DigitalBank
VAULT
ENCRYPTION

The DBV SuperEncrypted Smartphone is a unique combination of ultra encryption technologies , both software and hardware based, with a cyber defense architecture which enables the use of public cellular communication infrastructure to securely transfer classified information and conduct top classified calls.

The DBV is the only cell phone solution in the market that cannot be hacked by known and unknown Online & Offline Cyber Attack Tools and Spyware. Immune to: Interception, Location Tracking, Cyber Espionage, Forensic Data Extraction, Electronic Surveillance.

DigitalBank Vault Smartphone: Anonymous, Unbreakable, Untraceable, Impenetrable, Anti Tapping SuperEncrypted Video & Audio Calls, Instant Messaging, File Transfers.

Every DigitalBank Vault Smartphone device is built from the hardware chip up to isolate, encrypt, and secure your data – including confidential files storage and data transfers, video & audio classified communications, top secret text messaging and file sharing.

DigitalBank Vault Smartphone provides strong security guarantees against both software and hardware attacks, both online or offline attacks.

DigitalBank Vault Smartphone is independent from the primary processor that runs Android, code running on the DigitalBank Vault Smartphone Encryption Processor is resistant to attacks that exploit shared resources, such as software side-channel attacks that can compromise other software executing on the same processor.

This separation means DigitalBank Vault Smartphone protects sensitive data even if the primary phone processor itself is completely compromised.

In addition to being resistant to software attacks, DigitalBank Vault Smartphone is also designed to be tamper-proof to thwart hardware attacks, which require that an attacker have physical possession of a device to extract secrets.

* Image simulated for illustrati

DigitalBank Vault Smartphone is resistant to hardware attacks such as the following:

Physical probing to disclose data
Physical manipulation of the circuitry to deactivate security mechanisms
Forced information leakage
Hardware side-channel attacks such as differential power analysis to disclose data
Fault injection to bypass security mechanisms.

The DigitalBank Vault Smartphone Super Encryption system is designed to operate separately from other SoC components. It has its own secure processing environment consisting of the DB Processor,DB SuperEncryption Engine, encrypted SRAM, and encrypted ROM.

It also provides enhanced security and data protection against various hardware-based attacks, by monitoring the hardware status and its environment using a series of security sensors or detectors including:

High and Low Temperature detectors
High and Low Supply Voltage detectors
Supply Voltage Glitch detector
Laser detector

Only fully encrypted communication is allowed.

Above Military Grade Quantum Safe SuperEncryption is governing all data exchanged or stored within the phone.

DBV BASED CELLULAR DEVICES ARCHITECTURE:

Modified COTS phone protected against online & offline penetration.

No GPS. Anti Tracing Technology. Anti Triangulation Tracking .

Sophisticated Anti Location services that are based on Wifi, Cell Towers, and GPS. DBV phones are taking care of all the 3 aspects of location tracking.

Phone transmitting capability is disabled forcing all communication via an additional internal ultra encrypted modem and encrypted antennas.
This modem and encryption engine are built in the phone.

There is a built-in GPS frequency jammer module. Jamming frequencies: CDMA, GSM, 3G, 4G LTE, 4G, 5G. Towers will not be able to get the data on the cell towers, such as MMC (country code), MNC (carrier code), LAC (a code of a current cell) and cell ID (unique cell tower ID). DBV cellphones won't give the info on the cell towers they are connected to.

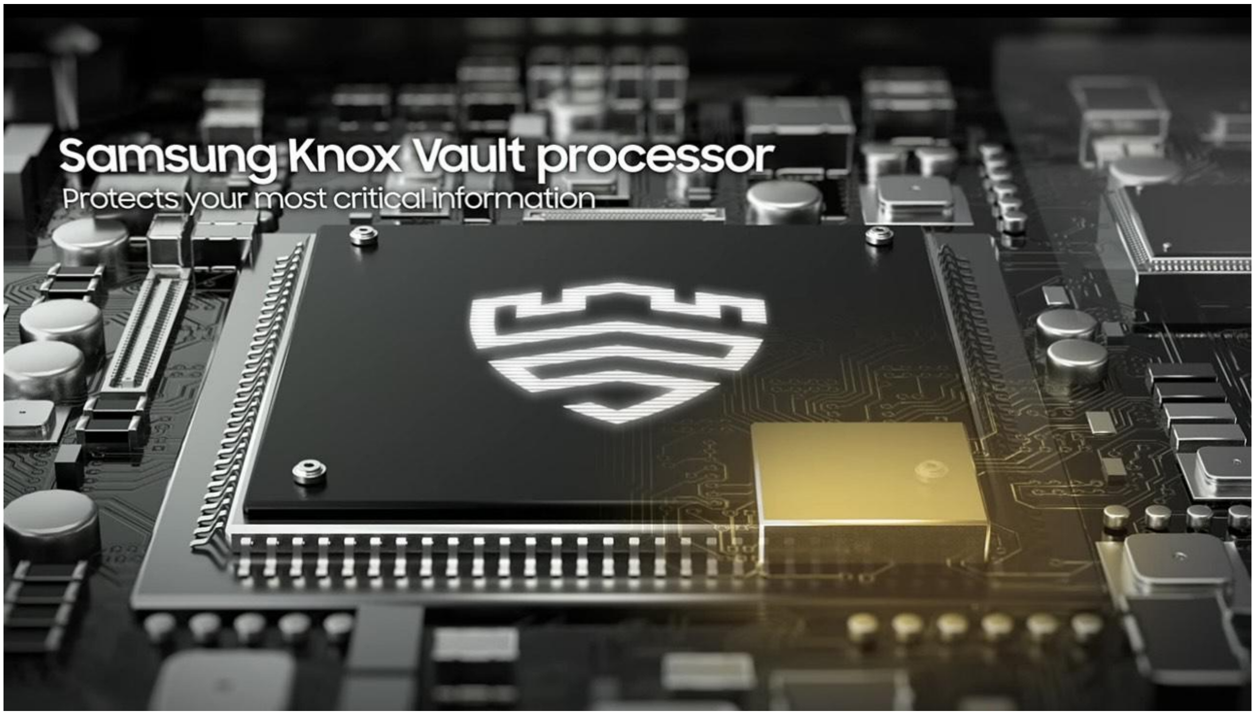
Anti Spyware & Anti Malware: Installing a malicious app or spyware on the phone is impossible, remotely or even physically , and no breach of the phone by itself is feasible.

The DBV phone provides highly secure voice calls, video conference, text chat , file transfers and other applications, completely isolated from the cellular unclassified infrastructure.
The modified Samsung phone is coupled to a security module that includes an advanced encryption engine along an advanced cyber secured cellular modem. Modified phone is running a special ROM to support trusted boot and secure operations.

Ultra Encrypted Cameras. Fully Encrypted Bluetooth and Cyber Shielded Wifi connections (any single internal and external connections is cyber defended by a one time pad random encryption)

Top Level Superior Security
DBV encryption engines feature multiple isolated cores to protect from network attacks both from the red and from the black sides.
Networks at both sides are equally protected by configurable deep-packet inspection (DPI) firewalls. Security monitoring services are running at all times to detect potential physical or network penetration attempts. Physical security features supported by this module is the largest set available in the industry today.

Revolutionary Cyber Defense Architecture
Using the latest smart-phone technology with trusted encryption and communication provides cost-effective solutions for users that need absolute secrecy and total privacy . DBV Super encrypted phones can run on commercial cellular phone infrastructure or on dedicated tactical military or government infrastructure. The DBV crypto engines are designed and assembled using the latest smart-phones technologies and processes.


Samsung Knox Vault processor
Protects your most critical information

Compatibility

The use of COTS Samsung phone, enables the use of standard commercial software applications widely available for Android platforms. In most cases, customers do not need to develop complex tailored applications.

No special software drivers needed to operate and to manage this product. Users may connect auxiliary tethered devices such as laptops or desktop computers. Dedicated App store having Cyber secured modified applications. Ruggedized commercial Android applications.

Main Hardware Changes :

INTERNAL ANTENNAS (ENCRYPTED)

CELLULAR MODEM (ENCRYPTED)

CAMERAS (ENCRYPTED)

BLUETOOTH (ENCRYPTED)

WIFI MODULE (ENCRYPTED)

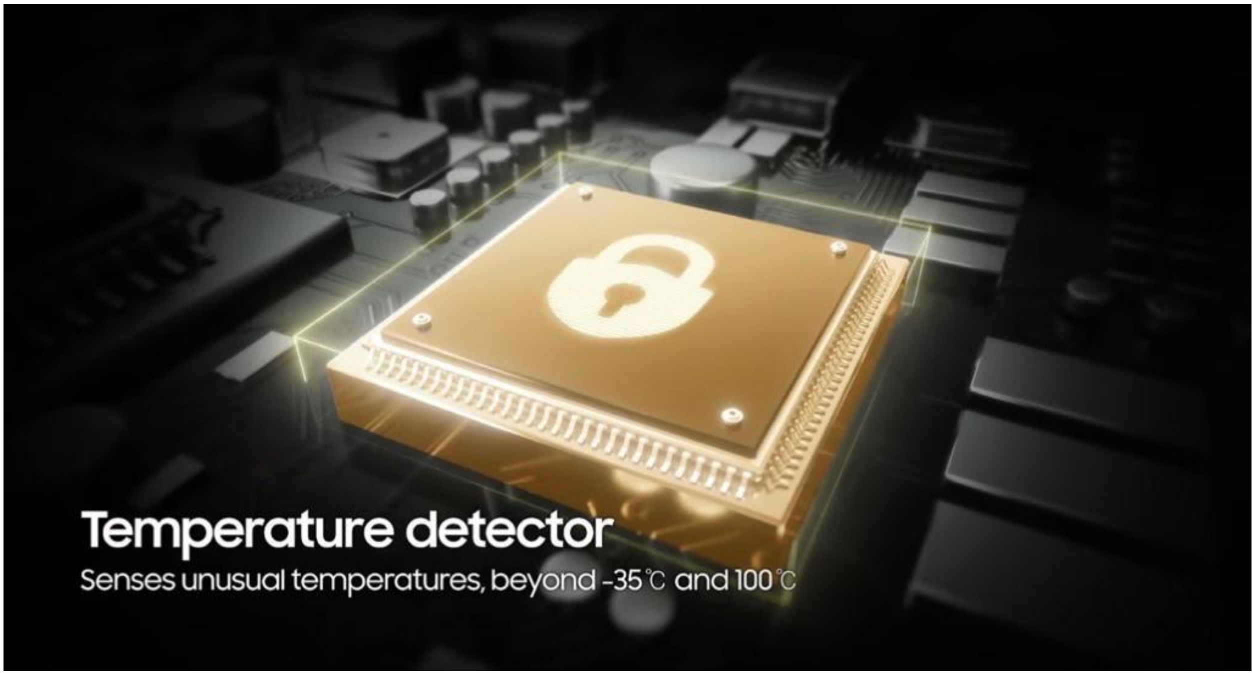
CHIPSET (ENCRYPTED)

AIR GAPPED PROCESSORS

ISOLATED ENCRYPTED TRANSMITTERS

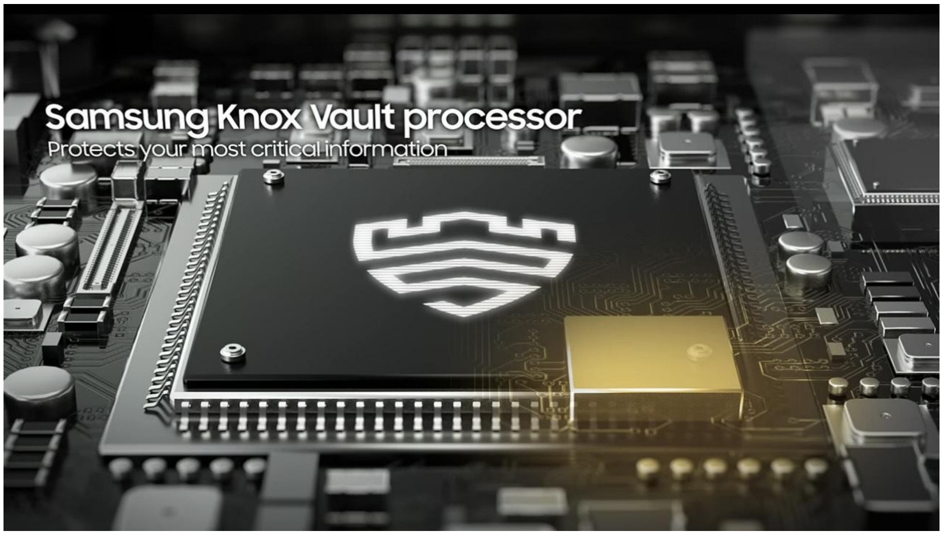
DATA MANAGEMENT SYSTEM

MEMORY CELLS & MICROCHIPS SETS (ENCRYPTED)



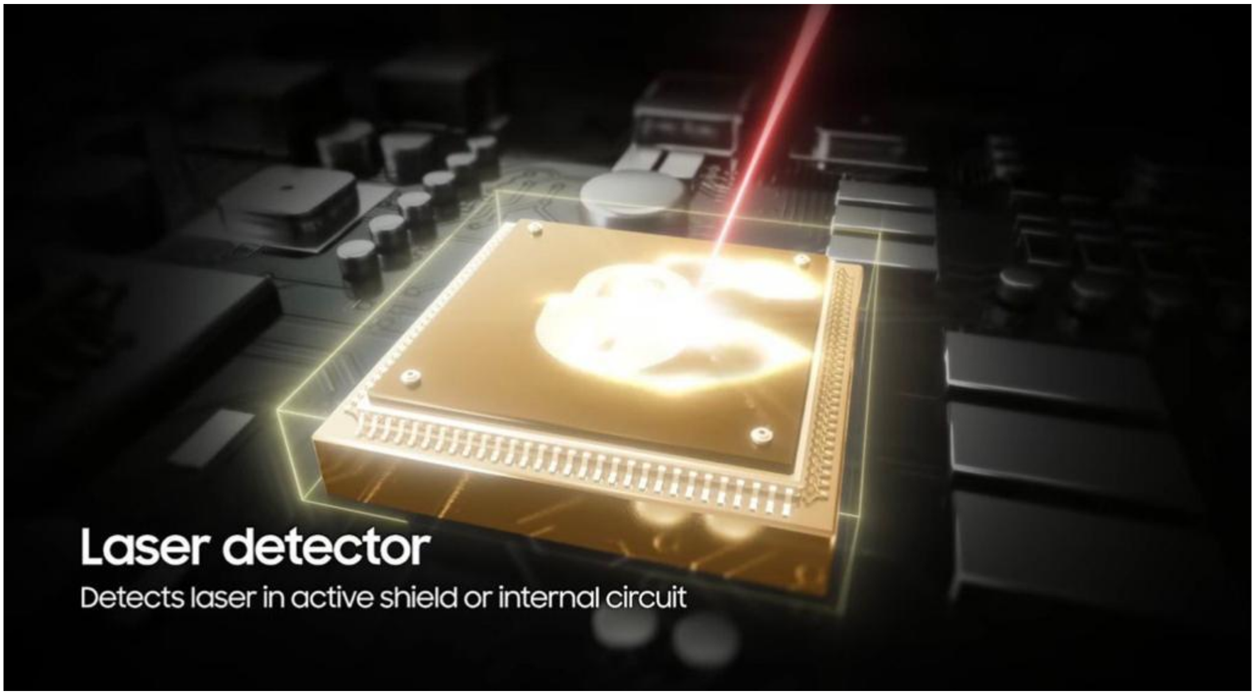
This above mentioned set of cyber defense features allows the phone to to be completely resistant to all Spyware Attacks, and can be used anywhere in the World. End-to-End security architecture – the encryption system is totally isolated from the internet.

High-Bandwidth military/intelligence agencies strengthen encryption allowing Classified\Private traffic on commercial LTE/5G networks.


Samsung Knox Vault processor
Protects your most critical information

The DigitalBank Vault Smartphone Processor
The DigitalBank Vault Smartphone Processor provides the main computing power for “secret partition”, providing the strongest isolation (100% air gapped) , the DigitalBank Vault Smartphone Processor is separated from the primary processor of the smartphone. This separation helps prevent side-channel attacks that depend on malicious software sharing the same execution core as the target software under attack.

By executing the instructions and managing data on the encrypted SRAM, the Knox Vault Processor also guarantees a physically isolated execution environment. The DigitalBank Vault Smartphone Encrypted System ROM where the secure boot loader code is located is also separated and protected by the hardware protection mechanisms.
When the DigitalBank Vault Smartphone Processor starts, the ROM code is loaded to SRAM. While the ROM code loads the DigitalBank Vault Smartphone Processor firmware, with the help of the modules running on the SOC main processor, the software stack of DigitalBank Vault Smartphone has its own secure boot chain.



DigitalBank Vault Smartphone Internal Hardware 24/7 monitor
The DigitalBank Vault Smartphone Hardware Monitor checks for abnormal hardware status from the security sensors and detectors. The monitoring and detection cannot be affected or bypassed by any application running on the DigitalBank Vault Smartphone Processor.

DigitalBank Vault Smartphone SuperEncryption Engine Tech Specs :

1. A hardware cryptographic module provides the following cryptographic functions:Independent Offline “Air Gapped” Self Working SuperEncryption System, not internet connected, with no servers or third party services involvement.

2. Mathematical Unbreakable Quantum Safe Encryption. Resist any attacks of unlimited resources. “Above Government” Level Encryption.

3. Random Encryption Keys Generated by the user only, just for a few milliseconds, then erased permanently from the system, not stored anywhere and never exchanged, with any third party, including the communicating counterpart, therefore encryption keys cannot be intercepted or hacked.

4. Totally Immune to any type of Digital Forensic Analysis, no physical extraction of data is possible, with all the most advanced forensic tools available today.

5. SuperEncryption Proprietary technology composed of 4 Consecutive Layers of Symmetric Encryption:

A. FOREVER SECURE QUANTUM SAFE OTP One Time Pad Cipher(The User can create an infinite number of symmetric keys with just a ‘passphrase’, each key generated is in the length up to “one-time-pad”, that is mathematically Uncrackable.

B. AES 256

C. Blowfish 448

D. TwoFish 256

DigitalBank Vault Smartphone SuperEncryption is Unbreakable and Indecipherable, no matter how much computational power you will apply. "Above Government" level of encryption. Encrypted Files convey zero info about original content.

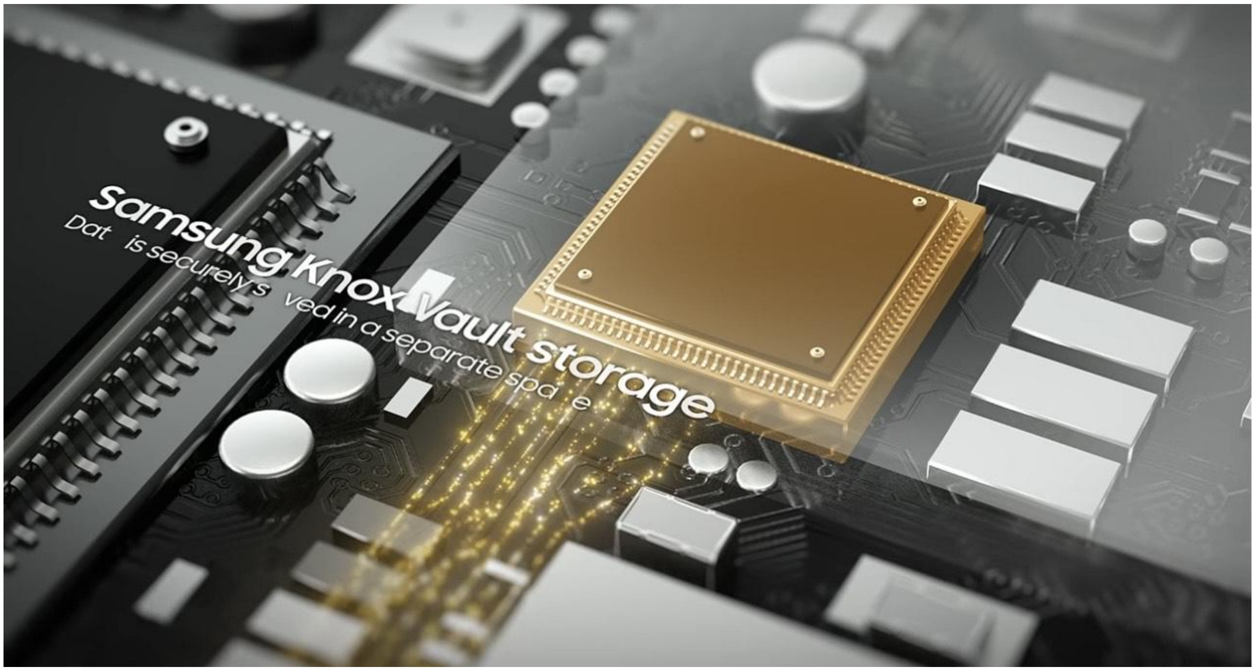
6. Personal, Unique, SuperEncrypted System for each client, coming with a dedicated set of encryption algorithms, allowing to create a private, individual communication network between two or more DigitalBank Vault Smartphone devices and managing encrypted databases and Peer to Peer encrypted file exchanges.

Active shield removal detector
Detects abnormal activities that try to remove the shield of the chip

7.UNTRACEABLE COMMUNICATION NETWORK
Private Ultra Encrypted Peer to Peer, serverless communication network ,anonymous, peer to peer, SuperEncrypted, ÿor voice/video calls, text messaging, transfering of encrypted files between two remote devices, without leaving any digital trails. More Secure than any ‘face to face meeting”.

ANONYMOUS
No registration or login.
No authentication Needed.

OFFLINE
Air Gapped. Immune to remote hacking and espionage, ransomware, malware, data breach, digital surveillance, eavesdropping, tapping,interception.


Samsung Knox Vault storage
Dat is securely s ved in a separate spa e

If you have secret data to exchange and you want to be absolutely sure that no state-sponsored hackers, no foreign Governments, no Intelligence agencies will be ever able to decipher the Files and communications , you need an Above Military Level DigitalBank Vault Smartphone Encryption Machine ”

SERVERLESS
Independent Offline “Air Gapped” Self Working (Stand Alone) SuperEncryption System, not internet connected, with no servers or third party services involvement.

MULTI SIGNATURE- MULTI LAYER ENCRYPTION- MULTI LINGUAL
One or more users can encrypt/decrypt files together.
Security Layered Access.
The DigitalBank Vault Smartphone Encryption System works in all languages.

HOMOMORPHIC ENCRYPTION

Working on SuperEncrypted Files without never decrypting them, therefore prevents exposure of unencrypted content.

Protection from Attacks

DigitalBank Vault Smartphone is tested to provide protection against the following classes of hardware probing attacks.

Physical probing

An attacker might physically probe secure hardware to disclose user data or other critical information, while the data is stored in memory or being processed. The attacker directly measures information using electric contact with the secure hardware internals, using techniques commonly employed in IC failure analysis and IC reverse engineering.

Physical manipulation

An attacker might physically modify the secure hardware to change user data, secure hardware software, or security services or mechanisms. The attacker might make modifications through techniques commonly employed in IC failure analysis and IC reverse engineering. To make these modifications, the attacker identifies hardware security mechanisms, layout characteristics, or software design, including how secure hardware treats user data. Changes of circuitry or data can be permanent or temporary.

Forced information leakage

An attacker might exploit information that is leaked from the secure hardware in order to disclose confidential user data, even if the information leakage is not inherent but caused by the attacker. For example, fault injection or physical manipulation might cause information leakage from signals which normally do not contain significant information about secrets.

Side-channel attack

An attacker might exploit information that is leaked from the secure hardware during its operation in order to disclose confidential user data. Direct contact with the secure hardware internals is not required. Information leakage might occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time. One example is the Differential Power Analysis (DPA). This leakage can be interpreted as a covert channel transmission, but is more closely related to the measurement of operating parameters. These operating parameters might be derived either from direct measurements or measurement of emanations. The attacker can associate the measurements with the specific operation being performed.

Fault injection

An attacker might cause a malfunction of the secure hardware software by applying environmental stress like light or a power glitch. This attack type could modify the hardware and software functions, or deactivate or affect security mechanisms of the secure hardware. Thus, the attacker could disclose or manipulate the user data existing in the secure hardware. For example, the modification of the security hardware function might affect the quality of random numbers provided by the random number generator, and then the software may get constant values or values with low entropy.