


I'm not robot  reCAPTCHA

I am not robot!

Simple key loader technical manual

Handheld fill device An E-8 crew member entering data using an AN/PYQ-10 before a flight The AN/PYQ-10 Simple Key Loader (SKL) is a ruggedized, portable, hand-held fill device, for securely receiving, storing, and transferring data between compatible cryptographic and communications equipment. The SKL was designed and built by Ralph Osterhout[citation needed] and then sold to Sierra Nevada Corporation, with software developed by Science Applications International Corporation (SAIC) under the auspices of the United States Army. It is intended to supplement and eventually replace the AN/CYZ-10 Data Transfer Device (DTD).



The PYQ-10 provides all the functions currently resident in the CYZ-10 and incorporates new features that provide streamlined management of COMSEC key, Electronic Protection (EP) data, and Signal Operating Instructions (SOI). Cryptographic functions are performed by an embedded KOV-21 card developed by the National Security Agency (NSA). The AN/PYQ-10 supports both the DS-101 and DS-102 interfaces, as well as the KSD-64 Crypto Ignition Key.[1] The SKL is backward-compatible with existing End Cryptographic Units (ECU) and forward-compatible with future security equipment and systems, including NSA's Key Management Infrastructure. Between 2005 and 2007, the U.S. Army budget included funds for over 24,000 SKL units.



This price includes the unit and the internal encryptor card.[2] References ^ 20keys.html[permanent dead link] ^ "Committee Staff Procurement Backup Book Fiscal Year (FY) 2007 Budget Estimates" (PDF). Dept of the Army. Feb 2006. Retrieved 11 August 2012. Sierra Nevada SKL spec sheet 2005 US Army Weapons System Handbook Retrieved from " This article needs additional citations for verification. Please help improve this article by adding citations to reliable sources. Unsourced material may be challenged and removed.Find sources: "Fill device" - news - newspapers - books - scholar - JSTOR (September 2022) (Learn how and when to remove this template message) Module used to load cryptographic keys into encryption machines KY-57 voice encryptor. Note fill port in center. A KYK-13 fill device. A fill device or key loader is a module used to load cryptographic keys into electronic encryption machines. Fill devices are usually hand held and electronic ones are battery operated. Older mechanical encryption systems, such as rotor machines, were keyed by setting the positions of wheels and plugs from a printed keying list. Electronic systems required some way to load the necessary cryptovariable data. In the 1950s and 1960s, systems such as the U.S. National Security Agency KW-26 and the Soviet Union's Fialka used punched cards for this purpose. Later NSA encryption systems incorporated a serial port fill connector and developed several common fill devices (CFDs) that could be used with multiple systems. A CFD was plugged in when new keys were to be loaded. Newer NSA systems allow "over the air keying" (OTAR), but a master key often must still be loaded using a fill device. NSA uses two serial protocols for key fill, DS-101 and DS-102. Both employ the same U-229 6-pin connector type used for U.S. military audio handsets, with the DS-101 being the newer of the two serial fill protocols. The DS-101 protocol can also be used to load cryptographic algorithms and software updates for crypto modules.

PDF 346 mb SIMPLE KEY LOADER TECHNICAL MANUAL (It is strongly suggested to begin browsing the first section, Introduction in the Table of Contents section at the top of the subject, you should use the table of contents to simply obtain the subject you are looking for, considering that it is organized hierarchically. According to our log, this PDF file is submitted on 18 Nov, 2016, registered under serial number of -, having data size around 323.02, in case you want to download it, visit our website.)

If you missed what exactly are you looking for, possibly seeking some other sources for SIMPLE KEY LOADER TECHNICAL MANUAL, can help what is listed on the table of contents on the bottom. This list is organized with the most common and relevant file compatible to your search term and we regularly update it for your convenience by our system. We hope you could find something useful by providing you much more choices.

Download PDF

In order to download, visit this URL below, enter the book title on the search box and submit:

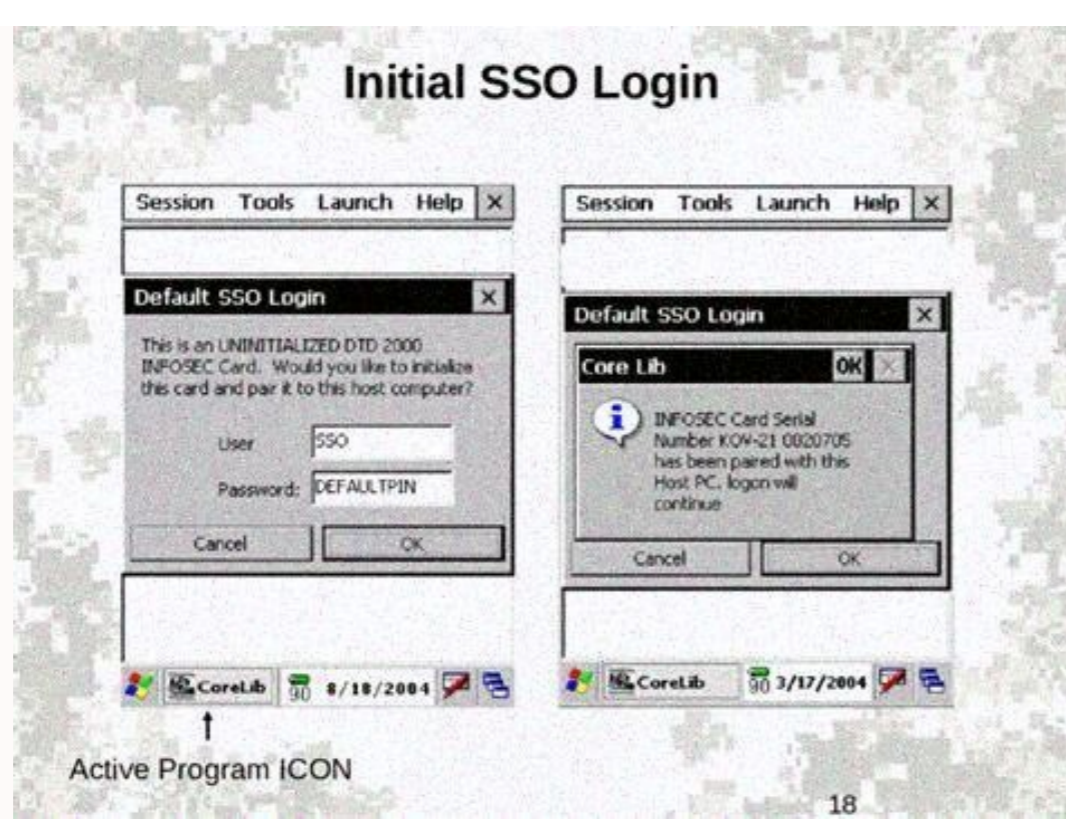
<http://pdfbling.org/>

PDF for simplekeyloader technical manual

Between 2005 and 2007, the U.S. Army budget included funds for over 24,000 SKL units. The estimated price for FY07 was \$1708 each. When released in May 2005, the price was \$1695 each. This price includes the unit and the internal encryptor card.[2] References ^ 20keys.html[permanent dead link] ^ "Committee Staff Procurement Backup Book Fiscal Year (FY) 2007 Budget Estimates" (PDF). Dept of the Army. Feb 2006. Retrieved 11 August 2012. Sierra Nevada SKL spec sheet 2005 US Army Weapons System Handbook Retrieved from " This article needs additional citations for verification. Please help improve this article by adding citations to reliable sources. Unsourced material may be challenged and removed.Find sources: "Fill device" - news - newspapers - books - scholar - JSTOR (September 2022) (Learn how and when to remove this template message) Module used to load cryptographic keys into encryption machines KY-57 voice encryptor. Note fill port in center. A KYK-13 fill device. A fill device or key loader is a module used to load cryptographic keys into electronic encryption machines. Fill devices are usually hand held and electronic ones are battery operated. Older mechanical encryption systems, such as rotor machines, were keyed by setting the positions of wheels and plugs from a printed keying list. Electronic systems required some way to load the necessary cryptovariable data. In the 1950s and 1960s, systems such as the U.S. National Security Agency KW-26 and the Soviet Union's Fialka used punched cards for this purpose. Later NSA encryption systems incorporated a serial port fill connector and developed several common fill devices (CFDs) that could be used with multiple systems. A CFD was plugged in when new keys were to be loaded. Newer NSA systems allow "over the air keying" (OTAR), but a master key often must still be loaded using a fill device. NSA uses two serial protocols for key fill, DS-101 and DS-102. Both employ the same U-229 6-pin connector type used for U.S. military audio handsets, with the DS-101 being the newer of the two serial fill protocols. The DS-101 protocol can also be used to load cryptographic algorithms and software updates for crypto modules.



The PYQ-10 provides all the functions currently resident in the CYZ-10 and incorporates new features that provide streamlined management of COMSEC key, Electronic Protection (EP) data, and Signal Operating Instructions (SOI). Cryptographic functions are performed by an embedded KOV-21 card developed by the National Security Agency (NSA). The AN/PYQ-10 supports both the DS-101 and DS-102 interfaces, as well as the KSD-64 Crypto Ignition Key.[1] The SKL is backward-compatible with existing End Cryptographic Units (ECU) and forward-compatible with future security equipment and systems, including NSA's Key Management Infrastructure. Between 2005 and 2007, the U.S. Army budget included funds for over 24,000 SKL units. The estimated price for FY07 was \$1708 each. When released in May 2005, the price was \$1695 each. This price includes the unit and the internal encryptor card.[2] References ^ 20keys.html[permanent dead link] ^ "Committee Staff Procurement Backup Book Fiscal Year (FY) 2007 Budget Estimates" (PDF). Dept of the Army. Feb 2006.



18

Dept of the Army. Feb 2006.
Retrieved 11 August 2012. Sierra Nevada SKL spec sheet 2005 US Army Weapons System Handbook Retrieved from " This article needs additional citations for verification. Please help improve this article by adding citations to reliable sources. Unsourced material may be challenged and removed.Find sources: "Fill device" - news - newspapers - books - scholar - JSTOR (September 2022) (Learn how and when to remove this template message) Module used to load cryptographic keys into encryption machines KY-57 voice encryptor. Note fill port in center. A KYK-13 fill device. A fill device or key loader is a module used to load cryptographic keys into electronic encryption machines. Fill devices are usually hand held and electronic ones are battery operated. Older mechanical encryption systems, such as rotor machines, were keyed by setting the positions of wheels and plugs from a printed keying list. Electronic systems required some way to load the necessary cryptovariable data. In the 1950s and 1960s, systems such as the U.S. National Security Agency KW-26 and the Soviet Union's Fialka used punched cards for this purpose. Later NSA encryption systems incorporated a serial port fill connector and developed several common fill devices (CFDs) that could be used with multiple systems. A CFD was plugged in when new keys were to be loaded. Newer NSA systems allow "over the air rekeying" (OTAR), but a master key often must still be loaded using a fill device. NSA uses two serial protocols for key fill, DS-101 and DS-102. Both employ the same U-229 6-pin connector type used for U.S. military audio handsets, with the DS-101 being the newer of the two serial fill protocols. The DS-101 protocol can also be used to load cryptographic algorithms and software updates for crypto modules. Besides encryption devices, systems that can require key fill include IFF, GPS and frequency hopping radios such as Have Quick and SINGARS. Common fill devices employed by NSA include: KYK-28 pin gun used with the NESTOR (encryption) system KYK-13 Electronic Transfer Device KYX-15 Net Control Device[1] MX-10579 ECCM Fill Device (SINGARS)[2] K01-18 paper tape reader. Can read 8-level paper or PET tape, which is manually pulled through the reader slot by the operator. It is battery powered and has no internal storage, so it can load keys of different lengths, including the 128-bit keys used by more modern systems. The K01-18 can also be used to load keys into other fill devices that do have internal storage, such as the KYK-13 and AN/CYZ-10. The K01-18 only supports the DS-102 interface. AN/CYZ-10 Data Transfer Device (DTD) - a small PDA-like unit that can store up to 1000 keys, maintains an automatic internal audit trail of all security-relevant events that can be uploaded to the LMD/KP, encrypts key for storage, and is programmable. It is capable of keying multiple information systems security (INFOSEC) devices and is compatible with such COMSEC equipment as SINGARS radios, KY-57 VINSON, KG-84, and others that are keyed by common fill devices (CFDs). The AN/CYZ-10 supports both the DS-101 and DS-102 interfaces. It was developed in the early 1990s, weighs about 4 lb (1.8 kg), and was designed to be fully compatible with future INFOSEC equipment meeting DS-101 signaling and benign fill standards. It will eventually replace the legacy family of CFDs, including the KYK-13, KYX-15 electronic storage devices, and the K01-18 paper tape reader. Only the DTD and the K01-18 support newer, 128-bit keys. Secure DTD2000 System (SDS) - Named KIK-20, this was the next generation common fill device replacement for the DTD when it started production in 2006. It employs the Windows CE operating system.[3] AN/PYQ-10 Simple Key Loader (SKL) - a simpler replacement for the DTD. KSD-64 Crypto ignition key (CIK) KIK-30, a more recent fill device, is trademarked as the "Really Simple Key Loader" (RASKL) with "single button key-squirt." It supports a wide variety of devices and keys.[4] The older KYK-13, [5] KYX-15 and MX-10579 are limited to certain key types. See also List of cryptographic key types References ^ "KYX-15". ^ "MX-18290/VRC Fill Device, ELEK CCM". ^ "SDS Secure DTD2000 System KIK-20". ^ permanent dead link ^ "KYK-13". External links Fill devices KYX-15 pictures Wikimedia Commons has media related to Fill devices in the National Cryptologic Museum. Retrieved from "