.
- Unsecured talk time up to four hours.