

Lowering the High Cost of Security – STU-III Access Control – Crypto Ignition Key

Department of Defense

The Department of Defense manages a comprehensive inventory of installations and facilities to ensure our nation has all the assets necessary to keep Americans safe. The Department's physical plant is huge by any standard, consisting of more than 600,000 individual buildings and structures located at more than 6,000 different locations or sites.

Secure Telephones

Datakey Electronics first INFOSEC program was a secure voice communication program commonly known as STU-III (Secure Telephone Unit, Third Generation). When initially designing the system, it was decided that the requirements for the portable data carriers were:

- High level of security to increase their marketability and client confidence
- Rugged and reliable to avoid down time and replacement costs
- Fully engineered system to reduce R&D costs and time-to-market
- Long-term support to avoid expensive re-design and implementation costs

The Solution is KEY

For this program Datakey Electronics developed the KSD-64A (STU-III) Key. These Keys are used daily to secure classified conversations by encrypting, or scrambling, voice transmissions on phones supplied by AT&T, Martin Marietta, RCA, and Motorola.

After enabling the phone, the Key is re-programmed for use as an electronic access control device, or Crypto Ignition Key (CIK). Phone users must



present a STU-III Key prior to each encrypted conversation. The CIK data is updated automatically with each use. Since its introduction in 1987, the STU-III program has put more than one million Keys into use, and has been incorporated into other communications equipment.

Fully Engineered



The KC16/64PCB Keyceptacle® is a PC board-mount connector designed into all STU-III secure telephones and rated for 200,000 cycles. This Keyceptacle provides intuitive

operation, positive Key retention and an ergonomic "click" into position. It also contains a Last-On/First-Off (LOFO) contact that can be used to alert the host bus that Keys have made secure contact with the Keyceptacle so that signals can be safely transmitted. In addition to the mating Keyceptacle, Datakey Electronics also manufactures the PKS-703 Reader/Writer, commonly referred to as a "Keyloader", for uploading and downloading data from the KSD-64A Key.

Over, please...

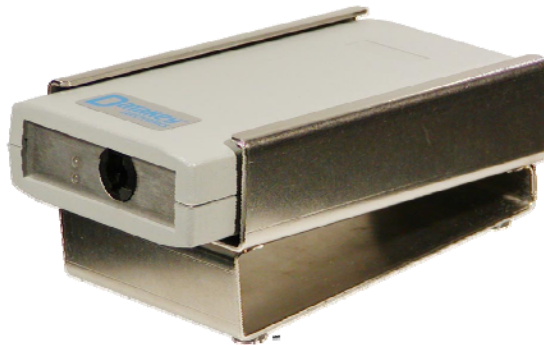




DOD, cont.

They Chose Datakey Electronics

Datakey Electronics is the recognized leader in Crypto Ignition Keys (CIKs). In addition to the Keys, Datakey Electronics' manufactures the complete system including mating Keyceptacles[®] and Reader/Writers. Datakey Electronics developed the first Crypto Ignition Key and has continued to be the leading supplier to defense contractors and OEMs for secure portable data carriers. Since its introduction in 1987, the STU-III program has put more than one million Keys in use.



www.datakey.com ■ 800-328-8828 ■ 952-746-4066

