KOI-18

General Purpose Tape Reader — Punched Key Fill Device

Historical Overview & Operational Guide

NSA, 1968–2019 · DS-102 Protocol · Paper-Mylar-Paper Key Tape

> *"The whole chain of national secrecy ended, for the operator, at a strip of punched tape and a human thumb. You pressed INITIATE, you pulled the tape through the slot at arm speed, you watched for the lamp to flash, and you moved on to the next device. It was the simplest piece of cryptographic equipment in the United States military inventory, and for fifty years it was the one that connected every other piece to the keys it needed."*

Part I — Historical Background

1.1 Origins and the DS-102 Fill Architecture

By the late 1960s, NSA cryptographic equipment had moved past the patch-panel, plugboard, and rotor-setting era and into the world of electronic key loading. Devices like the KG-13, the KW-7 Orestes, and the second-generation KW-37 fleet broadcast encryptor all needed to be loaded with cryptovariables — binary key streams — through a standardized physical port rather than a mechanical setup routine. NSA chose a simple solution: the U-229 six-pin connector already standardized for military audio handsets, and a serial fill protocol later formalized as DS-102.

The key-distribution problem remained, however, separate from the key-loading problem. Until electronic key management became viable in the 1990s, cryptographic keys had to be physically transported from the NSA production facility to the end unit — aircraft, ship, ground station, field radio. The chosen medium was paper-mylar-paper laminated tape, eight bits wide, with the cryptographic material punched into it as holes. A hole represented a binary 1; the absence of a hole represented a binary 0. The laminated construction gave the tape enough dimensional stability to survive repeated handling and reading, and the mylar core made it resistant to the tearing that pure paper tape suffered.

The KOI-18 General Purpose Tape Reader, introduced into field service in the late 1960s, was the device that bridged these two worlds. It accepted an NSA punched key tape on one side and

it emitted the resulting bit stream onto a DS-102 fill cable on the other. It had no internal storage, no cryptographic logic of its own, and no intelligence beyond the optoelectronics needed to read the tape. That minimalism was the point: the KOI-18 could load any key of any length onto any DS-102-compatible device, and it would still be useful when the keys it loaded grew from 64 bits to 128 bits to any arbitrary length the NSA decided to generate.

1.2 Why It Survived Five Decades

Paper tape feels archaic for the 1990s, let alone for equipment still being loaded this way in the 2010s. But the KOI-18 persisted because of two interlocking facts. First, United States military platforms keep their radios and crypto equipment for a very long time. The KY-57 VINSON voice encryptor entered service in 1978 and was still the default tactical voice crypto on many aircraft thirty-five years later. The KG-84 data encryptor did the same. These legacy devices spoke DS-102, and the KOI-18 was the universal tool for speaking back to them.

Second, the replacement fill devices — KYK-13, AN/CYZ-10, AN/PYQ-10 Simple Key Loader, KIK-20, and later the NGLD-M — all had internal storage of their own. They could hold a handful of keys in battery-backed memory, and they could squirt those keys into end devices quickly. But someone still had to get the keys into the storage device to begin with. For years, the answer to that problem was: pull a KOI-18 through a tape to load the KYK-13, then walk the KYK-13 around the airframe. The KOI-18 was the tape-to-electronic gateway through which the entire flight-line cryptographic supply chain passed.

Only on October 2, 2019 did the last roll of NSA punched key tape come off the production machines at Fort Meade, officially ending the fifty-one-year punched-tape era for United States military cryptography.

> **Historical Note:** *The KOI-18 entered service at roughly the same moment the C-5A Galaxy entered operational flight with Military Airlift Command — 1969, on both counts. For the entire operational life of the original Galaxy airframe and well into the service of the C-5B and C-5M Super Galaxy variants, the KOI-18 was the standard means by which the aircraft's secure communications suite received its daily keys. Two pieces of equipment, contemporaries at birth, stayed paired through half a century of operations.*

Part II — How the Device Works

2.1 Physical Description

The KOI-18 is a compact, handheld, battery-powered device, roughly the size of a paperback book. One face carries a slot through which the tape is drawn by hand; the opposite face carries the U-229 six-pin connector that mates with the fill cable to the target device. An indicator lamp

— visible to the operator as the tape is pulled — confirms reads and flags parity failures. A small switch or button initiates a load. That is the entire user interface.

Internally, the device consists of a photo-optical reader array that senses light passing through the holes in the tape, a line-driver circuit that converts the parallel hole pattern into the DS-102 serial fill protocol, a parity-check circuit, and a small battery compartment. The original specification called for a 6.5-volt mercury cell (BA-1572/U); later variants used a 6.3-volt alkaline equivalent (BA-5372/U). There is no microprocessor, no firmware, and nothing that can be updated in the field. The device is purely combinational logic, which means it cannot be made obsolete by a software change — only by the disappearance of the standards it implements.

2.2 The Key Tape

PROPERTY	SPECIFICATION
Width	Eight data tracks plus a smaller sprocket track through the center
Construction	Paper-mylar-paper laminate for dimensional stability and tear resistance
Encoding	Hole = binary 1; absence of hole = binary 0
Production	NSA Central Security Service key production facility, Fort Meade, Maryland
Distribution	Sealed tamper-evident canisters, serialized and tracked by short-title
Classification	Classified at the level of the traffic the key protects — up to TOP SECRET / CRYPTO
Usage convention	One tape edition per crypto-period; segments consumed and destroyed on a daily cadence

Each tape carries multiple segments — typically thirty-one, one per day of the month, sometimes with separate A and B halves for overlapping usage windows. The segments are physically separated by printed boundaries but belong to a single issued edition. The short-title identifier on the canister — for example USKAT-634D — is the reference by which the COMSEC custodian, the operator, and the accountability ledger all track what key is loaded on what device at what time.

2.3 The Load Procedure

The procedure reads today like a ritual, and in a sense it was — a well-defined sequence drilled into every operator cleared to perform it, identical from one aircraft bay to the next, from one flight line to the next, for fifty years.

- Step 1 — Draw the material. The operator signed for a specific tape canister from the COMSEC custodian, keyed to the aircraft's tail number, the mission profile, and the current crypto-period. The signature was two-person wherever the local regulations required it.
- Step 2 — Inspect the seal. The canister's tamper-evident seal was visually verified before opening. A broken seal was a reportable COMSEC incident requiring immediate notification up the chain; the tape was treated as potentially compromised and pulled from use.
- Step 3 — Identify the segment. Each day's segment was labeled; the operator selected the segment corresponding to the current Julian date. Using the wrong segment was a fault condition — the crypto device would load, but the traffic would not decrypt at the far end, which is an expensive way to discover a procedural error.
- Step 4 — Connect. The U-229 cable joined the KOI-18 to the fill port of the target device — either a crypto end unit directly, or an intermediate storage fill device like a KYK-13.
- Step 5 — Initiate. The operator pressed INITIATE on the target device (or on the KYK-13), placing it in load-receive mode. The target now waited for the DS-102 bit stream.
- Step 6 — Pull. The operator fed the tape into the KOI-18 slot and drew it through by hand at a steady pace — roughly the speed of a firm pencil stroke. Too fast and the optoelectronic reader could miss a hole; too slow and the target's internal timer could fault. With practice, the correct pace became reflexive.
- Step 7 — Verify. The indicator lamp on the KOI-18 confirmed a clean read; on the target device, a parity check confirmed that the key arrived intact. A second "OFF CHECK" or equivalent verification pass was typical immediately after the load, with a specific lamp behavior confirming good parity.
- Step 8 — Destroy or zeroize. Single-use key tape segments were burned or shredded immediately after successful load. Multi-use segments were returned to the canister, the canister was resealed according to local procedure, and the custodian was notified of the remaining supply. The accountability log entry — short-title, edition, segment, date, time, target device, operator signature — was then completed.
- Step 9 — Repeat. A single aircraft typically hosted five to twelve cryptographic devices that all required fresh keys. The operator worked through them in turn, sometimes using the KOI-18 directly for each, more often loading a KYK-13 with multiple keys and then carrying the KYK-13 from station to station.

> **Operator Note:** *The physical act of pulling the tape by hand introduced a specific human rhythm into the loading process. The tape had to move smoothly and at a relatively constant speed, which meant operators developed a kinesthetic sense for the correct draw. Cold hands in the winter, gloves on the flight line, or a tape that had curled in storage all changed*

> *the feel of the pull. Experienced operators could identify a bad segment by the way it passed through the reader before the lamp even confirmed the fault.*

Part III — The Daily Turnover

3.1 Why Keys Changed Every Day

The operational heartbeat underneath the entire KOI-18 era was the daily cryptographic period — the cryptoperiod — at which keys were replaced and the previous day's key destroyed. Military symmetric traffic keys were typically authorized for a period of one to seven days, most commonly one. The rationale is twofold. First, the longer a key is in use, the larger the volume of intercepted ciphertext an adversary can accumulate under it, and the more valuable cryptanalytic exploitation of that key becomes if it is ever broken. Second, the longer a key is in circulation, the greater the opportunity for physical compromise — a tape canister misplaced, a device captured, a clearance withdrawn.

Setting a fixed daily replacement schedule bounded both risks. Intercepted traffic older than twenty-four hours was protected by a key that had already been destroyed; a captured device loaded with yesterday's key compromised nothing that was still operationally current. And the cadence — same time every day — kept the entire distributed force in synchronization without requiring real-time coordination.

3.2 Hotel Juliet — The Ritual of the Hour

In NSA parlance, the daily key change was called HJ — Hotel Juliet in the NATO phonetic alphabet — short for "Hour of Julian date change." The abbreviation started as accountant shorthand for the midnight roll-over of the Julian date and became, over time, the colloquial term for the key-change event itself. "HJ at zero-six Zulu" was a complete and fully understood operational statement: every cryptographic device in the affected net would transition to the next day's key at 0600 UTC, and the operator responsible for each device would have that key loaded and verified before the hour arrived.

The specific HJ hour varied by command, by theater, and by operational circumstance. Some commands ran on local midnight. Some ran on Zulu midnight. Some used other fixed offsets that aligned with flight operations or with the rotation of watch-standing crews. Whatever the chosen hour, the procedure surrounding it was identical: previous day's key destroyed, next day's key loaded, loaded key verified, accountability log updated. The KOI-18 was the instrument of this transition for every device that did not otherwise receive its keys electronically.

3.3 A Day on the Flight Line

For the operator assigned to the aircraft's comm load — on a C-5 Galaxy this was often the flight engineer, sometimes the loadmaster, sometimes a dedicated COMSEC custodian on larger missions — the daily arc looked like this. An hour or two before the scheduled HJ, the operator signed out the day's tape canister and the KYK-13 assigned to the aircraft. They verified the canister seal, identified the correct segment for the current Julian date, and proceeded to the aircraft. On board, they worked the list of crypto devices in a defined order — typically the least accessible first, so that the aircraft could be closed up afterward with minimum rework.

For each device: connect the fill cable, initiate, load, verify, log. Some devices — the KY-57/58 for voice, the KG-84 for teletype, the KG-13 and KW-46 for older broadcast circuits, the IFF Mode 4 transponder, the HAVE QUICK and SINCGARS frequency-hopping radios, the GPS precise-positioning receiver — each had their own access panel, their own fill port, their own procedures. A full comm load on a C-5 could take thirty to ninety minutes depending on device count and accessibility. When the last device was loaded and the last log entry signed, the consumed tape segments were taken to the burn bag; the KYK-13 was zeroized and returned to the custodian; and the aircraft was ready to fly secure.

This sequence, repeated across the U.S. Air Force, the Navy, the Army, the Marine Corps, and allied forces under NATO standardization agreements, constituted one of the largest sustained physical-security operations in the history of cryptography. Every day, at the HJ hour, tens of thousands of cryptographic devices worldwide were rekeyed — each one by a cleared operator, each one with a specific tape segment, each one through a KOI-18 or a device loaded by a KOI-18. The system worked because it was boring, standardized, and drilled.

> **Operational Observation:** *The daily key change imposed a rhythm on operational life that rarely appears in public accounts of military flying. For a crew based at Dover or Travis or Ramstein, flying C-5s on strategic airlift missions, HJ was not an event — it was an hour of the day, like briefing or preflight, and missing it meant the aircraft could not be dispatched on a secure-communications mission. The KOI-18 was, functionally, the clock hand that ticked those hours forward.*

Part IV — End of the Tape Era

4.1 The Replacement Stack

Electronic fill devices progressively displaced the KOI-18 as the default key-loading tool. The KYK-13, introduced in 1976, could hold six 128-bit keys in internal battery-backed storage, making it possible to carry an entire aircraft's key complement in a pocket-sized box. The AN/CYZ-10 Data Transfer Device, fielded in the early 1990s, stored up to a thousand keys, maintained an automatic internal audit trail, and could key multiple generations of COMSEC equipment. The

AN/PYQ-10 Simple Key Loader and the KIK-20 Secure DTD 2000 System followed, and the Next Generation Load Device-Medium is now replacing them.

At each generation the KOI-18 became less central but did not disappear. It remained the device that could load an arbitrary-length key onto an arbitrary-era DS-102 target, and it remained the fallback when electronic fill devices failed or were unavailable. Units that operated legacy equipment — and legacy equipment is the rule rather than the exception in military aviation — kept a KOI-18 in the COMSEC locker as a matter of course.

4.2 October 2, 2019

The NSA spokesperson's statement was quiet and unceremonial. On October 2, 2019, the last roll of punched key tape came off the production machines at Fort Meade. After fifty-one years of continuous output — through every generation of crypto equipment the agency had fielded, through three decades of Cold War and two decades of Global War on Terror — the paper-mylar-paper era was over in U.S. service. The transition had been underway for more than a decade, driven both by cost and by the greater security of electronic key distribution, but the final cutover was marked by a single production line shutting down.

Tapes already issued to units remained in use until their crypto-periods expired. Some units operated on tape for weeks or months after the production line closed. But the pipeline upstream of them was gone, and by the early 2020s the KOI-18 had effectively retired from first-line service — kept in museums, reserved for training, and still held by allied forces who had not yet completed their own transitions.

4.3 Continuing Use Abroad

The United Kingdom Ministry of Defence continues to produce and consume paper key tape through its Key Production Authority, processing thousands of orders per year in the same paper-mylar-paper format. Other NATO nations, and allied services in various stages of modernization, continue to operate KOI-18 readers in support of their own legacy cryptographic stocks. The device, and the tape it reads, are not historical relics yet; they are simply no longer the American standard.

4.4 Summary

The KOI-18 General Purpose Tape Reader is the hand-operated photo-optical device that, for fifty-one years, served as the interface between NSA punched key tape and every U.S. military cryptographic end unit that spoke the DS-102 fill protocol. It carried no intelligence of its own; it stored no keys; it ran on a single battery and required no maintenance beyond the occasional cleaning of its read head. It was the physical instrument of the daily Hotel Juliet key-change ritual on aircraft, ships, and ground stations across the world. It was, in the most literal sense, how every C-5 Galaxy from 1969 onward learned each day's secrets.