KIV-7

Embeddable KG-84 COMSEC Module

The KIV-7 is a compact miniaturized embeddable version of the American military KG-84 encryption device, developed in the mid-1990s by AlliedSignal Corporation (USA), to meet the growing demand for secure data communication links. The KIV-7 was manufactured by Mykotronx in the USA (now: SafeNet), as a commercial-off-the-shelf (COTS) product.

The image on the right shows a typical KIV-7HS unit. It has the same form-factor as a 5¼" CD-ROM player, allowing it to be built into a free expansion bay of a standard personal computer.

The initial KIV-7 unit was suitable for use on digital serial lines with data rates between 50 b/s and 288 Kb/s in asynchronous mode and 0.5 Mb/s in synchronous mode. The **KIV-7HS** (high speed) is even capable of 1.544 Mbps in synchronous mode. The unit is interoperable with the earlier (slower) military KG-84, KG-84A and KG-84C encryption devices.

Due to miniaturisation of the KG-84, the KIV-7 was suitable for a wide variety of applications, ranging from modern PCs to submarines. Although the unit does not come in a ruggedised housing, it is very small and is fully complient with NSA TEMPEST requirements. This makes it ideal for space and load constraint environments. It only needs a single 5V power supply.

Rack mount expansion assemblies were also available for the KIV-7, allowing 2, 4 or 8 units to share a single frame. Such rack mount solutions were supplied by both Mykotronx and Pulse Engineering. Over time, the KIV-7 has been improved several times and the latest version, the KIV-7MiP, is still in use with the Army today (2011) as a network link encryptor.

Crypto keys

In order to transmit encrypted data, the KIV-7 needs a Crypto Ignition Key (CIK, see below) and at least one Traffic Encryption Key (TEK). This is the minimum requirement for sending encrypted data. In addition to this, a Key Encryption Key (KEK) can be installed to allow new keys to be sent securely over a radio link. The latter is often referred to as Over-the-Air Rekeying (OTAR).

The TEKs and KEKs are loaded into the KIV-7 by means of a standard military key transfer device (a so-called *filler* or *key fill device*) with either the DS-101 or DS-102 protocol. The filler connects to the recessed standard 6-pin U-229 NATO-compatible fill connector on the left of the front panel. Up to 10 TEKs can be stored.

Suitable devices include the military DS-102 units KYK-13, KYX-15 and KOI-18. It can also be used with the more recent AN/CYZ-10 that also supports the later DS-101 protocol. Both standard and tagged key formats can be used

The TEKs and KEKs are retained in the KIV-7s memory even when power is turned off or the CIK is removed. For this to work, a 3.6V Lithium battery should be present in a small compartment at the bottom. If security is compromised, the user has to press the INITIATE and ZEROIZE keys simultaneously in order to delete all keys from memory, rendering the device useless.

Keys can be loaded into the KIV-7 directly by means of a suitable key generator or, as described above, with a *key transfer device*. Alternatively, the KIV-7 keys can also be updated remotely, as the device supports *Over The Air Rekeying* (OTAR). The latter requires the use of a KEK.

Crypto Ignition Key (CIK)

The KIV-7 can only be operated when a suitable Crypto Ignition Key (CIK) is present in the CIK slot at the right of the front panel. It is a standard NSA-approved physical - plastic - key that can be inserted either way around and is activated by turning it 90° clockwise, just like a normal key.

The CIK, shown in the image on the right, contains a 1KB flash memory device that is used for protection of the keys stored inside the KIV-7. When the CIK is removed, transmission is no longer possible. The combination of **KIV-7** and **CIK** should be treated as classified and should never be left together unattended.

One blank CIK is supplied with every KIV-7 unit. It can be initialised by a blank (zeroized) KIV-7 unit. Blank keys are supplied by Datakey in the USA, where it is known as the 1KB DK-series with Microwire interface and form factor A.

When crypto variables (i.e. the keys) are loaded into the KIV-7, the KIV-7 generates a random key that is used to encrypt the actual traffic encryption keys (TEKs). This random key is knows as the Key Encryption Key (KEK) and is stored inside the CIK. For this reason, the CIK is said to be *paired* with the device. The keys can only be retrieved by the KIV-7 if the appropriate CIK is present.

A CIK that is paired with one KIV-7 unit, can not be used to activate another KIV-7 unit. A CIK by itself is not a classified item. When the operator had to leave a KIV-7 unit unattended, he had to take the CIK with him. A KIV-7 without the matching CIK has no function and can not be used to decode any traffic or retrieve the original keys. As an extra safety measure, all keys (i.e. they TEKs inside the KIV-7 and the KEK inside the CIK) can be cleared by pressing the INITIATE and ZEROIZE buttons simultaneously. This is known as **ZEROIZING** and even works when the device is off.