# End to end encryption in WhatsApp

The term 'end-to-end encryption' (E2EE) has entered the common lexical use and is no more restricted to the geeks, thanks to WhatsApp which popularised it and brought it to over a billion users globally. It has become the part of our daily digital life as it is the definitive security mechanism that protects our personal data (messages etc.) such that it can only be read on by the sender, and by the recipient on the other end. No one else, including the hackers or the government, can snoop and read the encrypted data.

**How does end-to-end encryption work?**

WhatsApp's end-to-end encryption ensures that only you and the person you're communicating with can read what's sent. Nobody in between, not even WhatsApp, can read the messages. The messages are secured with locks, and only the recipient has the special key to unlock and read the messages. WhatsApp uses Signal Protocol developed by Open Whisper Systems. The following steps describes the working of E2EE when two people communicate on WhatsApp.

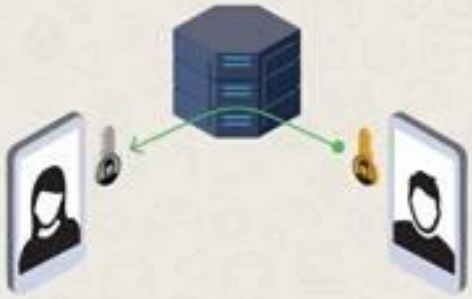
1. When the user first opens the WhatsApp, two different keys (public & private) are generated. The encryption process takes place on the phone itself.
2. The private key must remain with the user whereas the public key is transferred to the receiver via the centralised WhatsApp server.
3. The public key encrypts the senders message on the phone even before it reaches the centralised server.
4. The server is only used to transmit the encrypted message. The message can only be unlocked by the private key of the receiver. No third part, including WhatsApp can intercept and read the message.
5. If a hacker tries to hack and read the messages, they would fail because of the encryption.

# WhatsApp is Secure

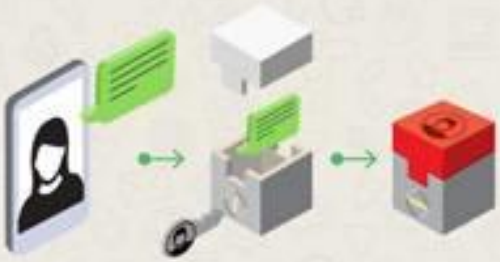
## How end-to-end encryption works

1. Two keys, public and private are generated when a user opens WhatsApp for the first time. The encryption process takes place on your phone.

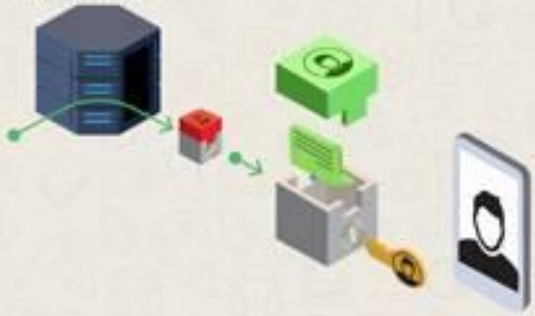
2. The private key remains with the user on the phone. The public key is transmitted through the server to the receiver.



3. The public key encrypts the sender's message on the phone even before it reaches the server.



4. The server is only used to transmit the encrypted message. Only the receiver's private key can unlock the message. No third party including WhatsApp can read the message.



## A hacker's nightmare

If someone tries to hack WhatsApp, they will not be able to reach any messages because they are end-to-end encrypted.

## Verify end-to-end encryption yourself

Simply tap on the contact name, open the contact info screen. Tap Encryption to view the QR code and 60-digit number.

WhatsApp

### How do I verify that WhatsApp is using end-to-end encryption?

To manually verify the encryption between the sender and the receiver, simply tap on the contacts name on WhatsApp to open the info screen. Now tap on 'Encryption' to view the QR code and 60-digit number. You can scan your contacts' QR code or visually compare the 60-digit number. If you scan the QR code, and if they match, then your chats are encrypted and no one is intercepting your messages or calls.

# BIOS

## What is BIOS?

Stands for "Basic Input/Output System." Most people don't need to ever mess with the BIOS on a computer, but it can be helpful to know what it is. The BIOS is a program pre-installed on Windows-based computers (not on Macs) that the computer uses to start up. The CPU accesses the BIOS even before the operating system is loaded. The BIOS then checks all your hardware connections and locates all your devices. If everything is OK, the BIOS loads the operating system into the computer's memory and finishes the boot-up process.

Since the BIOS manages the hard drives, it can't reside on one, and since it is available before the computer boots up, it can't live in the RAM. So where can this amazing, yet elusive BIOS be found? It is actually located in the ROM (Read-Only Memory) of the computer. More specifically, it resides in an eraseable programmable read-only memory (EPROM) chip. So, as soon as you turn your computer on, the CPU accesses the EPROM and gives control to the BIOS.

The BIOS also is used after the computer has booted up. It acts as an intermediary between the CPU and the I/O (input/output) devices. Because of the BIOS, your programs and your operating system don't have to know exact details (like hardware addresses) about the I/O devices attached to your PC. When device details change, only the BIOS needs to be updated. You can make these changes by entering the BIOS when your system starts up. To access the BIOS, hold down the DELETE or F2 key as soon as your computer begins to start up.

## Purpose of BIOS

BIOS enables computers to perform certain operations as soon as they are turned on. The principal job of a computer's BIOS is to govern the early stages of the startup process, ensuring that the operating system is correctly loaded into memory. BIOS is

vital to the operation of most modern computers, and knowing some facts about it could help you troubleshoot issues with your machine.

## POST

The first job of the BIOS after you switch your computer on is to perform the Power On Self Test. During the POST, the BIOS checks the computer's hardware in order to ensure that it is able to complete the startup process. If the POST is completed successfully, the system usually emits a beep. If the test fails, however, the system generally emits a series of beeps. You can use the number, duration and pattern of these beeps to identify the cause of the test failure.

## Startup

With the POST completed, the BIOS then attempts to load the operating system through a program known as a bootstrap loader, which is designed to locate any available operating systems; if a legitimate OS is found, it is loaded into memory. BIOS drivers are also loaded at this point. These are programs designed to give the computer basic control over hardware devices such as mice, keyboards, network hardware and storage devices.

## Security

The BIOS can also play a role in computer security. Most BIOS software versions have the option to password-protect the boot process, which means that you must enter a password before any BIOS activity can take place. With the BIOS performing virtually all of its functions during startup, this effectively password-protects the operation of the whole computer. However, resetting a lost BIOS password can be time-consuming and involve working on some of the computer's most sensitive components.

## Hardware

The BIOS software itself generally resides on a Read-Only Memory, or ROM, or a flash memory chip attached to your computer's motherboard. The location of the BIOS software on the chip is important, as it is the first software to take control of your computer when you turn it on. If the BIOS was not always located in the same place on the same chip, your computer's microprocessor would not know where to locate it, and the boot process could not take place.

## Booting Process

Booting (also known as booting up) is the initial set of operations that a computer system performs when electrical power is switched on. The process begins when a computer that has been turned off is re-energized, and ends when the computer is ready to perform its normal operations. On modern general purpose computers, this can take tens of seconds and typically involves performing power-on self-test, locating and initializing peripheral devices, and then finding, loading and starting an operating system. Many computer systems also allow these operations to be initiated by a software command without cycling power, in what is known as a soft reboot, though some of the initial operations might be skipped on a soft reboot. A boot loader is a computer program that loads the main operating system or runtime environment for the computer after completion of self-tests.

The computer term boot is short for bootstrap or bootstrap load and derives from the phrase to pull oneself up by one's bootstraps. The usage calls attention to the paradox that a computer cannot run without first loading software but some software must run before any software can be loaded. Early computers used a variety of ad-hoc methods to get a fragment of software into memory to solve this problem. The invention of integrated circuit Read-only memory (ROM) of various types solved the paradox by allowing computers to be shipped with a start up program that could not be erased, but growth in the size of ROM has allowed ever more elaborate start up procedures to be implemented.

There are numerous examples of single and multi-stage boot sequences that begin with the execution of boot program(s) stored in boot ROMs. During the booting process, the binary code of an operating system or runtime environment may be loaded from nonvolatile secondary storage (such as a hard disk drive) into volatile, or random-access memory (RAM) and then executed. Some simpler embedded systems do not require a noticeable boot sequence to begin functioning and may simply run operational programs stored in read-only memory (ROM) when turned on.

# RAID Vs LVM

## RAID:

- RAID is used for redundancy.
- A RAID device is a physical grouping of disk devices in order to create a logical presentation of one device to an Operating System for redundancy or performance or a combination of the two.
- RAID is a way to create a redundant or striped block device with redundancy using other physical block devices.
- RAID is either a software or a hardware technique to create data storage redundancy across multiple block devices based on required RAID levels.
- RAID is NOT any kind of Data backup solution. Its a solution to prevent one of the SPOFs (Single Point of Failure) i.e. DISK failure. By configuring RAID you are just providing an emergency substitute for the Primary disk. It NEVER means that you have configured DATA backup.

## LVM:

- LVM is a way in which you partition the hard disk logically and it contains its own advantages.
- LVM is a logical layer that that can be anipulated in order to create and, or expand a logical presentation of a disk device to an Operating System.
- LVM usually sits on top of RAID blocks or even standard block devices to accomplish the same result as a partitioning, however it is much more flexible than partitions. You can create multiple volumes

crossing multiple physical devices, remove physical devices without loosing data, resize the volumes, create snapshots, etc

- LVM is a software tool to manage large pool of storage devices making them appear as a single manageable pool of storage resource. LVM can be used to manage a large pool of what we call Just-a-bunch-of-Disk (JBOD) presenting them as a single logical volume and thereby create various partitions for software RAID.
- LVM is a disk management approach that allows us to create, extend, reduce, delete or resize the volume groups or logical volumes.