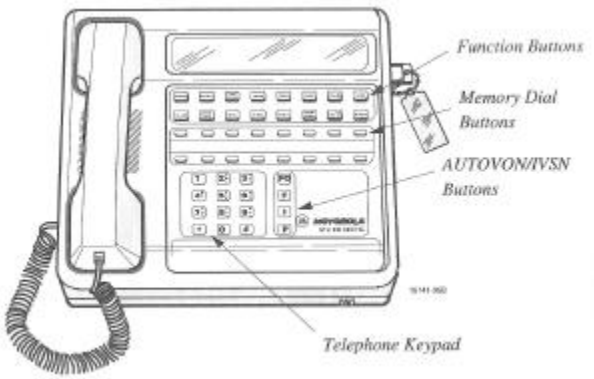
KY-71D (STU-II/B)

STU-II/B was a secure telephone unit, designed by the NSA, for use by NATO forces and governments of friendly nations. The design was based on third generation STU-III (not STU-II) crypto phones. It was introduced in the early 1990's to replace the earlier STU-II. It was interoperable with the STU-II (KY-71) and other compatible equipment.

An example of a STU-II/B phone is the **Motorola STU-II/B SECTEL** that is based on the Motorola SECTEL range of STU-III phones. At first glance, the phone is nearly identical to, say, a SECTEL 2500, but there are some significant differences.

The image on the right was taken from the SECTEL STU-II/B user manual. It shows the extended keypad of the Motorola range of SECTEL phones. The extra keys are for AUTOVON/IVSN operation only (see below).



First of all, the STU-II/B has 4 additional key on the keypad (see below). Secondly, the cryptographic keys are loaded into the STU-II/B by means of a NATO-standard fill device, such as the KYK-13 or the KOI-18. For this purpose, the unit is fitted with a U-229 connector at the rear. All keys are loaded this way, rather than with the KSD-64 key storage device. The KSD-64 is used here only as a Crypto Ignition Key (CIK).

Extra Keys

Compared to the SECTEL STU-III phones, the STU-II/B has four additional keys. They are located to the right of the existing numerical keypad and are present for backward compatibility with the non-secure AUTOVON and IVSN systems. AUTOVON (Automatic Voice Network) was a military phone system that was built in the US in 1963. It was designed to survive nuclear attacks and allowed non-secure voice calls with precedence (priority override).

IVSN was the *Initial Voice Switched Network* developed by NATO in the mid-1970s for unclassified voice calls. Starting with 4 switches in Europe in 1980, the system grew to 24 switches at the peak of its use in the mid-1980s. When it was closed down on 30 November 2005 it still consisted of 18 switches, some of which are still in use today.

- FO - Flash override
- F - Flash
- I - Immediate
- P - Priority

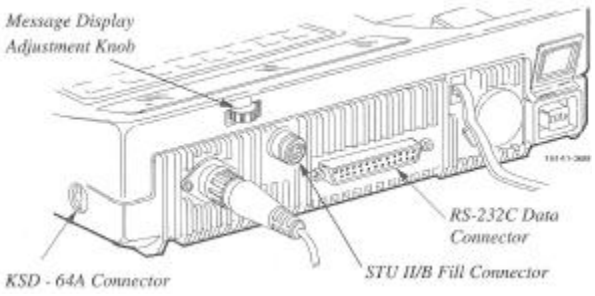
The four extra keys generate DTMF-signals in the rarely used 1633Hz column. On some later keyboards, these keys are sometimes called A, B, C and D. After a nuclear attack, it would be very difficult for government officials to obtain a free telephone line, as nearly everyone would try to make a phone call.

By pressing the letter **P**, the user would signal the switch to appoint a free line by priority. Higher ranking officials were allowed to press **I** (Immediate) to get an even higher priority. Military users were allowed to press **F** (Flash) in order to get a free line nearly instantly. It was thought that only the president and his circle were allowed to use **FO** (Flash Override) to give them the highest possible priority.

Key filling

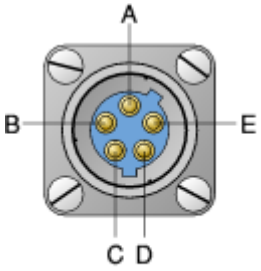
On a normal STU-III phone, the plastic KSD-64 key is used as a CIK and to load key variables into the phone. On a STU-II/B, the KSD-64 is only used as a Crypto Ignition Key (CIK) (see below). The key variables are instead loaded into the phone by means of a standard military key fill device, such as the KYK-13 or the KOI-18, connected to the standard U-299 connector at the rear.

The drawing on the right shows the rear panel of the STU-II/B telephone. To the right of the power connector is a US Army/NATO-standard 5-pin U-229 socket (U-183/B) that allows the connection of a KYK-13 or similar.

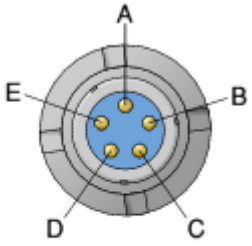


Two FILL procedures are possible: NET FILL and UNIQUE FILL (KDC Mode). Up to 17 net variables and 1 unique key can be stored inside the STU-II/B. When using the unique key, a valid telephone number of a Key Distribution Center (KDC) have been entered first.

The STU-II/B supports the (older) DS-102 standard for key loading. The pin out of the U229 connector is specified in the table below. Before loading a key, the STU-II/B first has to be put in the appropriate mode. Then the key filler must be attached and activated. If a suitable key has not been sent by the key filler within 10 seconds, the operation has failed and all existing keys will be destroyed. This is done as an extra safety measure against tampering.



Female panel mount
GC-629



Male panel mount
U-183/U

Pin	DS-102	Description	
A	GND	Ground (common wire)	
B	-	Not used	
C	ACK	FILL request acknowledgment	
D	DATA	Fill data into STU-II/B	
E	CLK	Fill clock into STU-II/B	
F	-	-	

Crypto Ignition Keys

For secure operation, a STU-II/B must be unlocked by inserting and activating a KSD-64A Key Storage Device. With the STU-II/B, the KSD-64A is only used as a Crypto Ignition Key (CIK) and not as a key fill device.

The KSD is entered into a so-called *key acceptable* at the right of the SECTEL unit, just below the display. Once inserted, it needs to be rotated 1/4 clockwise, in order to unlock the secure features of the phone.

The STU-II/B supports the following CIKs:

- **Master CIK**
  Only one Master CIK can be created for each STU-II/B terminal. The Master CIK is unique to this particular terminal. This key is normally used and controlled by the Communications Security (COMSEC) custodian. It allows *Interoperable CIKs* (see below) to be added to the terminal after the fill procedure is complete. It also allows the speakerphone feature to be enabled or disabled.
- **Interoperable CIK**
  This CIK is to be used by a typical user. 'Interoperable' means that the user can access up to 7 terminals with one CIK. The CIK data is stored in fields 2 thru 8 of the interoperable CIK.

Modes of operation

The STU-II/B has three modes of operation, each with a varying degree of security. The required mode of operation can be selected by pressing the MODE key until the display shows the correct mode. A responding STU-II/B will follow this setting automatically.

- **KDC mode**
  KDC mode requires the availability of a so-called Key Distribution Center (KDC) and offers the highest level of security. In this mode, the user first places a call to the KDC to obtain a so-called **KDC Message** before completing a call to another STU-II/B. The KDC Message contains the per-call keying variable that allows the user to setup a secure call with one specific terminal. The STU-II/B can store KDC messages for up to 21 terminals. This mode supports full-duplex voice calls and data communication up to 9600 baud and half-duplex voice and data communication at 2400 baud.
- **Net mode (Net Point-to-Point)**
  This mode allows secure communication with another STU-II, STU-II/B or compatible device, which has the same Net keying material. The SECTEL STU-II/B can store 17 Net variables. This mode supports full-duplex voice calls and data communication up to 9600 baud and half-duplex voice and data communication at 2400 baud.
- **Multipoint (Net Broadcast)**
  This mode is used to broadcast secure voice and data to multiple users. It is one means of establishing a conference call. Multipoint communication is possible between multiple STU-II and STU-II/B terminals, provided they are loaded with the same Net keying material. In this mode, voice communication is possible in half-duplex only. Data can be transferred in synchronous half-duplex mode at 2400 baud only.