**COMSEC**

From Wikipedia, the free encyclopedia

*Not to be confused with* [*Commonwealth Securities*](http://en.wikipedia.org/wiki/Commonwealth_Securities)*.*

The compound word **COMSEC** is prevalent in the [United States Department of Defense](http://en.wikipedia.org/wiki/United_States_Department_of_Defense) culture with hundreds of secondary and tertiary words. Historically, it is originated from [**COM**munications **SEC**urity](http://en.wikipedia.org/wiki/Communications_security); however, in the 21st century, the compound word is used without regards to its origin in thousands of pages of manuals and documents and by millions of personnel over the last fifty years. Another example is OK in the current culture; almost detached from its historical origin. Its [taxonomy](http://en.wikipedia.org/wiki/Taxonomy) has created hundreds of terms, processes, devices, and concepts. Some of the main ones, related phrases and devices, are defined here to standardize the comprehension in reading the COMSEC documents and talking to people with COMSEC experience. [COMSEC equipment](http://en.wikipedia.org/wiki/COMSEC_equipment) provides [security](http://en.wikipedia.org/wiki/Security) for [telecommunications](http://en.wikipedia.org/wiki/Telecommunications) by converting information to a form unintelligible to an unauthorized [interceptor](http://en.wikipedia.org/wiki/Interceptor) and, subsequently, by reconverting such information in its original form for authorized [recipients](http://en.wikipedia.org/w/index.php?title=Recipients&action=edit&redlink=1). Also, devices designed specifically to aid in, or as an essential element of, the conversion process.

**Function**

COMSEC is used to protect both [classified](http://en.wikipedia.org/wiki/Classified) and [unclassified](http://en.wikipedia.org/wiki/Unclassified) traffic passed via tactical or strategic switched systems within Department of Defense (including Joint Task Force) [computer networks](http://en.wikipedia.org/wiki/Computer_network). Its use applies to voice, data, video, information processing systems, and needed communications. COMSEC interfaces with components using varied transmission media. COMSEC measures are for: Voice/Data, Analog/Digital, Manual/ Electronic Key, Classified/SBU, Wired(Land)/ Wireless(Cell).

**COMSEC material**

**COMSEC material** includes:

* Keys: AEK, TEK, KEK, OWK
* Devices: Reader/ Transfer: KYK-13, KOI-18, KYX-15
* Documents: Manual
* Equipment: crypto-, crypto-ancillary, crypto-production, authentication,

CCI, KG-30

* Firmware/ Software: LCMS

**Acronyms**

* AKMS = the Army Key Management System
* AEK = Algorithmic Encryption Key
* CT3 = Common Tier 3
* CCI = Controlled Cryptographic Item
* EKMS = Electronic Key Management System
* NSA = National Security Agency
* ACES = Automated Communications Engineering Software
* DTD = The Data Transfer Device
* DIRNSA = Director of National Security Agency
* TEK = Traffic [Encryption](http://en.wikipedia.org/wiki/Encryption) Key
* TED = Trunk Encryption Device such as the WALBURN/KG family of CCI
* KEK = Key Encryption Key
* OWK = Over the Wire Key
* OTAR = Over The Air Rekeying
* LCMS = Local COMSEC Management Software
* KYK-13 = Electronic Transfer Device
* KOI-18 = Tape Reader General Purpose
* KYX-15 = Electronic Transfer Device
* KG-30 = TSEC family of COMSEC equipment
* TSEC = Telecommunications Security(Sometimes referred to in error transmission security or TRANSEC)
* SOI = Signal Operating Instruction
* SKL = Simple Key Loader
* TPI = Two Person Integrity

**COMSEC equipment**

**COMSEC equipment** is equipment designed to provide [security](http://en.wikipedia.org/wiki/Security) to [telecommunications](http://en.wikipedia.org/wiki/Telecommunications) (COMSEC) using [cryptography](http://en.wikipedia.org/wiki/Cryptography).

**See also**

COMSEC Equipment designated as telecommunications security (TSEC), Joint Electronic Type Designation System, and [Controlled Cryptographic Item](http://en.wikipedia.org/wiki/Controlled_Cryptographic_Item) (CCI). They provide security to telecommunications by scrambling information, unintelligible to an unauthorized interceptor, later, converting it to its original form for authorized recipients. The equipment designed to aid in scrambling format. Note: COMSEC equipment includes crypto-equipment, crypto-support equipment, crypto production equipment, and authentication equipment.

* [NSA encryption systems](http://en.wikipedia.org/wiki/NSA_encryption_systems)
* [Type 1 encryption](http://en.wikipedia.org/wiki/Type_1_encryption)

TELEPHONE/TERMINAL EQUIPMENT:
[STU-III](http://en.wikipedia.org/wiki/STU-III) (Type 1)

Motorola STU-III / SECTEL 1500(July 01, 2007)

AT&T STU-III (March 10, 2006)

STU-III (Type 2)

Type 2 STU-III. (March 10, 2006)

STU-III (Type 3)

Type 3 STU-III. (March 10, 2006)

STU-III DNVT

Motorola STU-III / SECTEL MMT/DNVT Adapter (July 01, 2007)

[STE](http://en.wikipedia.org/wiki/Secure_Terminal_Equipment)

STE (the new generation). (July 01, 2007)

CRYPTO:CCI

Note: secure voice over internet protocol ([SVOIP](http://en.wikipedia.org/w/index.php?title=SVOIP&action=edit&redlink=1)) has become the defacto standard for securing voice communication, replacing the need for STU-X and STE equipment in much of the US DoD. Effective 1 Jan 08, all new secure voice equipment items in [USCENTCOM](http://en.wikipedia.org/wiki/USCENTCOM) areas of operation is required to be satisfied with SVOIP technology. Effective 1 Jan 09, all STE/STU-X equipment items are to be returned as surplus gear in accordance with USCENTCOM PL 117-02-1.

**Term**

crypto-equipment: Any equipment that embodies [cryptographic](http://en.wikipedia.org/wiki/Cryptographic) logic or performs one or more cryptographic functions (key generation, encryption, and authentication).
crypto-ancillary equipment: Equipment designed specifically to facilitate efficient or reliable operation of crypto-equipment, without performing cryptographic functions itself. [INFOSEC-99]
crypto-production: equipment used to produce or load keying material
CCI: Equipment which contains COMSEC embedded devices

The [EKMS](http://en.wikipedia.org/wiki/EKMS) is DoD key management, COMSEC material distribution, and logistics support system. The NSA established the EKMS program to meet:
-Supplying electronic key to COMSEC devices in securely and timely manner
-Providing COMSEC managers with an automated system capable of ordering, generation, production, distribution, storage, security accounting, and access control
The Army's platform in the four-tiered EKMS, AKMS, automates frequency management and COMSEC management operations. It eliminates paper keying material, hardcopy SOI, and associated time and resource-intensive courier distribution. It has 4 components:
-LCMS
-ACES
-CT3
-SKL

LCMS provides:
-automation for the detailed accounting required for every COMSEC account
-electronic key generation and distribution capability

ACES is the [frequency](http://en.wikipedia.org/wiki/Frequency) management portion of AKMS. ACES has been designated by the Military Communications Electronics Board as the joint standard for use by all services in development of frequency management and crypto net planning.

CT3 with DTD software is in a fielded, ruggedized hand-held device that handles, views, stores, and loads SOI, Key, and electronic protection data. DTD provides an improved net-control device to automate crypto-net control operations for communications networks employing electronically-keyed COMSEC equipment.

SKL is a hand-held PDA that handles, views, stores, and loads SOI, Key, and electronic protection data.

The RED/BLACK concept requires electrical and electronic circuits, components, and systems which handle unencrypted information (BLACK) be separated from those which handle encrypted information (RED). RED/ BLACK concept differentiates between:
-circuits, components, equipment, and systems
-the physical areas in which they are contained

**Sources**
<http://www.dtic.mil/doctrine/jel/cjcsd/cjcsi/6511_01.pdf> <http://www.gordon.army.mil/sigbde15/Schools/25L/c03lp1.html> <http://www.dtic.mil/whs/directives/corres/pdf/466002p.pdf> <http://cryptome.sabotage.org/HB202D.PDF> <http://peoc3t.monmouth.army.mil/netops/akms.html>

* [Cryptography machines](http://www.jproc.ca/crypto/menu.html)