# History of the TSEC/KL-7 ADONIS & POLLUX

## The first standard U.S. Armed Forces Tactical Lightweight Rotor Cipher Machine Using Electronics

**Dirk Rijmenants**

**ABSTRACT**

The TSEC/KL-7 was the first crypto machine using electronics, developed as standard crypto device for the U.S. Armed Forces, the CIA and FBI, and later also used by NATO. This article presents the history of its development and use by the different services and countries.

**KEYWORDS**

TSEC/KL-7, AFSAM-7, ADONIS, POLLUX, ASA, AFSA, NSA, CIA, FBI, NATO

**ARTICLE**

Compiled May 17, 2022. Updated August 31, 2024. Ed 03 (7.1.0)

**CONTACT**

Dirk Rijmenants
Cipher Machines and Cryptology
https://www.ciphermachinesandcryptology.com
E-mail: dr.defcom@telenet.be

**INTRODUCTION**

The TSEC/KL-7 is an American off-line crypto machine, developed by the Army Security Agency (ASA) and the Armed Forces Security Agency (AFSA) under de name AFSAM-7, introduced by the National Security Agency (NSA) in 1953 and renamed TSEC/KL-7 in 1955. The KL-7 was the first tactical lightweight rotor-based crypto machine using electronics, developed as standard crypto device. The machine was extensively used by the U.S. military, CIA, FBI and NATO, had excellent cryptographic properties and was designed to resist any cryptanalytic attack, even when its technical details were known. Two security breaches occurred in the 1960s when two U.S. warrant officers independently sold both the KL-7 design and key lists to the Soviets.

## BRIEF DESCRIPTION OF THE KL-7

The TSEC/KL-7 is an off-line non-reciprocal rotor cipher machine with electro-mechanical and electronic components, including four electron tubes. The machine measures 12 x 12 x 3.37 inches (30,5 x 30,5 x 16,2 cm) and weighs 20.5 lbs (9,3 Kg), which was quite compact for such a complex machine in the 1950s. The main components:

- TSEC/KL-7 (AFSAM-7) is the complete machine.
- KLB-7/TSEC Base is the base of the machine and supports all other components. Its contact panel assembly has spring-loaded contacts across its surface that mate with the various other parts of the machine, making exchange of defective parts quite easy.
- KLA-7/TSEC (AFSAM-107) Rotor Stepping Unit is located on top of the base and contains the stepping mechanism and the actuator switches to manually advance the rotors if required. The Rotor Stepping Unit also carries the Cipher Unit.
- KLK-7/TSEC (AFSAM-207) Cipher Unit, also referred to as rotor cage, holds 8 rotors that perform the actual encryption. One of the rotors is stationary.

The KL-7 operates on 24 Volts DC (e.g. vehicle battery) that powers a DC motor with AC generator in the same housing. The motor also provides mechanical power to the pulse generator, printer drum and rotor stepping mechanism. The 24 Volts are also used for the vacuum tube filaments and the rotor stepping electro-magnets. The AC generator provides power to the electronics. An optional AC power converter to convert 110 or 220 Volts AC into 24 Volts was also available.

The keyboard contains 26 letters, 10 figures, the letters and figures keys, space bar and repeat key. Underneath the keyboard is the Sliding Contact Board, operated by the Selector handle to change between Plain, Encipher and Decipher mode. When a key is depressed, the signal travels through the eight rotors to the printer. Which character is printed depends on the signal direction through the rotors, as chosen with the Selector handle, the selection of the eight 36-pins rotors from a set of 12, their internal wiring, the selected notch ring for each rotor, the order of those rotors in the Cipher Unit and their position at the start of the message.

The printer has a clockwise rotating print drum. At the same axle is a pulse generator with a rotating magnetic armature and fixed double stator with 37 pulse coils in a 360-degree pattern. When a pulse coil circuit is activated, its pulse is amplified by the electronics to energize the print hammer at the exact moment when the character passes the hammer.

When a character is printed, this also activates a clutch, connecting the printer axle through reduction gears with a second axle to provide both timing signals through its camshaft and mechanical power for the Rotor Stepping Unit. The rotors can step individually after each keystroke. This requires the activation of electromagnets that either allow or prevent the mechanical power from the DC motor to move a particular rotor (the electromagnets themselves do not move the rotors). Which rotors advance one position is determined by the notch rings on seven rotors (one rotor is fixed stationary). The notch rings control seven switches, connected to a logic maze circuitry that activates the stepping magnets to advance one single or multiple rotors, depending on the circuit's logic. [1] [2] [3]

Full technical description at https://www.ciphermachinesandcryptology.com/en/kl-7.htm

## DEVELOPMENT OF THE AFSAM-7 AND TSEC/KL-7

The development of the KL-7 involved several agencies. The Signal Intelligence Service (SIS), established in 1929 as part of the Army Signal Corps, was responsible for cryptanalysis under the direction of renowned cryptologist William F. Friedman. In March 1943, the SIS was renamed Signal Security Service (SSS) and in July 1943 again renamed Signal Security Agency (SSA). Its successor, the Army Security Agency (ASA), was established in September 1945 and existed until late 1976.[4]

In 1949, the Armed Forces Security Agency (AFSA) was established to merge all Communications Security (COMSEC) and Communications Intelligence (COMINT) efforts. William Friedman led AFSA's cryptologic division, and this agency gave the machine its initial name AFSAM-7. However, the means and responsibilities of AFSA were scattered over many different civil and military services. To improve coordination, the National Security Agency (NSA) was established in 1952, with Friedman as chief cryptologist. The development of the KL-7 therefore involved the ASA, AFSA and NSA.[5] [6] [7] [8]

The roots of the KL-7 are found in the Second World War when the U.S. Army SIGABA rotor cipher machine, called ECM (Electric Cipher Machine) by the Navy, and the SIGABA CCM (Combined Cipher Machine) had set a new standard for secure high-level communications between the Allies. At tactical level, the lightweight mechanical M-209 was widely used. By the end of the war, the M-209 was no longer considered secure and the U.S. Army expressed the need for a lightweight secure crypto machine that could replace the M-209 but would have a cryptographic strength, similar to the SIGABA.

The U.S. Navy was also seeking a small cipher machine with the qualities of the ECM, with a focus on saving weight. In March 1945, the Army headquarters requested the Signal Security Agency (SSA), soon after renamed Army Security Agency (ASA), to develop a machine that would fit their needs. Meanwhile, the CCM, based on the AJAX crypto principle and used by both the U.S. and United Kingdom, was outdated and needed replacement.

The project was designated MX-507 and ASA saw it as a long-range research project. The researchers quickly decided to opt for a rotor-based machine. They also had to design a completely new lightweight printing system, as the new machine was required to operate off-line and print out the messages on a paper strip. Eventually, they were able to reduce a printer system to one quarter of its original size and weight.[9]

ASA applied a new cryptographic principle, called re-entry or re-flexing, which required 36-pins rotors. The idea was to take parts of the cipher output, re-enter the output back into the enciphering process and re-encipher it again. Cryptanalyst Albert W. Small conceived the system in 1940 and filed it for patent in 1944. However, his patent was placed under Patent Office Secrecy Order. This would cause a patent conflict in 1957.[10]

The rotors were a further development of the early WW2 rotors. The so-called Blue Rotor, used until the late 1950s, was a fairly large Hebern type 26-pins rotor, simple and rugged. The regular rewiring of those rotors, required for security reasons, was quite complicated. A modified version of the Blue Rotor, called White Rotor, carried an alphabet ring and notch ring.

The U.S. Navy also developed a smaller Hebern type 26-pins rotor, called Yellow Rotor, for their successor of the CCM. There was also a study to use printed rotors, with the circuits etched onto the rotor body. That that project ended in 1953 and was ultimately discontinued.

The Armed Forces Security Agency (AFSA) was created in 1949. AFSA was the first American central cryptologic organization. One of its primary goals was to provide standardization of secure communications devices and determine a general policy for crypto equipment. The research of the ASA was transferred to AFSA in December 1949. The MX-507 was renamed AFSAM-7, which stands for Armed Forces Security Agency Machine No 7.

After a series of cryptologic studies, already initiated in 1946, AFSA decided to use the 36-pins Red Rotor with rotatable alphabet ring and notch ring, for both the off-line AFSAM-7 and the AFSAM-9 teletype encryption. However, the Red Rotor had two major problems. Tolerance issues with the plastic molding process and contact problems. The rotor used beryllium copper contacts of which particles wore off and turned into abrasive non-conductive copper oxide, which worsened the wear even more, and also caused contact problems.

From 1946 on, several external contractors studied the problems with the Red Rotors. Tests with 200 contact materials did not find better materials than beryllium copper and the plastic compound was still the best suitable. After more modifications and improvements, the Red Rotor was accepted but contact problems persisted.

After ten years research, costing $1,250,000, they arrived at the Orange Rotor. One of the improvements was a rotatable alphabet ring, set by depressing and rotating the ring, without having to remove it from the rotor. Production of the Orange Rotor started in 1956. This rotor became the standard 36-pins rotor, later also for the KL-47B and KW-9. The development and production of the rotors involved Molded Insulation Co, Minneapolis-Honeywell Regulator Co, and American Phenolic Corp (Amphenol).[11]

In April 1949, the United States and its allies had formed the North Atlantic Treaty Organization (NATO) and deteriorating relations with the Soviet Union resulted into a grim Cold War. Secure communications between the NATO members was an important part of making a front against the USSR. An additional challenge, faced by AFSA, was to design for themselves a machine that could also be distributed among their NATO allies without disclosing vital secret crypto technology that could end up into Soviet hands.

With such a large organization as NATO, it was more than likely that this machine or its specifications would eventually reach Russian soil. The design had to resist by far any possible cryptanalytic attack by Soviet codebreakers, even when the technical details of the machine were disclosed. The security of the machine had to depend solely on the secrecy of the key settings, thus obeying Kerckhoffs' well-known law on cryptography.

In September 1950, AFSA demonstrated an engineering model. The final design used eight 36-pins rotors, a re-entry of ten rotor signals, and a most complex irregular stepping of the rotors, electrically controlled by notch rings on the rotors. The problems with the printer timing and the letter/figures shift system were solved by a clever design with electron tubes, making the AFSAM-7 the first tactical cipher machine ever to use electronics.[12]

During the ad hoc committee of the BRUSA COMSEC conference, William Friedman, Albert Small and Abraham Sinkov discussed the AFSAM-7. Friedman explained that the purpose of the conference was to discuss a limited exchange of cryptographic principles. When asked about the implications of the capture of the AFSAM-7, Small answered that it would not affect the security of U.S. communication for some time.[13]

The AFSAM-7 was approved, and the Army was asked to build prototype models. By December 1950, the Army declared the AFSAM-7 ready for production. The machine would become the first standard crypto machine in the U.S. Armed Forces. The crypto system was designated POLLUX. Contractors were selected and operational and maintenance manuals composed.

In February 1951, contracts were signed to produce 25,000 AFSAM-7s at a rate of 5,000 per year. The first repair and maintenance course for Army and Air Force personnel was scheduled in September 1951. However, due to tooling problems and material shortages, delivery of the AFSAM-7 was delayed to June 1952, and then delayed again to January 1953. [14] [15]

In 1951, the BRUTUS crypto principle was proposed as replacement for the CCM's outdated AJAX principle. The BRUTUS rotor stepping maze controlled the irregular movement of the rotors, with rotors 2 and 6 rotating in opposite direction, and differed from the POLLUX stepping logic. BRUTUS used seven 26-pins rotors from a set of ten, with removable cams and alphabet rings. The number of notches on the notch pattern had to be 7, 9, 11, 15, 17 or 19 (co-primes). Meanwhile, the Navy had been developing its own machine, initially named Portable Cipher Machine (PCM) and later renamed AFSAM-47. They had already adopted the BRUTUS crypto principle earlier on for their AFSAM-47, but production, planned for late 1950, was already delayed.

The upper-case system on the British TYPEX cipher machine was non-standard and a combined U.S./U.K. system was therefore impossible until TYPEX was replaced. The CCM Replacement's Working Party suggested a system for combined use, to achieve compatibility between the AFSAM-7, AFSAM-47, the British SINGLET, and other U.K and U.S. machines. This comprised the Space key to piggyback on letter Z, switch to figures on J and switch to letters on V.

However, the design of the AFSAM-47 used eight upper case characters and was only compatible with the British SINGLET machine. Neither the limited nor extended upper-case system could be introduced until the British stopped using the TYPEX with BRUTUS adaptor. The limited upper-case system with numerals and space was eventually adopted for all combined cipher machines. Until a combined policy was agreed, all cipher machines designed for U.S./U.K. use should at least include the limited upper-case system.[16]

In October 1951, AFSA announced two types of operation. The AFSAM-7 traffic for high-level communications was designated ADONIS, and the traffic for the Army and Air Force designated POLLUX. The differences between the two crypto systems were the rotor sets, and the Message Rotor Alignment procedure at the start of each individual message.

In 1952, the British services wanted to use the BRUTUS crypto principle to replace the CCM, as agreed in 1951. However, analysis showed that initial and long-term costs for NATO requirements, parts and rotors were less expensive for ADONIS with 36-pins rotors, compared to BRUTUS.

Plans were made for a phased introduction of the ADONIS principle in combined machines by January 1955. ADONIS equipment would be made available to the U.K. until they could produce their own crypto machine with ADONIS principle, later designated SINGLET. The final production contract for the AFSAM-7 was signed on February 9, 1952.[17]

The U.S. urged to standardize ADONIS with 36-pins Red Rotors as they could apply the re-entry principle, which was impossible with 26 pins rotors. ADONIS also avoided the use of rotor cage adaptors to remain compatible with other combined cipher machines. AFSA's successor, the newly formed National Security Agency (NSA), also preferred ADONIS because the AFSAM-9 teletype encryption machine with nine 36-pins rotors, later renamed TSEC/KW-9, was also in development. As it turned out later, the TSEC/KW-9 pushed the speed of electromechanical encryption to its limit and suffered regular synchronization loss.[18]

In December 1952, the U.S. Office of Communications Security Conference discussed the replacement of the CCM. Participants were, among others, the U.S. Army, Navy, Air Force and cryptologists William Friedman and Albert Small. By then, the British used the early POLLUX principle. Although technically identical, ADONIS conveyed the Message Indicator (i.e. rotor start positions) in encrypted form to the receiver and the earlier POLLUX used a less secure method in clear. Friedman raised the question whether they should say nothing to the British about POLLUX being inadequate and ADONIS more secure.

Meanwhile, the production of the Navy AFSAM-47 kept delaying and the security of BRUTUS was questioned. One proposal was to improve security of the BRUTUS with its 26-pins rotors by adding a plugboard. Although this could make it more secure than ADONIS, the AFSAM-7 was already developed and in production by the Burroughs corporation. The BRUTUS based Navy AFSAM-47, manufactured by Teletype Corporation and subcontractors, was two years behind. The U.S. Army and Air Force preferred the AFSAM-7, and it could be made available for combined and NATO use by early 1955. The use of a plugboard for the AFSAM-7 was also briefly discussed, but Friedman argued that operators highly disapproved the idea because setting a plugboard was prone to errors, and also creates problems when a message from the previous day would arrive.

In the long term, the AFSAM-7 with 36-pins rotors was more secure than the Navy AFSAM-47 with 26-pins rotors because the AFSAM-7 would resist cryptanalysis longer than the AFSAM-47. According to Friedman, cryptologists from both the U.S. and U.K agreed against BRUTUS for the AFSAM-47. Albert Small also preferred the ADONIS principle, but the U.S. Navy insisted on continuing production of the AFSAM-47 with BRUTUS principle. Although the British also preferred BRUTUS, in the end it was practicality, production costs and quick replacement that prevailed.[19]

It was officially agreed that the SIGABA CCM machine, using the less secure AJAX principle, urgently required replacement, as all cryptanalytic attacks that worked on AJAX also worked on the CSP 2200, a modified SIGABA ECM Mark II. Friedman made it clear that ADONIS and AFSAM-7 were the answer to the CCM problem. Meanwhile, Navy tests on the AFSAM-47B, a modified AFSAM-47 with 36-pins rotors, compatible with ADONIS, were underway and already performed 100 hours on the KL-47 printer without error. However, any production of the AFSAM-47B was at least two years behind on the AFSAM-47 production.[20]

The Joint Chiefs of Staff therefore believed that replacement of the CCM by a machine with the BRUTUS principle should be suspended until service tests of the AFSAM-7 were completed. The Navy however insisted on keeping the AFSAM-47 with BRUTUS and wait to see if the AFSAM-7 ADONIS tests and production would succeed or fail, before redesigning their own AFSAM-47 with 26-pin rotors into the AFSAM-47B with ADONIS and 36-pin rotors.[21]

By November 1953, the British part of the COMSEC Conference, which assessed the security of cryptographic equipment, was not in favor of POLLUX, because using the Message Indicators in clear posed the risk of in-depth messages, and recovery of the key settings, certainly with high traffic volumes. In contrast, ADONIS was considered secure for all classifications for at least ten years, if good operating standards were maintained. U.S. cryptologists even considered the machine secure for the next twenty years. However, the British considered the AFSAM-47 with BRUTUS principle only secure for the next five years. They now also recommended to replace the British CCM as soon as possible, as that machine was regarded insecure within three years. The TYPEX II and Typex Mk 22 remained secure for the next five years.[22] [23] [24] [25] [26]

The AFSAM-7, favored by the NSA, eventually proved successful and the ADONIS principle was also chosen for the Navy AFSAM-47B. The NSA introduced the AFSAM-7 in the U.S. Armed Forces, and a smaller number of AFSAM-7s was also purchased by the Federal Bureau of Investigation (FBI) and the Central Intelligence Agency (CIA).

In March 1954, the U.S Joint Chief of Staffs approved the introduction of the ADONIS crypto principle, now used in both AFSAM-7 and AFSAM-47B, into the medium and high levels of NATO by mid-1956.[27] The AFSAM-7 was cryptographically more than capable to resist any attack at the moment of its release. In 1955, the AFSAM-7 was renamed TSEC-KL-7, according to the new nomenclature for crypto equipment, as determined by the NSC in 1954, where TSEC = Telecommunications Security, K = Cryptographic, L = Literal (ciphertext in letters).[28]

The AFSAM-47B was renamed TSEC/KL-47. Individual components of the KL-7 and KL-47 were manufactured by several different U.S. government-contracted companies. After final assembly at various locations, the machines became the property of the NSA and were distributed within the U.S. Although cryptographically compatible with the KL-7, the KL-47 still had the extended upper-case system with punctuations, while the KL-7 only had the limited upper-case system with numerals. Therefore, to avoid decryption errors, any message sent from a KL-47 to a KL-7 required spelling out the punctuation marks, or omitting them.

An ancillary Baudot paper tape reader called TSEC/HL-1 was developed for the KL-7 to enable directly reading and processing of five-bit level punched tape, as produced by standard teleprinters. This required the removal of the KL-7 keyboard and installation of the KLX-7/TSEC keyboard adaptor between keyboard and chassis.

In 1957, Boris Hagelin, engineer and founder of the Swiss firm Crypto AG, told NSA cryptologist William Friedman that he had filed a patent application for the re-entry principle in 1953. Hagelin's U.S. patent No. 2.802.047 was issued in 1957 and conflicted with the patent from Albert Small, who had already filed the application for patent in 1944, at the insistence of no less than William Friedman. Moreover, in 1956, Small had requested declassification of his pending patents, still under Secrecy Order.[29] [30]

The issue of conflicting patents had to be resolved. The NSA feared that sensitive information would be disclosed and preferred that the pending application from Albert Small was not made public, if Small would not acquire legal claims for compensation. Another option was to release only unclassified portions of the patents. Eventually, the conflict was solved, and Albert Small's Patent 2.984.700 was issued in 1961. Crypto AG also used the re-entry principle in its HX-63, twelve years after the introduction of the AFSAM-7.[31] [32]

## TEMPEST ISSUES

TEMPEST, the procedures and techniques to shield devices against eavesdropping on unintentionally emitted signals was in its early stages of research when the KL-7 was being developed. Although Bell engineers recognized the risk of unwanted stray signals as early as 1943, the initial attempts to reduce these signals were limited to filters on the power supply and shielding as much as possible. The first breakthrough came in 1956 with the introduction of low voltage circuits with transistors, but this was four years after the introduction of the KL-7, and the first extensive TEMPEST regulations were only drafted in 1958.[33] [34]

De KL-7 has a radio interference filter between the external power supply and its electronics, but some electrical contacts and coils could still be a source of unwanted signals. In 1955, the NSA conducted a study to determine whether the coil of the printer magnet, which activates the print hammer, would emit signals that could be exploited. These print coil signals were detectable up to 25 feet from the machine.

Analysis of recorded signals during decipherment of a message on the KL-7 showed that measuring the interval between the intercepted pulses of the print magnet, and knowing the order of the letters on the print drum, enabled the recovery of the plain text. Variations in the KL-7 motor speed between pulses could complicate measurement of the intervals, but other signals, radiated at the same distance, could determine the change of motor speed, making recovery of the plain text much easier. They also found a correlation between the number of rotors that stepped and print drum speed deviations.

The KL-7 remained in use without additional technical changes to reduce unwanted signals, but the 1958 TEMPEST regulations undoubtedly advised operating the machine at fixed or tactical locations were eavesdropping at close range was unlikely. Nevertheless, even at secure locations, unwanted signals could unexpectedly piggyback on other equipment and enable eavesdropping from far greater distances.[35]

## THE KL-7 IN SERVICE

The KL-7 was initially only intended for use by the U.S. Army, Air Force, Navy, the CIA and FBI. During the 1953 Communications Security Conference in London, the NSA proposed to share the ADONIS crypto principle with their NATO allies. The goal was to improve communications security and interoperability, and to replace the less secure Combined Cipher Machine (CCM) by the AFSAM-7.

From 1951 to 1954, the Army Security Agency (ASA) procured 6547 units. Once delivered, they would replace the less secure M-209. The FBI placed an order for 120 AFSAM-7s, 120 Office Cases at $100 each, an additional 120 AFSAM-207 Cipher Units (i.e. KLK-7/TSEC) at $50 each, 250 sets of Rotors (two per machine to enable swift daily key change), 5 spare AFSAM-107 Stepping Units (i.e. KLA-7/TSEC), 5 spare AC Power Converters at $25 each, paper tape and ink ribbons. The order totaled $258,900. However, by 1953, the cost of the FBI order had risen to $299,232 ($3,365,084 in present 2022) due to rising production costs.[36]

ASA initially received 650 AFSAM-7s of which 120 for the FBI. These were gradually issued, two per FBI office. Meanwhile, the twenty FBI offices with the highest message volume already received AFSAM-7s on loan from the NSA, and the NSA would also train FBI personnel in operating the AFSAM-7. The CIA received its first four AFSAM-7 for local testing in 1954 but use in the field only started the following year.[37] [38]

By 1954, all FBI offices, Quantico, the White House Signal Detachment (WHSD), the Seat of Government, and President Dwight Eisenhower's Air Force One were equipped with the AFSAM-7. However, many AFSAM-7s from the early production runs had several technical issues. In April 1954, the NSA director received a list of deficiencies, noted by the Chief Army Field Forces during testing.

To meet the performance standards, ASA requested modifications for a total of 2339 AFSAM-7s from the 1st, 2nd and 3rd production run, at that moment in storage facilities. These were returned the next month to the Burroughs Corporation. When the second shipment arrived at ASA, it was discovered that 615 from the 1400 already delivered AFSAM-7s required modifications. As a result, machines from the White House, ASA Europe and ASA Pacific had to be replaced by modified versions.[39] [40]

The U.S. Joint Chiefs of Staff approved the use of the AFSAM-7 by NATO in 1954. The plan was to introduce the machine to medium and high levels by mid-1956. The NSA did recognize that the AFSAM-7, or reproductions with the same cryptographic principle, would eventually also find their way to non-military use in those countries, or might even end up in Soviet hands.

The NSA was confident the AFSAM-7 was secure against any attempt by the Soviets to decipher the messages, even when its cryptographic principles and specifications were compromised. The machine was therefore certified for Top Secret messages at the start of its career.

Meanwhile, the new British BID/60 SINGLET crypto machine was developed with identical crypto principle as the AFSAM-7, to replace the outdated CCM (LUCIFER), which was the British CCM-Typex, interoperable with the American CCM/SIGABA. The SINGLET greatly resembled the AFSAM-7, and used rotors that were identical to those of the AFSAM-7, but was not expected to be in production before 1960. In 1954, the U.S. decided to make available 3,500 AFSAM-7 units to the United Kingdom, and 3,000 units to other NATO countries. These machines were on loan and remained property of the NSA.[41]

In early 1955, the Standing Group of the North Atlantic Military Committee (NAMC), which provides policy guidance, decided to supply the AFSAM-7 to Supreme Allied Commander Europe (SACEUR) for further distribution to all NATO members.[42] Target date to replace the CCM by the AFSAM-7 was 1 July 1956. Meanwhile, the AFSAM-7 was renamed TSEC/KL-7.

In 1955, the U.S. Army Security Agency Europe assigned two military instructors to NATO. They assisted in training of NATO personnel, designated to repair and maintain the TSEC/KL-7. Those who attended the maintenance school had to be qualified as teletypewriter mechanic and have the proper security clearances. Basic knowledge of electronics was also desirable.[43] [44]

In September 1955, the NAMC listed the provision of KL-7s. The then current allocation quantities were for Belgium 156, Denmark (including Greenland and Faeroes) 158, France 711 (including the Commander Biscay Atlantic sub-area and the Commander Moroccan Atlantic sub-area), Greece 200, Italy 603, Luxembourg 15, Netherlands 239, Norway 169, Portugal (including the Commander Continental Portugal and the Island Commanders of Azores and Madeira) 168. Each country's Ministry of Defense Army, Navy and Air departments received 4 KL-7s each, and the Supreme Commanders 12 KL-7s.

In the Allied Headquarters, the HQ commanders in chief received 12 KL-7s. The Allied Land Commands, Allied Army Groups & Tactical Air Forces, and the Armies & Tactical Air Forces 8 KL-7s each. The Army Corps & Air Divisions received 6 KL-7s, The Army Division, Air Force Escadres, and Wing Groups 3 KL-7s. The independent brigades 2, National District Commands 2, major fleet Bases 4, Island Commands 3, Patrol Force Commanders and Flag Officers 2 each, Naval and Maritime Air Bases 3. The ocean-going aircraft carriers, battleships and cruisers 2 each, destroyers, destroyer escorts, submarines and Patrol Coastal boats 1 each. Temporary or alternative Naval or Maritime Air bases received 2 KL-7s.[45]

Note that 3,500 units were already assigned to the UK in 1954. In the following years, more KL-7s were allocated to additional countries and military echelons, with the 1965 allocations as the last known.[46]

In 1956, NATO decided to order the HL-1 tape reader and KLX-7/TSEC keyboard adaptor to cope with the increasing volume of encrypted traffic.[47] The NATO members had to determine their required stock of KL-7 spare parts, and could also order a kit with basic spare parts at the price of $150 per machine. The spare parts and kits were gradually delivered between 1957 and 1960.[48] [49]

Also in 1956, the CIA's Operations and Training Division planned the AFSAM-7 for mobile message centers. Noise issues were solved with a soundproof container and a keyboard adaptor became available in 1957. That year, CIA O&T personnel also visited the NSA to observe the HL-1 tape reader that could process perforated tapes. The HL-1 was later installed on loan at the CIA Signal Center.[50] [51] [52]

In 1957, NATO agreed to adopt the KL-7 for second level NATO use, and for first level NATO use with ADONIS key lists, to replace the Typex (SIMPLEX) traffic that used the Typex II with SIMPLEX pads. This agreement also comprised each NATO member's Ministries of Defense and Foreign Affairs, their embassies in Paris and Washington, and their National Military Representative in Washington.[53] They extended the use of the KL-7 to minesweepers, fast patrol boats and long-range maritime aircraft in 1958.[54]

Besides the United States, the KL-7 was used by its NATO allies Australia, Belgium, Canada, Denmark, England, France, Federal Republic of Germany (former West Germany), Greece, Italy, Luxemburg, the Netherlands, Norway, New Zealand, Portugal and Turkey. Outside NATO, the KL-7 was also on loan to South Vietnam, South Korea and Nationalist China.[55]

Some clarification on those last three countries. South Vietnam, officially called Republic of Vietnam (RVN), existed from 1955 until the North Vietnamese victory in 1975 and formation of the current Socialist Republic of Vietnam (SRV). South Korea, officially the Republic of Korea (ROK), was formed in 1948 with the division of the Korean peninsula in two political entities along the 38th parallel, with the U.S.-backed South Korea, and Soviet-backed North Korea, officially the Democratic People's Republic of Korea (DPRK). The Republic of China, often called Nationalist China, was formed in 1912 by the Kuomintang. After the 1949 communist takeover, the Kuomintang fled to Taiwan, since then officially called Republic of China (ROC), which is disputed by mainland People's Republic of China (PRC) to this day.

In 1958, the price per KL-7 totaled $1458. The set comprised the KLB-7 base at $814, KLA-7 stepping unit $328, KLK-7 cipher unit $80, CE87054 Carrying Case $161, CE87066 AC Power Converter $75 and a set of rotors $100. A complete KL-7 would cost $15,748 when converted into present 2024.[56]

The extended use of the KL-7 was discussed, and NATO member Canada pointed out that the KL-7 had not yet reached 100% reliability, due to problems with the pulse generator, and a book cipher as back-up would be essential. The KL-7 was also used on NATO submarines. In 1959, they approved the Basic Submarine Code as back-up system for the KL-7. The code, in itself not secure enough, was used in conjunction with letter one-time pads.[57] In December 1959, NATO also authorized the use of KL-7 ADONIS for first level military and diplomatic traffic.[58] By 1966, some 25,000 KL-7 were produced for the U.S. and their allies. [59]

When France left NATO's military structure in 1966, NATO needed a separate crypto system to exclude France from their most sensitive communications. Initially, two new KL-7 ADONIS key lists and a new set of rotors with other internal wiring were introduced. NATO did continue to distribute COSMIC TOP SECRET key lists to France, but introduced separate key lists for the other NATO members, from which the French were excluded. The KL-7 key lists for General Small Ships, the Maritime Patrol Aircraft, Atlantic Channel North Sea and Baltic Area remained available to France.[60]

Despite its extensive use in many armed forces, the KL-7 was not always the most popular machine. The KL-7 was notorious for its keyboard and rotor contact problems. The operator often had to push firmly on the keys to get the machine cycling, not allowing him to get any speed. Dirty contacts and the beryllium copper issue could cause the machine to halt, the notorious so-called dead-rove. To avoid these problems, the rotors and keyboard contacts had to be cleaned regularly and meticulously.

The contact problems with keyboard and rotors were inherent to the design with numerous moving electrical contacts. In Plain mode, the signal from key to printer pulse coil only had to pass two contact points on the keyboard’s sliding contact board. In Cipher or Decipher mode, the route from key through all rotors to pulse coil passed at least 13 contact points.

However, due to the re-entry principle, the encrypted output could loop back to the input, through one of the ten re-entry wires, and re-encrypted again through the eight stepping rotors, resulting in up to ten passes through all rotors and their numerous contacts. In that case, a total of up to 472 contact points must function flawlessly. Dirt or copper oxide on one single contact point could therefore interrupt the electrical signal and halt the machine permanently, requiring extensive cleaning of all rotors and keyboard contacts.

During start-up, the electron tubes need 16 seconds to heat up before you can type on its keyboard, as the printer is controlled by the electron tubes. The KL-7 also has a high acoustical signature. When the KL-7 is turned on, the DC motor slowly takes speed, and the reduction gears produce a characteristic high-pitched noise. The advancing rotors also produce their own typical sound.

During its service time, the rotors of the KL-7 and KL-47 were regular rewired. Some rotors were rewired on a yearly basis on national or NATO level, and some rotors, often referred to as the NSA rotors, were to be sent directly to the NSA for rewiring by NSA personnel only. It was strictly forbidden to operators, even to the maintenance technicians with crypto clearance for KL-7, to check out the internal wiring of the rotors.

The technicians were not allowed to test the rotors pin-to-pin. They were instructed to place a defective rotor on a large conductive plate that made contact with all rotor pins at once, and then check out the connection on each pin at the other side with an Ohm meter. This way, the technician would see if a wire was broken, but didn’t know to which pin it corresponded to the contact on the other side.

There were some incidents where a KL-7 or KL-47 was compromised. One well known incident is the seizure of USS Pueblo by North Korea in 1968. Officially, the ship was an AGER-2 (Auxiliary General Environmental Research). In reality, the ship was stuffed with SIGINT (Signals Intelligence) and ELINT (Electronic Intelligence) equipment to eavesdrop on North Korean and Soviet communications. When the North Koreans attacked and boarded the ship, the U.S. Navy immediately stopped all communications with the KL-47 until the NSA had distributed new key lists. The machine itself was designed to resist cryptanalysis, even when the technical specifications were known to the adversary. What they didn’t know was that some KL-47 key lists were already compromised.[61]

During the Vietnam War, KL-7s were loaned to the Army of the Republic of Vietnam (ARVN). The COMSEC support for the KL-7 was organized by the ASA, located at Tan Son Nhut Air Base in Saigon (today Ho Chi Minh City). The Special COMSEC Support Unit at the Air Base provided crypto maintenance down to component level. Their mission, among others, was to support the crypto unit of the ARVN and to train them to perform basic maintenance and operating the KL-7. The Australians and New Zealanders also used the KL-7 in Vietnam.[62]

In 1965, the 101st U.S. ASA Security Detachment, operating under cover designator 7th Radio Research Unit, was based in Saigon. The 7th RRU conducted Signal Security analysis (SIGSEC) and performed cryptographic security analysis of the ARVN's use of the KL-7, to ensure the machines were used as prescribed. The 7th RRU concluded that the ARVN became quite proficient in using the KL-7.[63]

The U.S. forces in Vietnam used the KL-7 from division down to company level. However, a 101st ASA Detachment analysis revealed that Communications Security (COMSEC) was often neglected in the heat of battle. Operation SILVER BAYONET, with the famous Battle of Ia Drang in 1965, showed that a combination of underestimated enemy strength and poor COMSEC can cause heavy losses. The KL-7 was not used for intra-battalion communications and on lower echelons. Instead, they used manual systems, often cryptographically less secure or even plain unencrypted messages over radio.[64]

In the course of the Vietnam war, and also after the withdrawal of most U.S. troops in 1973 and the subsequent defeat of the ARVN in 1975, all kinds of crypto equipment fell into the hands of the North Vietnamese Army (NVA), including some KL-7s. One of those machines, a KL-7 belonging to a U.S. Marine unit, was handed over to the Russians who sent it to the Soviet Socialist Republic Poland for analysis. After the dissolution of the Soviet Union, Polish officials handed over that KL-7 to the NSA and is now in NSA's National Cryptologic Museum collection.

Advances in technology and the introduction of miniature electronic components increased the computational power to support cryptanalysis tremendously. As a result, the KL-7 was no longer considered secure enough by the mid-1960s and vital message traffic, enciphered with the KL-7, was often superenciphered (i.e. double enciphered) on other systems.

During the Cold War, signal units from several NATO member states provided secure communications to NATO in West Germany. From the early 1960s, NATO's Joint Headquarters in Rheindahlen was supported by British signal personnel and communications by teleprinter was online real-time encrypted with one-time tape mixers. Although they also used the KL-7, the offline encrypted KL-7 messages left the cipher room in five-letter groups, printed on paper strips and stuck onto A4 pages or message forms. These ciphertext groups were typed out onto punched teleprinter tapes for onward transmission and sent online, superenciphered using the ECOLEX one-time tape mixer.[65] By the 1970s, the KL-7 was largely replaced by the long-existing KW-37 JASON, KW-26 ROMULUS and KW-7 ORESTES online cipher equipment, and the fully electronic KL-51 RACE off-line cipher machine could be regarded as its successor. Some KL-7s stayed in service, mostly as back-up, and retired in the early 1980s.

Although the KL-7 was only meant to be used by the U.S. military, its NATO allies and some state departments, there are some cases where civilians operated the KL-7. One such case was the 1982 Falklands War. Within a few days, the British Navy had to sail a huge naval task force across the South Atlantic. They quickly chartered merchant ships to support the operations. One of them was the Eburna tanker, carrying fuel oil, diesel and aviation fuel, to transfer fuel at sea. The civil radio officers had no experience with naval communications or crypto systems and had to learn the basics of cryptography and operating the KL-7 within short time.[66] The last known recorded message, enciphered with a KL-7, was sent by the Canadian armed forces in June 1983.

## MAJOR SECURITY BREACHES

In 1974, a highly sensitive and well-placed source told the FBI that the Soviet foreign military intelligence directorate GRU had an agent with codename "Greenwood", who was an American from the U.S. military that had been posted in France and Vietnam. The FBI started counterintelligence operation "Hookshot" to identify the person, and the U.S. Army

Intelligence and Security Command (INSCOM) narrowed down the search to Joseph Helmich (1937-2002), a former U.S. Army Signals Warrant Officer who served in 1963 as crypto custodian in France, in 1964-65 in Vietnam with crypto clearance in a supply unit, and later at Fort Bragg, North Carolina. The FBI started an extensive investigation with surveillance.

In 1963, being faced with financial problems, Helmich had contacted the Soviet Embassy in Paris, France. He received $131,000 in return for technical information on the KL-7, at that moment the most widely used cipher machine in U.S. military. After returning to the United States, Helmich continued to provide KL-7 key lists to the Soviets until 1966, enabling them to decrypt KL-7 messages from U.S. troops and Military Intelligence units in Vietnam.

Although already under suspicion in 1964, because his wealth did not match his pay grade, it was only during an FBI surveillance in early 1980 that they observed him visiting the Soviet embassy in Canada to contact the KGB. After extensive interrogations, Helmich eventually confessed in 1981 and was sentenced to life imprisonment.[67] [68]

In 1985, the FBI received a tip from the ex-wife of John Walker (1937-2014), a retired U.S. Navy communications specialist. During FBI surveillance he dropped a grocery bag alongside a road, north of Washington D.C. The bag contained 129 copies of stolen secret U.S. Navy documents. At the same moment, a few miles further, a Soviet KGB agent left a grocery bag with $200,000. This was clearly a dead drop exchange to covertly exchange documents and money without meeting face-to-face. The following night, John Walker was arrested by the FBI in a motel.

The investigation shook up the military intelligence community. As later turned out, already in 1967, Chief Warrant Officer John Walker simply walked into the Soviet Embassy in Washington DC with a KL-47 key list and offered the Soviets to sell secret Navy documents for cash.

It was the beginning of a spying career of no less than 18 years. During a search of his house, the FBI discovered a special device, provide by Soviet Intelligence, to read the internal wiring of the KL-47 rotors. During interrogations, Walker admitted providing the Soviets with a complete technical maintenance manual, which enabled the reconstruction of a fully operational KL-47, cryptographically identical to the KL-7. He was also sentenced to life imprisonment.[69] [70]

## FINAL THOUGHTS

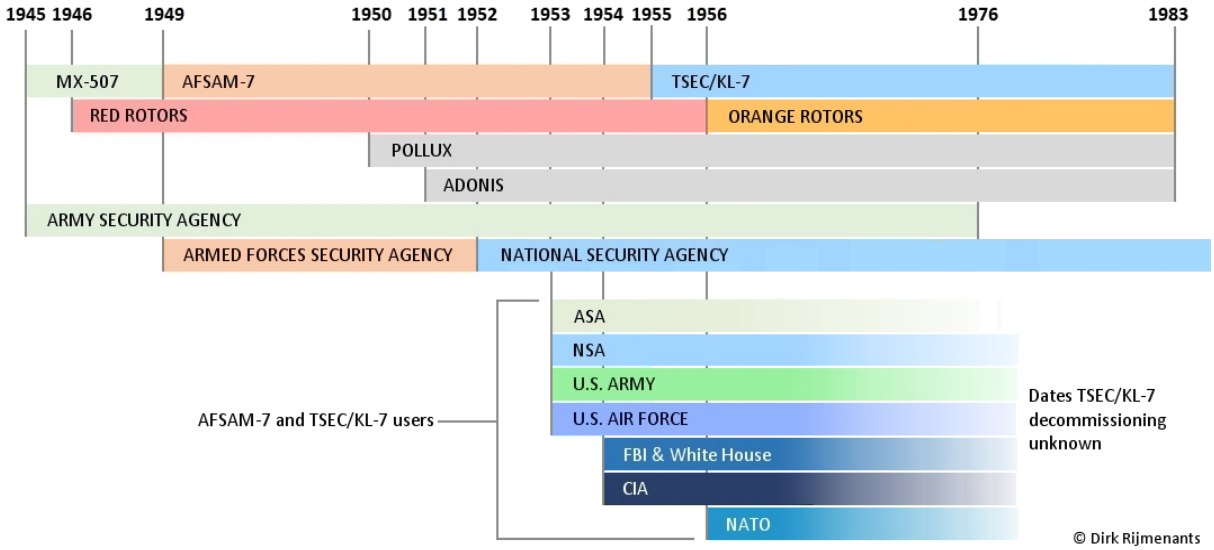
The KL-7 is a unique machine in several ways. It was the first machine, developed under a centralized cryptologic organization, and introduced as a standard crypto device in all parts of the U.S. armed forces and their allies. At that time, the KL-7 used the latest cryptologic techniques and was the first ever cipher machine with electronics, yet its rotor-based design would soon lose the battle against miniaturization of electronics and computational power. The KL-7 was one of the last purebred electromechanical cipher machines.

The compromise of some key sheets and disclosure of its technical details did not compromise all communications with the KL-7. Different key settings, also called crypto nets, are used for different services, military units, echelons, and at separate geographical locations. This practice, called compartmentalization, prevents a broad compromise of all communications when one single key setting is compromised.

The importance Soviet Intelligence gave to the KL-47 key lists, despite possessing all technical details of the machine, shows they probably were unable to break the KL-47 or KL-7 message traffic purely by cryptanalysis, or they didn't have sufficient computing power to decipher them within reasonable time for practical use. Many operators cursed the machine for its quirky keyboard and contact problems, requiring regular maintenance. They welcomed its fully electronic successors, but today speak with sentiment about that wonderful machine and even vividly remember the typical sound of its stepping rotors.

Although less known to the general public than the WWII German Enigma machine, the superior KL-7 served decades in many countries around world, collecting secrets and memories about the Cold War, companionship, and even exciting stories about treason and espionage. The KL-7 is a true Cold War cryptologic icon.

**TSEC/KL-7 TIMELINE**




The above timeline shows the development from MX-507 project to AFSAM-7 and TSEC/KL-7. The ASA developed, procured, and issued the machines. From 1949 on, the AFSA and its successor NSA were responsible for communications security. Although the AFSAM-7 existed on paper in 1949, it took two years from the 1950 engineering model to the actual production start in 1952, and delivery to the Armed Forces only started in early 1953. The POLLUX procedure for low-level traffic was adopted in 1950 and the more secure ADONIS procedure for high-level message traffic was added in 1951. Due to persistent problems, the Red Rotors were replaced by the Orange Rotors in 1956.

Although the NSA succeeded AFSA in 1952, the machine's name only changed to TSEC/KL-7 in 1955. The newer machines, produced from 1955 on, carried the name TSEC/KL-7, and older production runs were gradually retrofitted with the new name labels. Exact dates of final decommissioning of the KL-7's are unknown, as they were gradually recalled from the many different services and countries.

## BIOGRAPHICAL SKETCHES

Dirk Rijmenants has a passion for all things radio, electronics, programming and cryptology. During his 39-year career, he worked with a wide variety of COMSEC equipment, and on some as technician. Since 2004 he runs the Cipher Machines and Cryptology website and SIGINT Chatter blog to share his interest in cryptography, military and intelligence history.

## REFERENCES

All following documents are declassified and publicly available. Some references include page numbers to the relevant information. However, different versions of some documents exist, and page numbers may therefore vary, requiring the use of a search function to find the relevant information.

Some organizations or authors impose conditions or limitations on public or commercial use of their documents. The NSA documents are released through their Declassification & Transparency Initiatives, Freedom of Information Act releases (FOIA), the William F. Friedman Collection, and NSA Historical Releases. Other sources include FOIA's and historical releases, preserved by the National Security Archive and governmentattic.org, the CIA Reading Room and the Internet Archive. Please consult their terms of use. All NATO documents are from the NATO Archives Online at https://archives.nato.int. Please consult their guidelines for use, permission and credits. All referenced documents are also available at the KL-7 webpage: https://www.ciphermachinesandcryptology.com/en/kl-7.htm

---

[1] NSA - Repair and Maintenance Instructions for TSEC/KL-7 (AFSAM 7) Joint, 1955. Declassified 30 Mar 2009, FOIA Case #47709 by Bill Neill, and published by Nick England.

[2] NSA - Operating Instructions for TSEC/KL-7 ADONIS Operation, September 1966. Canadian CSEC information declassified and released 28 April 2001 CSEC ATIP Cace#A-2010-00015. NSA information declassified and released 21 April 2011, FOIA Case #64246.

[3] NSA - A History of U.S. Communications Security - David G. Boak Lectures, Volume I, original p33, July 1973. Released in 2015, ISCAP No. 2009-049.

[4] U.S. National Archives, Records of the National Security Agency/Central Security Service (NSA/CSS). Record Group 457, 1917-93. Timeline with dates establishment U.S. Army cryptologic services SIS, SSA and ASA.

[5] NSA - Post War Transition Period, the Army Security Agency 1945-1948, 7 April 1952. Declassified for release by NSA on 05-31-2016 pursuant to E.O. 13526, MDR Case 82626.

[6] NSA - The Early History of NSA by George F. Howe. Approved for release by NSA 18 Sep 2007. FOIA Case #7319.

[7] Joint Chiefs of Staff - Memorandum AFSA 1949, JCS memorandum to director of Armed Forces Security Agency on establishment of AFSA. ID A68965 Declassified for release by NSA on 12-04-2014 pursuant to E.O. 13526.

[8] AFSA Armed Forces Security Agency Council, establishment Armed Forces Security Agency, 1951. Doc ID A68919. Declassified for release by NSA on 1 March 2014 pursuant to E.O. 13526

[9] NSA - Cryptologic Almanac 50th Anniversary Series, AFSAM-7, p1-p3. Doc ID 3575720. Declassified and released by NSA 10 April 2007 pursuant to E.O 12958, as amended. MDR 51909.

[10] NSA - U.S. Signal Corps Patent Board, Meeting No 30, 1940. Friedman Collection, document ID A104884. The process of altering characteristics of Cryptographic Devices by Re-Cipherment or Re-Codement by Mr Albert W. Small, Junior Cryptanalyst.
[11] NSA - A History of U.S. Communications Security Post-World War II, Equipment - Part II, A.4, Rotors and Rotor Development, p80-84. Released 4 February 2011, pursuant to E.O. 13526. MDR59142, published by governmentattic.org
[12] NSA - Cryptologic Almanac 50th Anniversary Series, AFSAM-7, David A. Hatch, NSA doc ID 3575720. Declassified and released by NSA 10 April 2007 pursuant to E.O 12958, as amended. MDR 51909.
[13] NSA - Minutes of an ad hoc committee of the BRUSA COMSEC Conference, held on 30 September 1950. NSA Friedman Records, doc ID A67271.
[14] NSA - The National Communications Security Materiel Program, September 1954. Friedman collection, doc ID A61110. Declassified and released 30 January 2014 pursuant to O.E. 13526.
[15] NSA - Cryptologic Almanac 50th Anniversary Series, AFSAM-7, p5.
[16] NSA – Report of the U.K./U.S. Communications Security Conference Held in London In July 1951. Friedman records A67165. Released 20 May 2014.
[17] NSA - Memorandum for Members AFSAC, Replacement or the Combined Cipher Machine, 24 December 1952. Friedman Records, doc ID A59485.
[18] NSA - A History of U.S. Communications Security - David G. Boak Lectures, Volume I, original p33, July 1973. Released 14 October 2015, ISCAP No. 2009-049.
[19] NSA - Transcript of Office of Communications Security Conference, Replacement of the Combined Cipher Machine, 22 December 1952. Friedman Collection, document ID A59490. Released on 28 January 2014 pursuant to E.O. 13526.
[20] NSA – Letter AFSA Director Gen. Canine to Chief Division of Cryptography Department of State, Capt. Parke, Memo for Record, 24 June 1952. Attacks on AJAX, Hermes and CSP 2200 (HCM Mark 4). Released 19 Sept 2013. ID A272413,
[21] NSA - JCOS Staff Meeting, Replacement Combined Cipher Machine (CCM), 1953. Friedman collection, doc ID A59449. Released 27 January 2014 pursuant E.O. 13526.
[22] NSA - UK/US Communications Security Conference 1953 Report Sub-Committee to the Executive Committee - Security assessment of cryptographic equipment in use and under development, pdf p4-p5. NSA ID A522921. Released 27 May 2014 pursuant to E.O. 13526
[23] NSA - U.S. Communications Security Equipment, Part I, Literal Cipher Machines - AFSAM 7, AFSAM 47B, 1953. Friedman collection ID A522530, released 11 November 2014 pursuant to E.O. 13526.
[24] NSA - JCOS Staff Meeting, Replacement Combined Cipher Machine (CCM), 1953. Friedman collection, NSA doc ID A59449. Released 27 January 2014 pursuant E.O. 13526.
[25] NSA - Memorandum USCIB, Disclosure ADONIS Cryptoprinciple to NATO Countries, 30 September 1953. Friedman documents, NSA doc ID A61288.
[26] NSA - Program to Improve the Communications Security of NATO Countries, 21 September 1953. Memorandum for the Members of USCIB, Friedman documents, NSA doc ID A61293.
[27] NSA - Memorandum for the Members of USCIB, 3 May 1954. Release of AFSAM-7 to NATO Nations. Friedman documents, NSA doc ID A61057. Released 21 April 2014.
[28] NSA - Nomenclature For Communications Security Materials, 24 November 1954, doc ID A66119. Released in 2014 by NSA, pursuant to E.O. 13526.
[29] Patent nr 2,802,047 from August 6, 1957, B.C.W. Hagelin, Electric Switching Device For Ciphering Apparatus. Filed Oct. 16, 1953, ISCAP No. 2009-049
[30] NSA/CSS Archives, Memorandum For The Record, Hagelin Negotiations, 18 December 1957, report Friedman's visit Hagelin Laboratories, conflicting re-entry principle patents, NSA doc id A60669.
[31] NSA - Applications for Patent of Albert W. Small. NSA Chief Patents Branch, 27 February 1956. Request for declassification of re-entry principle, NSA doc ID A58689.
[32] A. W. Small, 1944 U.S. Patent 2.984.700, Method and Apparatus for Cryptography, re-entry principle filed Sept. 22, 1944. Issued May 16, 1961, after solving patent conflict.
[33] NSA - History of U.S. COMSEC, Vol I, 10th Lecture Tempest, original p89, and Vol II Tempest lecture (update) original p39. Release 14 October 2015.
[34] NSA - TEMPEST: A Signal Problem. Released by NSA on 27 September 2017, FOIA Case #51633.

[35] NSA - Plain Text Radiation Study of TSEC/KL-7 (AFSAM 7), Donald E. Schumacher, 2 August 1955.
[36] FBI - Automatic Ciphering Equipment, Note Mr. Harbo to D.J. Parsons. Purchase of 120 AFSAM-7, office cases, cipher units, rotor sets. FBI Record/Information Dissemination Section Records Management Division, FOIA Black Vault, pdf p46-47, 74-76,178 from 29 Sept 2015.
[37] FBI - Letters J.E. Hoover on FBI Bureau Codes, distribution TSEC/KL-7 (AFSAM-7), key lists FBI offices, training, 1960. SENSTUDY 75: FBI Files Shared with Church Committee (62-HQ-116395), p.3, p.5, p.17.
[38] CIA, Newsletter Sept. 9, 1953. Delivery AFSAM-7 in October 1953. Released 30 March 2001, FOIA CIA-RDP78S05452A000100030020-2.
[39] FBI - Memorandum of Conference AG's July 13, 1955, J.E. Hoover. AFSAM-7 procured for all field offices, Quantico and Govt. Government, pdf p257-262. FOIA No. 1145592- 00 governmentattic.org
[40] ASA, History of the Army Security Agency and Subordinate Units, Fiscal Year 1954, Volume I, Procurement of Cryptographic Equipment, p43-47. NSA Doc ID 6582943.
[41] NSA - Report of the U.K./U.S. Communication Security Conference 1953, sharing 3,500 AFSAM-7 to U.K. and 3,000 to other NATO countries. Friedman Documents, NSA Doc ID A523031.
[42] NATO – Memorandum SACEUR, proposed distribution of AFSAM 7 to NATO, target date 1 July 1956. NATO Doc Item SGM-179-55.
[43] NATO - Cryptographic Arrangements for NATO. KL-7, Typex SIMPLEX and Typex LUCIFER, NATO doc Item SGM-0287-56.
[44] NATO - Training of NATO Command and National Personnel in Operation, Maintenance and Repair of the TSEC/KL-7, 19 August 1955. NATO doc Item SGM-0586-55.
[45] NATO -Provision of an Off-Line Cipher Equipment for NATO use, 14 September 1956. NATO doc item SGM-687-55
[46] NATO - Allowance Table for ADONIS Equipment, 29 March 1965. list of countries and allotted KL-7 per department and military levels. NATO doc Item SGM-0115-65.
[47] NATO - Availability HL-1 and KLX-7, 23 March 1959. Request Federal Republic of Germany for 38 TSEC/HL-1 and KLX-7/TSEC. NATO doc Item SGM-0181-59.
[48] NATO - Automatic Use of the KL-7. TSEC/HL-1 tape reader and KLX-7 keyboard adaptor, 18 May 56. NATO doc Item SGM-0792-56.
[49] NATO - Policy Ordering and Maintaining Supply Spare Parts TSEC/KL-7, 21 December 1956. NATO doc Item SGM-0854-56.
[50] CIA - Monthly Report 1-30 Sept. 1956 Systems Engineering Branch - Engineering Division, AFSAM-7 for Mobile Message Center, noise issue, keyboard adaptor, pdf p4, p7. Released 17 July 2001, FOIA CIA-RDP78-02820A000100080017-4.
[51] CIA - Trip to NSA by O&T and Security Divisions, 9 August 1957. Released 13 November 2002, FOIA CIA-RDP78-02820A000300010030-4.
[52] CIA - operation 1951-66, AFSAM-7/KL-7 use at CIA Headquarters Signal Center, p82-87. Released 28 October 2004, FOIA CIA-RDP84-00499R000400080001-4.
[53] NATO - Replacement First Level Typex-Simplex Channels, 9 September 1957, including list of Ministries of Defense, Ministries Foreign Affairs, Secretary of State for External Affairs. NATO doc Item SGM-0588-57.
[54] NATO - Extension Use TSEC/KL-7 for General NATO Communications, 10 September 1958. NATO doc Item MCM-0115-58.
[55] NSA - Records related to the charter and meetings of the USCSB from 1940-1980. United States Communications Security Board (USCSB). Minutes of the Thirteenth Meeting 23 November 1970, governmentattic.org pdf p43.
[56] NATO - TSEC/KL-7 Meteorologic Use. Minesweeper, Patrol Boat, Maritime Aircraft, including price KL-7 and parts, 9 April 1958. NATO doc Item SGWM-208-58.
[57] NATO - Submarine Code in Conjunction with One-time Pad as Backup for KL-7, 24 February 1959. Use for command to all subs, and subs only to command. NATO doc Item SGM-0116-59.
[58] NATO - TSEC/KL-7 ADONIS Systems for National Traffic, 4 December 1959. Authorization for national military and diplomatic traffic. NATO doc Item SGM-0688-59.

[59] NSA - TSEC/KL-7 Canadian Senior Liaison Officer Washington, Canadian User Report After First Year of Operation, Report on First Year, including Interim Operating Instructions for Pollux Cryptosystems-Joint, January 1959.
[60] NATO - Distribution Cryptomaterial, 1 May 1967. After France leaving NATO, separate KL-7 key lists issued to France. NATO doc Item IMSWM-059-67.
[61] NSA - Cryptographic Damage Assessment, USS Pueblo, AGER-2, 23 January - 23 December 1968. NSA Doc ID 3075790. Released 2012 FOIA Case #40722.
[62] The KL-7 in Vietnam. COMSEC Support for the TSEC/KL-7 at Air Base Saigon, D. Maring, 2024.
[63] NSA - National Security Archive Electronic, Briefing Book No. 90, Dubious Secrets, Document 13A, Annual Historical Summary U.S. Army Security Agency, FY 1965. U.S. 101st USASA Security Detachment 7th RRU, Saigon, Vietnam.
[64] NSA - Working Against the Tide (COMSEC Monitoring and Analysis) Part Two, Chapter III - COMSEC Surveillance. June 1970. Viet Nam War era. Battle of Ia Drang 1965. Use of KL-7 at division down to company level, p90-95. Released 2004, FOIA #41608.
[65] The KL-7 at NATO in West Germany. ET's Story on OTT Mixers and the TSEC/KL-7, M. Davies, 2024.
[66] The KL-7 on Merchant Ships During the 1982 Falklands War, Operation Corporate and the KL-7 Cipher Machine on the Eburna Tanker, B. Kates, merchant ships civil radio officer, 2017-2022.
[67] FBI - Operation Hookshot, counterintelligence operation and identification Joseph George Helmich. NSIA-FBI files, National Security Archive, archive.org
[68] DNI - Office Director of National Intelligence, Counterintelligence - CI References, CI Reader Volume III. p265, Joseph George Helmich.
[69] DNI - Office Director of National Intelligence, Counterintelligence - CI References, CI Reader Volume III. p233, John Anthony Walker.
[70] U.S. Army Command and General Staff College - Analysis of the Systemic Security Weaknesses of the U.S. Navy Fleet Broadcasting System, 1967-1974, as Exploited by CWO John Walker. Major Laura Heath thesis.