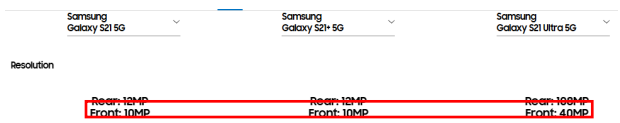
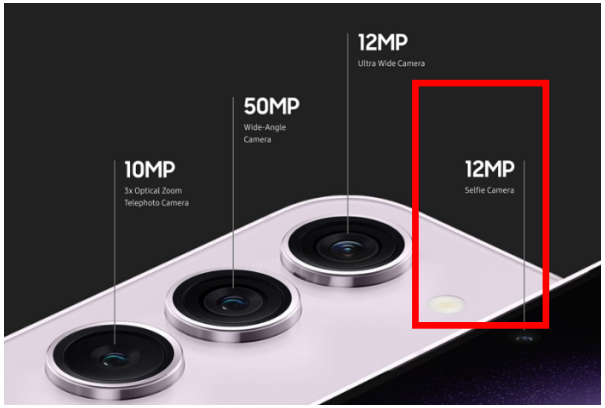
U.S. Patent No. 8,401,875 Claim Chart Against Samsung

Patent Claim Term	Samsung Devices
Claim 1. Apparatus for storing and managing personal and secured data and documentation files associated with a specific user, comprising:	The **Accused Instrumentalities** are Samsung devices for storing and managing personal and secure data and files that include Knox Vault, with Face Unlock and/or Fingerprint Unlock. On information and belief, infringing Samsung devices include, based on information to date: Galaxy S21, S21+, S21 Ultra (collectively, S21 line); Galaxy S22, S22+, S22 Ultra (collectively, S22 line); Galaxy S23, S23+, S23 (collectively, S23 line); and Galaxy Ultra, S24, S24+, S24 Ultra (collectively, S24 line) smartphones.[1]
a plurality of biometric sensors for reading a plurality of personal biological biometric identification parameters of the user holding the apparatus, said plurality of biometric sensors being integrated within the apparatus	**The Accused Instrumentalities have integrated biometric sensors for reading personal biological biometric identification parameters of the user holding the apparatus.** **For example, sensors include a front facing camera. Such a camera reads personal biological biometric identification parameters, such as facial characteristics.**

Galaxy S21 line	Galaxy S22 line
	• **Galaxy S22:** A 10MP front camera and 3 rear cameras, including a 12MP Ultra Wide lens, 50MP Wide lens, and 10MP Telephoto lens (3x optical zoom). • **Galaxy S22+:** A 10MP front camera and 3 rear cameras, including a 12MP Ultra Wide lens, 50MP Wide lens, and 10MP Telephoto lens (3x optical zoom). • **Galaxy S22 Ultra:** A 40MP front camera and 5 rear cameras, including a 12MP Ultra Wide lens, 108MP Wide lens, and two 10MP Telephoto lenses (3x and 10x optical zoom).
OSNH_00000355, *How the Galaxy S21 5G compares*, SEA (emphasis added). All S21 devices have at least one front facing camera.	OSNH_00000356-OSNH_00000363, *Differences between the Galaxy S22 models*, SEA. All S22 devices have at least one front facing camera.

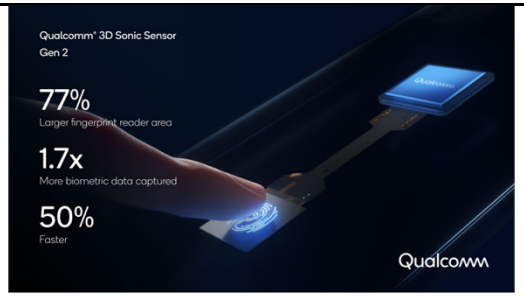
[1] These Galaxy S smartphones are exemplary based on limited publicly available information.

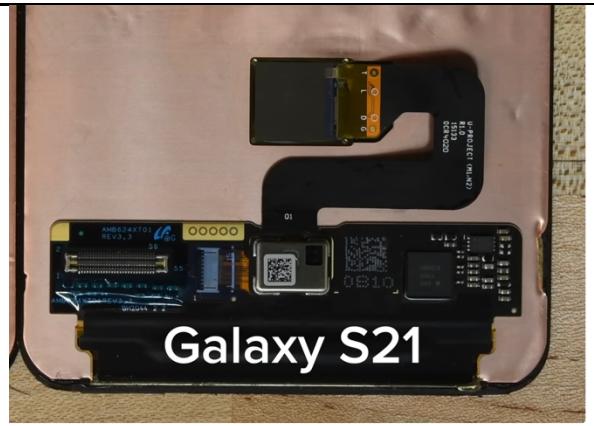
EX-1016
U.S. Patent 8,401,875

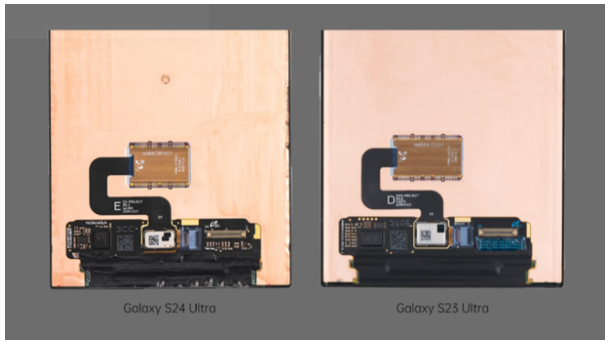
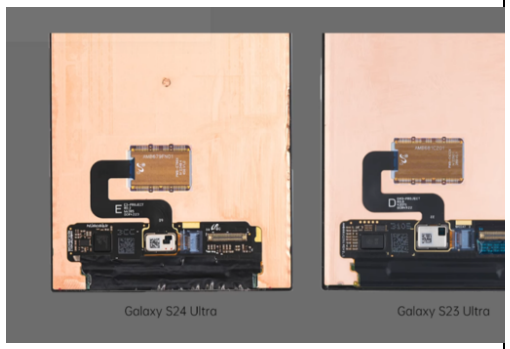
Galaxy S23 line	Galaxy S24 line
	
OSNH_00000321-OSNH_00000323, *Galaxy S23*, SEA (emphasis added). All S23 devices have at least one front facing camera.	OSNH_00000364, "Explore Camera" popout (emphasis added). All S24 devices have at least one front facing camera.

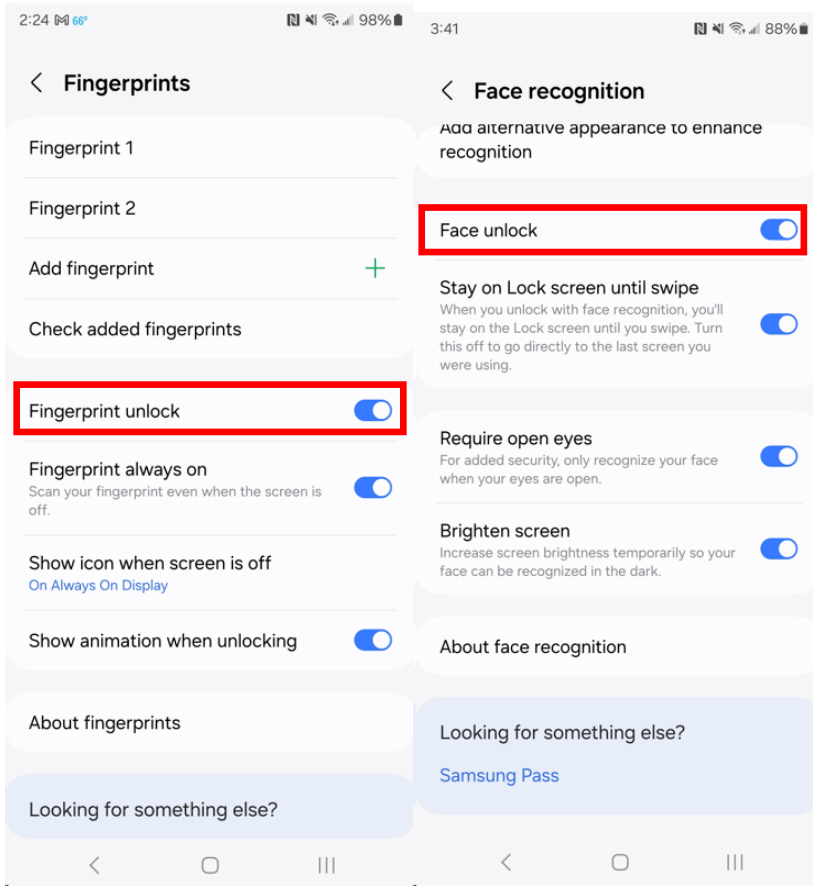
Additionally, sensors include an ultrasonic fingerprint scanner. Such a scanner reads personal biological biometric identification parameters, such as a user's unique fingerprint characteristics.

	Galaxy S21 line	Galaxy S22 line
	Samsung Galaxy S21 5G / Samsung Galaxy S21+ 5G / Samsung Galaxy S21 Ultra 5G Ultrasonic Fingerprint Scanner Yes / Yes / Yes	**Galaxy S22 | Galaxy S22+ | Galaxy S22 Ultra** • **Remove face data**: Delete existing faces. • **Add alternative appearance to enhance recognition**: Enhance face recognitic an alternative appearance. • **Face unlock**: Enable or disable face recognition security. • **Stay on Lock screen until swipe**: When you unlock your device with face recogn the Lock screen until you swipe the screen. • **Require open eyes**: Facial recognition will only recognize your face when your eye • **Brighten screen**: Increase the screen brightness temporarily so that your face can recognized in dark conditions. • **About face recognition**: Learn additional information about securing your device recognition. **Fingerprint scanner** Use fingerprint recognition as an alternative to entering passwords in certain apps. You ca your fingerprint to verify your identity when logging in to your Samsung account. To use yc fingerprint to unlock your device, you must set a pattern, PIN, or password. 1. From Settings, tap **Security and privacy** > **Biometrics** > **Fingerprints**. 2. Follow the prompts to register your fingerprint.
	OSNH_00000355, *How the Galaxy S21 5G compares*, *supra*. On information and belief, all Samsung S21 smartphones use the Qualcomm 3D Sonic Sensor Gen 2. OSNH_00000365-OSNH_00000372, *Qualcomm's Latest Flagship Snapdragon 888 5G Mobile Platform to Power the New Samsung Galaxy S21 Series*, Qualcomm (Jan. 13, 2021).	OSNH_00000373, *Galaxy S22 Biometric Security*. On information and belief, all Samsung S22 smartphones use the QBT2608 ultrasonic fingerprint sensor. On information and belief, all S22 devices have the same fingerprint scanner.

	 "Qualcomm 3D Sonic Sensors deliver a better user experience by using technological advances and acoustics (ultrasonic waves) to scan 3D features such as ridges, valleys, as well as pores of a user's finger for a deeply accurate image." OSNH_00000374-OSNH_00000377, Gordon Thomas, *Introducing Qualcomm 3D Sonic Sensor Gen 2*, Qualcomm, at 374 (Jan. 10, 2021). The S21 uses the new (for that time) Qualcomm 3D Sonic Sensor Gen 2, which on information and belief, is the Qualcomm QBT2608 ultrasonic fingerprint sensor.	

		 Video, Galaxy S21 Teardown: Best of the New Galaxies, at 3:20, available at https://www.ifixit.com/Teardown/Samsung+Galaxy+S21+Teardown/140337 (last visited Jul 26, 2024). *See also*, OSNH_00000346-OSNH_00000350, *3D Sonic Gen 2 Overview*, Qualcomm. On information and belief, all flagship S21 devices have the same fingerprint scanner.	

	Galaxy S23 line	**Galaxy S24 line**
		/ 
	OSNH_00000378-OSNH_00000383, Ben Schoon, *Samsung Galaxy S24 Ultra has a slightly newer fingerprint sensor*, at 380, 9to5google.com (Feb. 5, 2024). Samsung S23 uses the QBT2608 ultrasonic fingerprint sensor. On information and belief, all S23 devices have the same fingerprint scanner.	*Id.* Samsung S24 uses the QFS4008 ultrasonic fingerprint sensor. *See also*, OSNH_00000346-OSNH_00000350, *3D Sonic Gen 2 Overview*, *supra*. On information and belief, all S24 devices have the same fingerprint scanner.

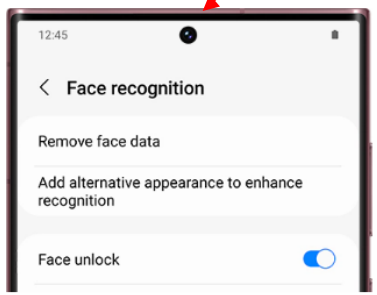
at least one life signs detector integrated within the apparatus, said life signs detector being configured to measure and record at least one of said user's life sign parameters	**The Accused Instrumentalities have at least one life signs detector (*e.g.*, the front camera, fingerprint scanner, and associated software), being configured to measure and record at least one of the user's life sign parameters.** **All Accused Instrumentalities have a Face Unlock and Fingerprint Unlock feature:**  *Galaxy S22 Ultra Screen Captures* (emphases added).

For example, the Accused Instrumentalities all include the Face Unlock feature that uses a camera to determine if a user's eyes are open (life sign parameter) to prevent spoofing and determine if the user is alive.

Facial recognition options

Once your face is registered to your device, you can use additional security options and settings. To access these options, navigate to **Settings**, and then tap **Security and privacy**. Tap **Biometrics**, then tap **Face recognition**, and then enter your security credentials. The following will be available:

- **Remove face data:** Delete the current face recognition data that is stored.
- **Add alternative appearance to enhance recognition:** This is useful if you change your hairstyle, facial hair, or makeup.
- **Face unlock:** Unlocks your device when your face is recognized.
- **Stay on Lock screen until swipe:** Remain on the Lock screen until you swipe even if you already used Face recognition.



- **Require open eyes:** For added security, the device will only recognize your face when your eyes are open.
- **Brighten screen:** Increase screen brightness temporarily so your face can be recognized in the dark.

OSNH_00000329, *Use Facial recognition security on a Galaxy phone or tablet* (emphasis added).

As shown below, the Face Unlock feature can measure whether a user's eyes are open:

Galaxy S21 line	Galaxy S22 line
For first time setup: 1. From the Face recognition screen, review the info about Face recognition then tap **Continue**. 2. If presented, select a lock screen option (e.g., pattern, PIN or password) then follow the steps to complete the process. → If necessary, refer to enable screen lock for assistance. 3. While holding the phone 8-20 inches away, position your face within the square displayed on-screen. 4. To continue, review the info about Backing up your Pattern, tap **Agree** then follow the on-screen directions to sign in to your Samsung account. 5. From the 'Face recognition' menu, tap any of the following switch(es) to turn on or off . ▫ **Face unlock**: When on, device unlocks with a recognized face. ▫ **Stay on Lock screen until swipe**: Once unlocked, remain on the lock screen until you swipe. ▫ **Require open eyes**: Your face will only be recognized when your eyes are open.	For first time setup: 1. From the Face recognition screen, review the info about Face recognition then tap **Continue**. 2. If presented, select a lock screen option (e.g., pattern, PIN or password) then follow the steps to complete the process. → If necessary, refer to Enable / Disable / Modify Screen Lock for assistance. 3. While holding the phone 8-20 inches away, position your face within the square displayed on-screen. 4. Tap **Done** (at the bottom). 5. To continue, review the info about Backing up your Pattern, tap **Agree** then follow the on-screen directions to sign in to your Samsung account. 6. From the 'Face recognition' menu, tap any of the following switch(es) to turn on or off . ▫ **Face unlock**: When on, device unlocks with a recognized face. ▫ **Stay on Lock screen until swipe**: Once unlocked, remain on the lock screen until you swipe. ▫ **Faster recognition**: When off, greater security is provided making it harder to unlock your phone using an image or video. ▫ **Require open eyes**: Your face will only be recognized when your eyes are open.
OSNH_00000384-OSNH_00000386 (emphases added).	OSNH_00000387-OSNH_00000389 (emphases added).

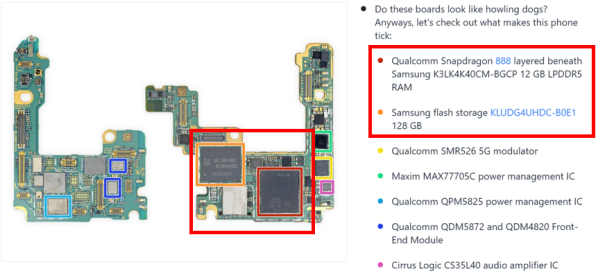
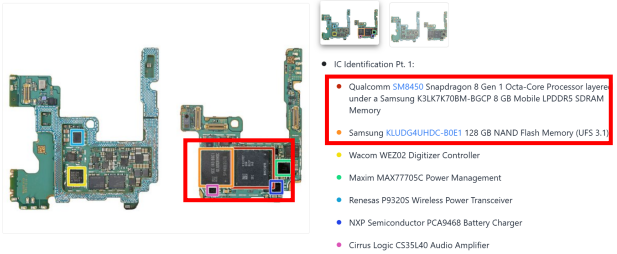
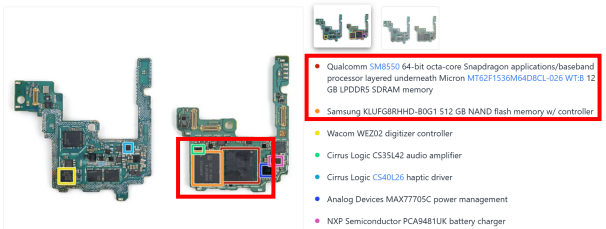
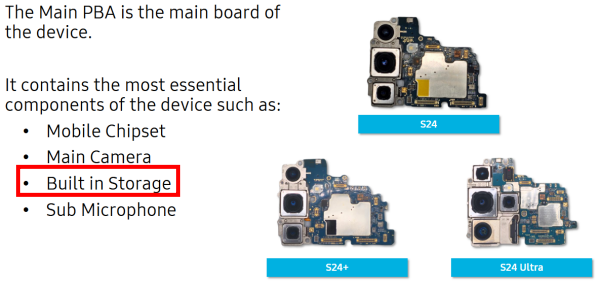
	Galaxy S23 line	Galaxy S24 line
	For first time setup: 1. From the Face recognition screen, review the info about Face recognition then tap **Continue**. 2. If presented, select a lock screen option (e.g., pattern, PIN or password) then follow the steps to complete the process. → If necessary, refer to enable screen lock for assistance. 3. While holding the phone 8-20 inches away, position your face within the square displayed on-screen. 4. Tap **Done** (at the bottom). 5. To continue, review the info about Backing up your Pattern, tap **Agree** then follow the on-screen directions to sign in to your Samsung account. 6. From the 'Face recognition' menu, tap any of the following switch(es) to turn on or off . ▫ **Face unlock**: When on, device unlocks with a recognized face. ▫ **Stay on Lock screen until swipe**: Once unlocked, remain on the lock screen until you swipe. ▫ **Faster recognition**: When off, greater security is provided making it harder to unlock your phone using an image or video. ▫ **Require open eyes**: Your face will only be recognized when your eyes are open.	For first time setup: 1. From the Face recognition screen, review the info about Face recognition then tap **Continue**. 2. If presented, select a lock screen option (e.g., pattern, PIN or password) then follow the steps to complete the process. → If necessary, refer to Enable / Disable / Modify Screen Lock for assistance. 3. While holding the phone 8-20 inches away, position your face within the circle displayed on-screen until 'Face registered' displays. 4. From the 'Face recognition' menu, tap any of the following switch(es) to turn on or off . ▫ **Face unlock**: When on, device unlocks with a recognized face. ▫ **Stay on Lock screen until swipe**: Once unlocked, remain on the lock screen unti you swipe. ▫ **Require open eyes**: Your face will only be recognized when your eyes are open.
	OSNH_00000390-OSNH_00000392 (emphases added).	OSNH_00000397-OSNH_00000398 (emphases added).

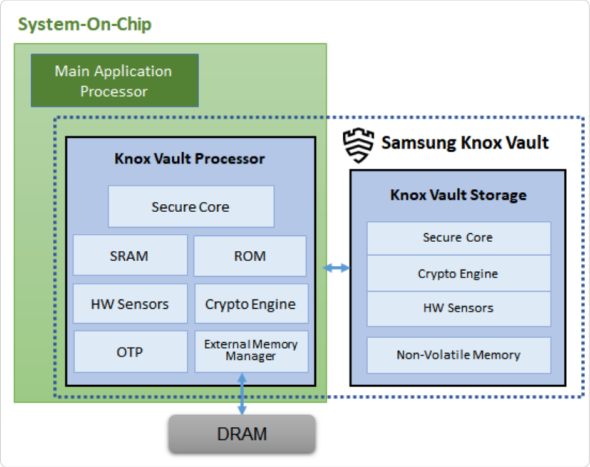
	Additionally, the Fingerprint Unlock feature uses a fingerprint reader to detect liveness, preventing spoofing attempts using fake molds. It monitors at least blood flow and uses machine learning to distinguish between fingerprints on a live human and forged replicas. Our ultrasonic sensor for fingerprint recognition can detect blood flow within the finger and actually prevent hackers from spoofing the device with a photo or a mold. This extra protection is called anti-spoofing, and it takes in additional information from the fingerprint and makes this solution unique compared to legacy optical solutions. Reading the pulses also leads to better performance than optical biometric passwords across a wide variety of conditions and contaminants, including when the finger is wet or dirty. OSNH_00000399-OSNH_00000400, Francisco Cheng, *Qualcomm 3D Sonic Sensor enables OEMs top-notch security and accuracy*, Qualcomm, at 399. *Id*. (Emphases added).

	On information and belief, the the Qualcomm 3D Sonic Sensor Generation 2 has at least blood flow anti-spoofing technology which was found in Generation 1: To read the valleys and ridges of a finger, the new sensor uses sound waves. It transmits an ultrasonic pulse against the finger to create a 3D reproduction of the fingerprint. This process makes it distinct from other solutions that use the 2D light-sensing optical approach. Moreover, the sensor is capable of detecting blood flow within the finger, making it hack-proof from a photo of a mold. OSNH_00000339-OSNH_00000345, Vishal Kawadkar, *How Qualcomm's 3D Sonic Fingerprint Sensor Could Be A Great Tool In Covid-19 Era*, at 341 (Jan. 12, 2021) (emphases added). **Delivering security-rich, built-in anti-spoofing security.** Safeguard a user's identity with the most advanced fingerprint security system available. 3D Sonic uses acoustic-based technology that reflects the unique features of a user's individuc fingerprint vs. optical solutions, which leaves users exposed to spoofing. With anti-spoofing built in, neither a photograph nor fake mold of your finger can access your phone. OSNH_00000335-OSNH_00000338, *Qualcomm 3D Sonic Sensor*, at 336 (emphasis added).

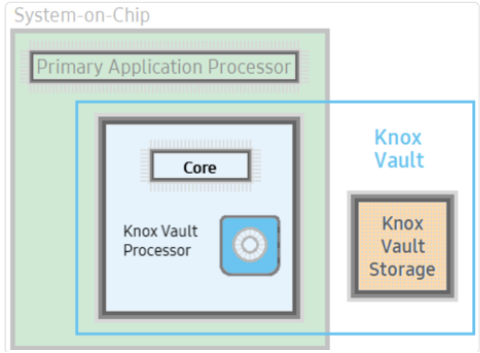
	Features • Supports mounting under display, metal, glass, plastic, and many other materials • One Tap Enrollment: No • Single finger support • 1:50K False Acceptance Rate (FAR) • Heart Rate Monitoring OSNH_00000346-OSNH_00000350, *3D Sonic Gen 2 Overview*, *supra* (emphasis added). On information and belief, the S21, S22, and S23 lines of products use the Qualcomm QFS2608 sensor, whereas the S24 line uses the Qualcomm QFS4008 sensor, and both sensors possess at least blood flow anti-spoofing technology. *Id*.

a first storage unit for the storage of said user's data and documentation files;	**The Accused Instrumentalities include a first storage unit.**

Galaxy S21 line	**Galaxy S22 line**
	
OSNH_00000401-OSNH_00000413, *Samsung Galaxy S21 Ultra Teardown*, at 408 (emphasis added).	OSNH_00000414-OSNH_00000421, *Samsung Galaxy S22 Ultra Chip ID*, at 416 (emphasis added).
Galaxy S23 line	**Galaxy S24 line**
	

<table>
<tr>
<td rowspan="3"></td>
<td>
<table>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>
</td>
<td>
	Samsung Galaxy S24	Samsung Galaxy S24 Plus	Samsung Galaxy S24 Ultra
RAM	8GB LPDDR5X	12GB LPDDR5X	12GB LPDDR5X
Storage	128GB or 256GB	256GB or 512GB	256, 512GB, or 1TB
</td>
</tr>
<tr>
<td>OSNH_00000422-OSNH_00000430, Galaxy S23 Ultra Chip ID, at 423 (emphasis added).</td>
<td>OSNH_00000431-OSNH_00000514, Samsung Galaxy S24 Repair Guide, at 437 (emphasis added); OSNH_00000515-OSNH_00000524, Andrew Grush, Samsung Galaxy S24 series specs: Everything you need to know, at 517 (June 24, 2024) (emphasis added).</td>
</tr>
<tr>
<td colspan="2">See also for all Accused Instrumentalities:
 

OSNH_00000647-OSNH_00000654, Knox Documentation, Knox Vault, SEC, at 650 (Feb. 20, 2024).</td>
</tr>
<tr>
<td>an authentication unit comprising a second storage unit, with said</td>
<td colspan="2">The Accused Instrumentalities include an authentication unit comprising a second storage unit.</td>
</tr>
</table>

second storage unit configured to store a pre-recorded set of personal biological biometric identification parameters uniquely associated with the specific user, wherein said authentication unit is configured to compare the plurality of personal biological biometric identification parameters of the user holding the apparatus with the pre-recorded set of personal biological biometric identification parameters stored in said second storage unit;	**All of the Accused Instrumentalities include Samsung's Knox Vault:** Knox Vault is integrated into Samsung devices starting from the Galaxy S21, and is comprised of components that are Common Criteria evaluated to the requirements in BSI PP0084 at EAL4+ or higher. These components are tested by an independent lab against a wide array of hardware attacks and through a review of their software and firmware. *Id.*; OSNH_00000525-OSNH_00000554, *Devices Secured by Knox*, at 527-528 (emphasis added). **The Knox Vault includes Knox Vault Storage (a second storage unit) separate from the phone's main storage (first storage unit) and is used for storing sensitive information like biological biometric identification parameters uniquely associated with the specific user:** Samsung's Knox Vault is an evolution of the hardware-based security that Samsung has been building within Galaxy smartphones for years. Knox Vault extends upon the protection offered by our TrustZone, the Trusted Execution Environment (TEE) pioneered by Samsung to protect sensitive data such as passwords, biometrics, and cryptographic keys. Whereas the TrustZone runs a different OS alongside Android on the primary application processor, Knox Vault operates completely independently from the primary processor running the Android OS.  OSNH_00000647-OSNH_00000654, *Knox Documentation, Knox Vault*, *supra*, at 647 (emphases added).

As a core component of the Knox security platform, Knox Vault is an isolated, tamper-proof, secure subsystem with its own processor and memory, as well as an interface to dedicated, non-volatile secure storage. Knox Vault can:

- Store sensitive data such as hardware-backed Android Keystore keys, the Samsung Attestation Key (SAK), biometric data, and blockchain credentials.
- Run security-critical code that authenticates users with increasing timeouts between failures and controls access to keys depending on authentication.

Knox Vault is integrated into Samsung devices starting from the Galaxy S21, and is comprised of components that are Common Criteria evaluated to the requirements in BSI PP0084 at EAL4+ or higher. These components are tested by an independent lab against a wide array of hardware attacks and through a review of their software and firmware.

Id. (emphasis added).

The Knox Vault has components used for authentication.

Samsung Knox Security Principles

Trust from the hardware up

Provide a safe execution environment for security-sensitive software

We provide security hardware dedicated to processing sensitive and confidential data while protecting against malware attacks.

Protected Video Playback, User authentication, and Payment Applications run in our safe execution environment. For User Authentication Apps, our safe execution environment blocks unauthorized access to sensitive biometric information. For Payment Apps, our safe execution environment ensures the secure handling of payment transactions.

OSNH_00000555-OSNH_00000557, *Samsung Knox Security Principles*, at 555 (emphasis added).

The Samsung Knox platform

Last updated February 20th, 2024

Samsung Knox brings defense-grade security on the most popular consumer devices to all enterprises. The Knox Platform provides best-in-class hardware-based security, policy management, and compliance capabilities beyond the standard features commonplace in today's mobile device market. The Knox Platform is the cornerstone of a strong mobile security strategy supporting a wide variety of Samsung devices ↗.

* * *

Hardware-backed security

The Knox Platform defends against security threats and protects enterprise data through layers of security built on top of a hardware-backed trusted environment.

- **Trusted environment** — A trusted environment separates security-critical code from the rest of the operating system. This strategic separation ensures only trusted processes that are isolated and protected from attacks and exploits can perform sensitive operations, such as user authentication and key encryption and decryption. Trusted environments perform integrity checks prior to executing any software. These checks detect malicious attempts to modify the trusted environment and the software running on the device.

* * *

Futhermore, the Knox Vault introduced with the Samsung Galaxy S21 offers an isolated, tamper-proof, secure subsystem with its own processor and memory. Knox Vault operates completely independently from the primary processor running the Android OS, and guards against attacks that exploit shared resources, such as software side-channel attacks that can compromise other software executing on the same processor. This separation means Knox Vault protects sensitive data even if the primary processor itself is completely compromised.

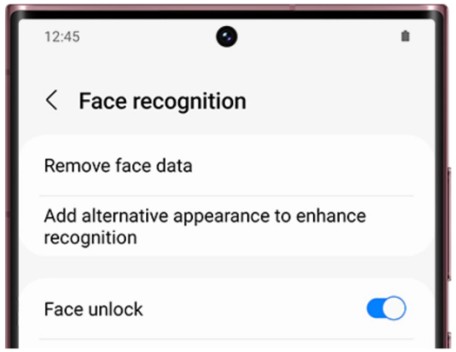
OSNH_00000558-OSNH_00000565, *The Samsung Knox Platform*, at 559, 562 (emphases added).

Personal biological biometric identification parameters uniquely associated with the specific user are stored.

For finger authentication, *e.g.*, the 2D print and print depth are stored.

	To read the valleys and ridges of a finger, the new sensor uses sound waves. It transmits an ultrasonic pulse against the finger to create a 3D reproduction of the fingerprint. This process makes it distinct from other solutions that use the 2D light-sensing optical approach. Moreover, the sensor is capable of detecting blood flow within the finger, making it hack-proof from a photo of a mold. OSNH_00000339-OSNH_00000345, Vishal Kawadkar, *How Qualcomm's 3D Sonic Fingerprint Sensor Could Be A Great Tool In Covid-19 Era*, at 341 (Jan. 12, 2021). **For facial authentication, *e.g.,* the width of a user's nose and distance between eyes are stored.** When a user opts to access their Galaxy S8 using facial recognition verification, the smartphone detects, aligns, extracts and compares facial landmark points such as the width of the user's nose or the distance between their eyes to stored data to grant or deny access. As the user continues to utilize the feature more and more, the phone gets better at recognizing them, despite small changes in the angle or position of their face during the verification process. Samsung's Biometric Technologies Bring Added Security and Convenience to the Galaxy S8 OSNH_00000670-OSNH_00000674, at 671. **For facial authentication, additional facial features (*e.g.*, hairstyle, facial hair, and makeup) can be stored.**

- **Remove face data:** Delete the current face recognition data that is stored.
- **Add alternative appearance to enhance recognition:** This is useful if you change your hairstyle, facial hair, or makeup.
- **Face unlock:** Unlocks your device when your face is recognized.
- **Stay on Lock screen until swipe:** Remain on the Lock screen until you swipe even if you already used Face recognition.



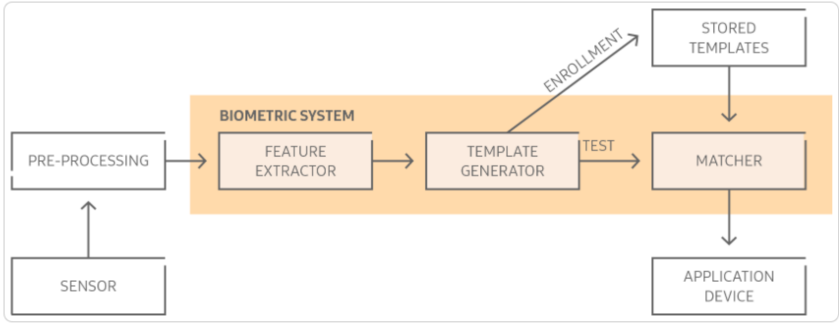
OSNH_00000329.

On information and belief, the Accused Instrumentalities store the above biological biometric identification parameters, or a representation of such data thereof.

During Face Unlock and Fingerprint Unlock, Knox Vault compares incoming data from the biosensors (*e.g.*, the front camera and fingerprint sensor) to the stored biological biometric identification parameters in the Knox Vault to determine if there is a valid match.

<table>
<tr>
<td></td>
<td>

Unique advantages of Knox Biometrics



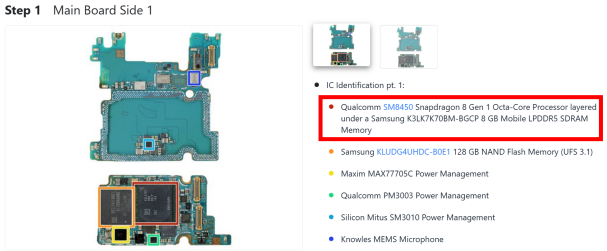
OSNH_00000351-OSNH_00000353 at 351, *Samsung Knox Documentation* (Feb. 20, 2024).

</td>
</tr>
<tr>
<td>a processor in communication with said plurality of biometric sensors, said first storage unit and said authentication unit;</td>
<td>

As shown below, all Accused Instrumentalities include one or more processors in communication with the biometric sensors, the first storage unit, and the authentication unit:

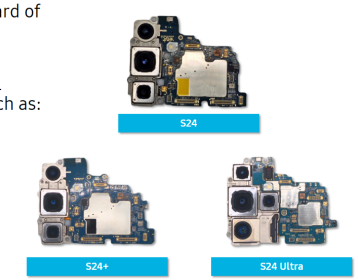
<table>
<tr><th>Galaxy S21 line</th><th>Galaxy S22 line</th></tr>
<tr>
<td>

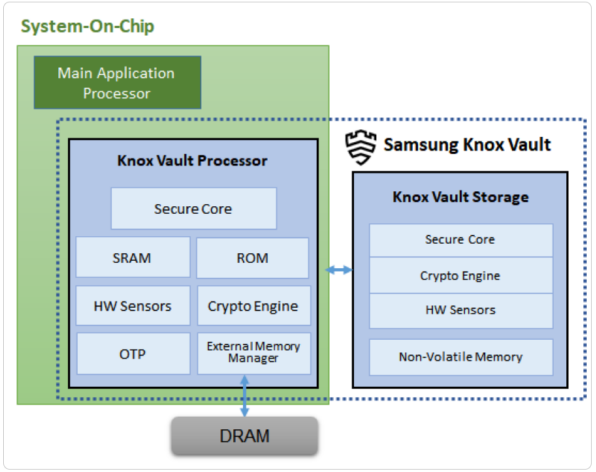
</td>
<td>



</td>
</tr>
</table>

</td>
</tr>
</table>

	OSNH_00000401-OSNH_00000413, *Samsung Galaxy S21 Ultra Teardown*, *supra*, at 408 (emphasis added).	OSNH_00000573-OSNH_00000578, *Samsung Galaxy S22 Chip ID*, at 574 (emphasis added).
	Galaxy S23 line	**Galaxy S24 line**
		The Main PBA is the main board of the device. It contains the most essential components of the device such as: • Mobile Chipset • Main Camera • Built in Storage • Sub Microphone  • Samsung's new Galaxy S24 lineup of flagship smartphones are powered by Qualcomm's latest Snapdragon 8 Gen 3 for Galaxy platform. • The chip is said to have an improved NPU, which has helped Samsung turn the S24 series into a group of AI smartphones. • The Snapdragon 8 Gen 3 for Galaxy platform powers the Galaxy S24 Ultra in all markets, but the S24 and S24 Plus use Samsung's Exynos chips in some regions.
	OSNH_00000422-OSNH_00000430, *Galaxy S23 Ultra Chip ID*, *supra*, at 423 (emphasis added).	OSNH_00000431-OSNH_00000514, *Samsung Galaxy S24 Repair Guide*, at 437; OSNH_00000579-OSNH_00000588, Brady Snyder, *AI features on the Galaxy S24 are powered by Snapdragon 8 Gen 3 for Galaxy, but not everywhere*, Android Central, at 580 (emphasis in original).



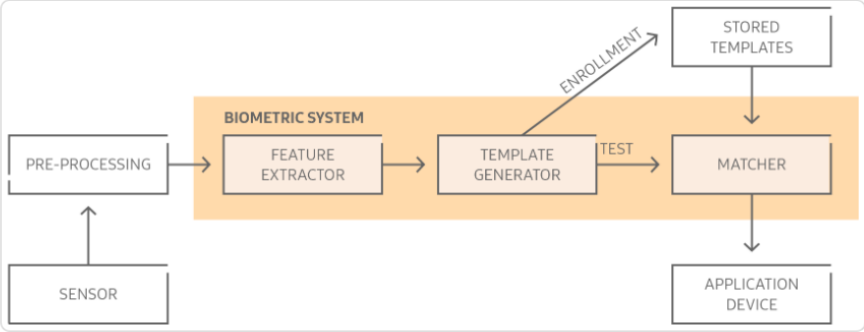
OSNH_00000647-OSNH_00000654, *Knox Documentation, Knox Vault*, *supra*, at 650.

Knox Vault Processor

The Knox Vault Processor provides the main computing power for Knox Vault. To provide the strongest isolation, the Knox Vault Processor is separated from the primary processor on the SoC. 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 SRAM, the Knox Vault Processor also guarantees a physically isolated execution environment. The Knox Vault Subsystem ROM where the secure boot loader code is located is also separated and protected by the hardware protection mechanisms. When the Knox Vault Processor starts, the ROM code is loaded to SRAM. While the ROM code loads the Knox Vault Processor firmware, with the help of the modules running on the SOC main processor, the software stack of Knox Vault Processor has its own secure boot chain.

Id. (emphasis added).

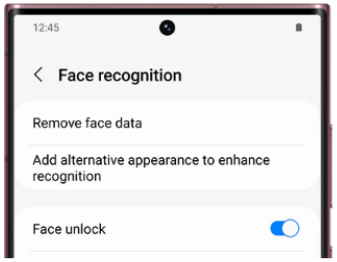
wherein access to the personal data and documentation files stored in said first storage unit is only enabled after said authentication unit positively matches each of the plurality of personal biological biometric identification parameters of the user holding the apparatus with the pre-recorded set of personal biological identification parameters stored in said second storage unit;	**As discussed on pgs. 1-16, the Accused Instrumentalities include the authentication features.** **These authentication features enable the user to access the phone and data thereon only when each of the incoming biometric data from the camera or fingerprint scanner matches the corresponding stored template data.** **Unique advantages of Knox Biometrics**  OSNH_00000351-OSNH_00000353, *Samsung Knox Documentation*, *supra* at 351.
wherein, whenever any of said at least one life signs detector detects a critical level of said user measured life sign parameters, the apparatus is configured to prevent access to said user's personal data and documentation files stored in said first storage unit.	**The Accused Instrumentalities further prevent access to the smartphone and data thereon if the front facing camera detector does not confirm a face with open eyes or if the fingerprint detector does not detect at least a fingerprint with life signs such as blood flow.** **The Accused Instrumentalities cannot be unlocked, or applications such as Samsung Wallet/Pay accessed, unless life signs are detected.**

Face Unlock:

Facial recognition options

Once your face is registered to your device, you can use additional security options and settings. To access these options, navigate to **Settings**, and then tap **Security and privacy**. Tap **Biometrics**, then tap **Face recognition**, and then enter your security credentials. The following will be available:

- **Remove face data:** Delete the current face recognition data that is stored.
- **Add alternative appearance to enhance recognition:** This is useful if you change your hairstyle, facial hair, or makeup.
- **Face unlock:** Unlocks your device when your face is recognized.
- **Stay on Lock screen until swipe:** Remain on the Lock screen until you swipe even if you already used Face recognition.



- **Require open eyes:** For added security, the device will only recognize your face when your eyes are open.
- **Brighten screen:** Increase screen brightness temporarily so your face can be recognized in the dark.

OSNH_00000329, *Use Facial recognition security on a Galaxy phone or tablet*, SEA (2024) (emphasis added).

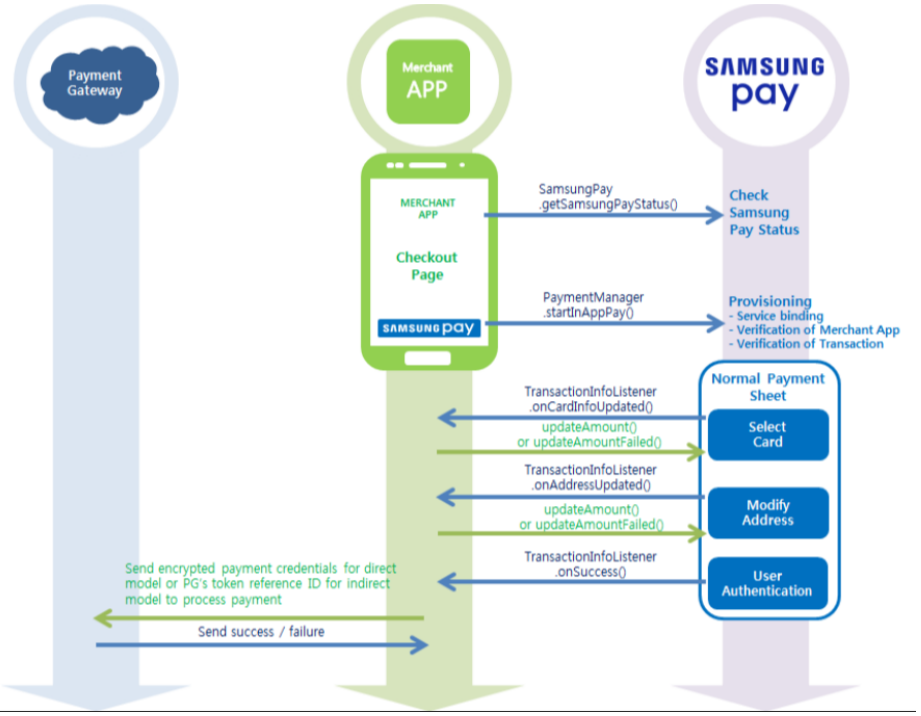
Fingerprint Unlock:

To read the valleys and ridges of a finger, the new sensor uses sound waves. It transmits an ultrasonic pulse against the finger to create a 3D reproduction of the fingerprint. This process makes it distinct from other solutions that use the 2D light-sensing optical approach. Moreover, the sensor is capable of detecting blood flow within the finger, making it hack-proof from a photo of a mold.

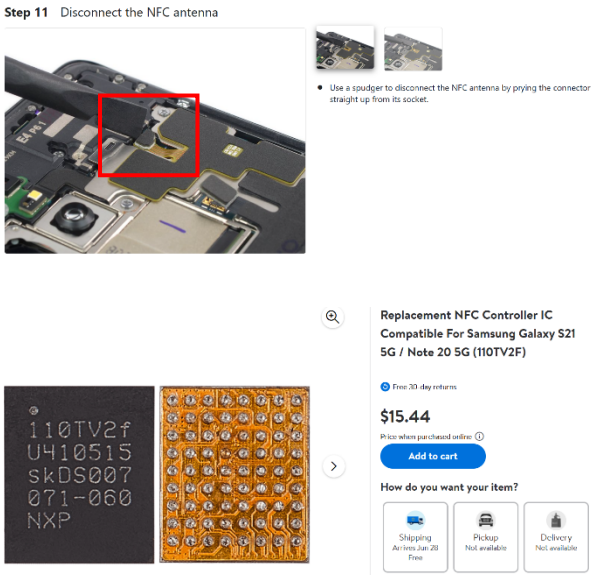
	OSNH_00000339-OSNH_00000345, Vishal Kawadkar, *How Qualcomm's 3D Sonic Fingerprint Sensor Could Be A Great Tool In Covid-19 Era*, at 341 (Jan. 12, 2021) (emphases added). **Delivering security-rich, built-in anti-spoofing security.** Safeguard a user's identity with the most advanced fingerprint security system available. 3D Sonic uses acoustic-based technology that reflects the unique features of a user's individua fingerprint vs. optical solutions, which leaves users exposed to spoofing. With anti-spoofing built in, neither a photograph nor fake mold of your finger can access your phone. OSNH_00000335-OSNH_00000338, *Qualcomm 3D Sonic Sensor*, *supra*, at 336 (emphasis added).

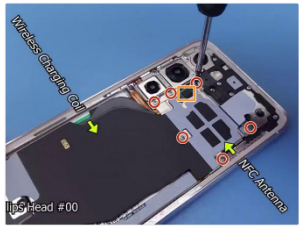
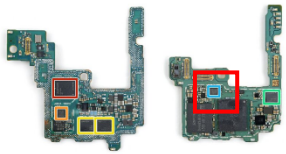
	Features • Supports mounting under display, metal, glass, plastic, and many other materials • One Tap Enrollment: No • Single finger support • 1:50K False Acceptance Rate (FAR) • Heart Rate Monitoring OSNH_00000346-OSNH_00000350, *3D Sonic Gen 2 Overview*, *supra,* at 347 (emphasis added).

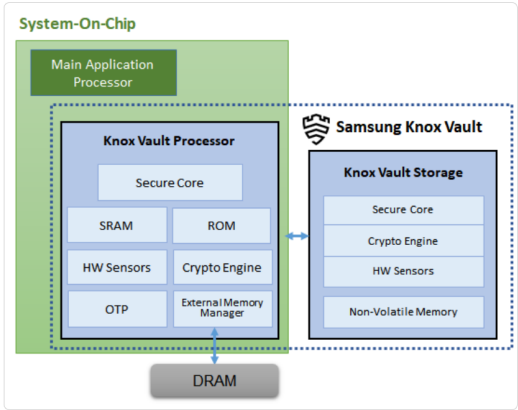
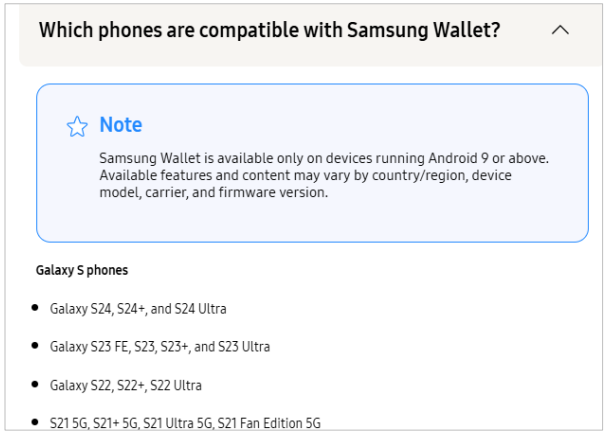
	 OSNH_00000339-OSNH_00000345, Vishal Kawadkar, *How Qualcomm's 3D Sonic Fingerprint Sensor Could Be A Great Tool In Covid-19 Era*, at 341 (Jan. 12, 2021) (emphasis added).

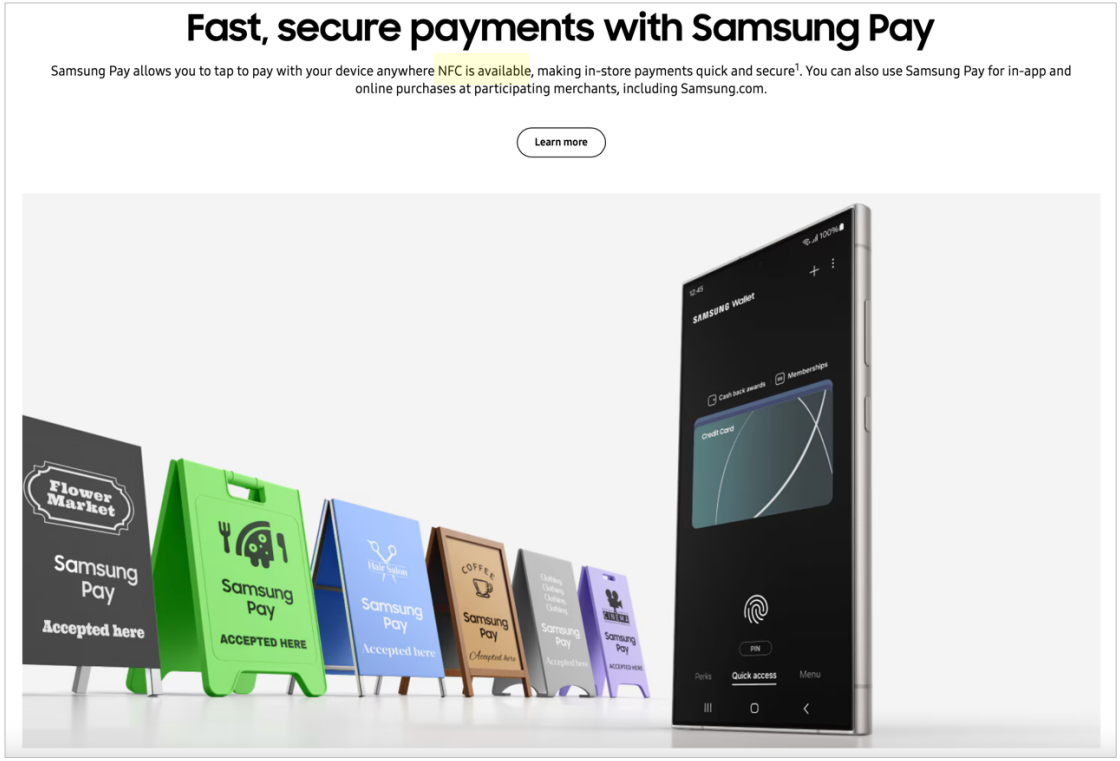
Claim 4. The apparatus according to claim 1, further comprising: communication and data connection means for communicating with an external device, said communication and data connection means being controlled by and in communication with said processor.	**An external device can be an external server, which may include a merchant or financial institution:**  OSNH_00000589-OSNH_00000591, *Samsung Pay SDK Programming Guide*, at 589. **The NFC controllers are controlled and in communication with the processors (pgs. 21–22) of the Accused Instrumentalities and include a data encoder/decoder and a wireless transceiver (pgs. 30–37).**

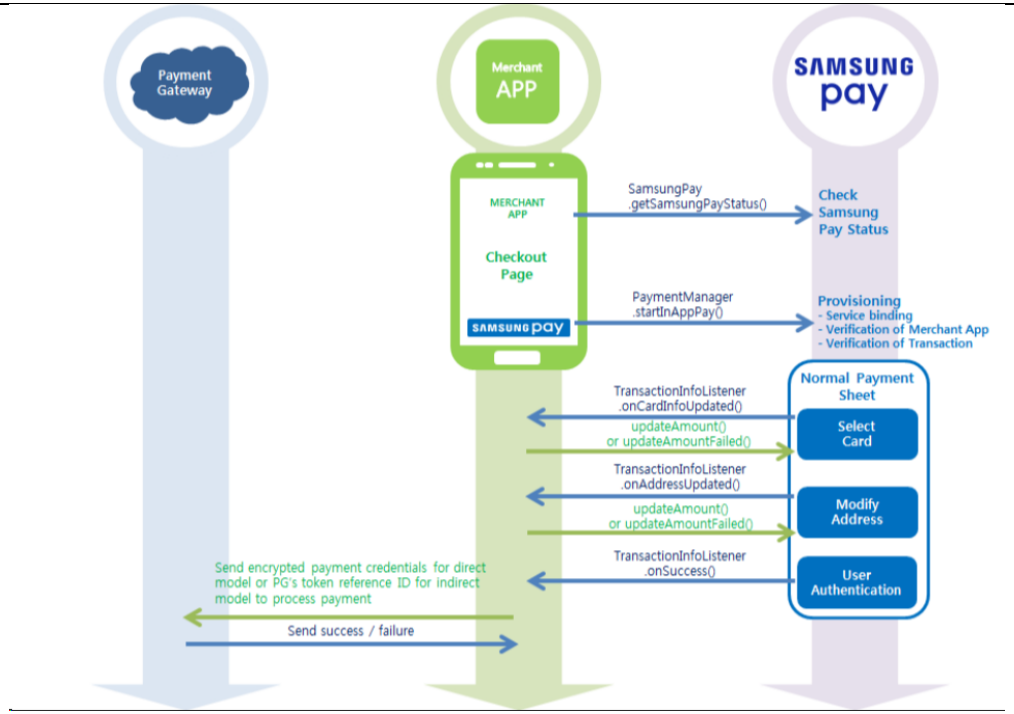
Claim 15. The apparatus according to claim 1, further comprising an integrated digital data encoder/decoder and a wireless transceiver module in communication with the processor,	**The Accused Instrumentalities have a digital data encoder/decoder and a wireless transceiver module, as evidenced below. For example, they include transceivers and encoders/decoders.**

Galaxy S21 line	Galaxy S22 line
	
OSNH_00000592-OSNH_00000601, *Samsung Galaxy S21 Ultra NFC Antenna & Charging Coil Assembly Replacement*, iFixit Repair Guide, at 599, (emphasis added); OSNH_00000602-OSNH_00000603, at 602 (last visited July 26, 2024).	OSNH_00000573-OSNH_00000578, *Samsung Galaxy S22 Ultra Chip ID*, *supra*, at 575 (emphasis added).

	Galaxy S23 line	Galaxy S24 line
	Step 2 Remove the Wireless Coil and NFC Antenna  • Unscrew the 6 Phillips #00 screws that weld the wireless charging base and the NFC antenna. • Disconnect the connector connecting the two antennas and remove everything. **Step 3** Main Board Side 1 - Connectivity  • Qualcomm WCN7851-101 FastConnect 7800 WiFi 7, 6, & 6E & Bluetooth 5.3 transceiver • NXP Semiconductor SR200T ? ultra-wideband transceiver • Qualcomm SDR735-001 RF transceiver • Qualcomm SMR546-002 RF transceiver • NXP Semiconductor SN220U ? NFC controller w/ secure elemen	The manufacturer with the main cost is Samsung. It supplied the Applications/Baseband Processor, DDR5X SDRAM, 3D TLC V-NAND Flash, RF Transceiver + GPS, NFC Controller, 8x Power Management, Camera Powe Management, 3x Envelope Power Tracker, and Clock Buffer. Samsung supplied a total of 18 chips for this device.
	OSNH_00000604-OSNH_00000612, *Galaxy S23 Teardown*, iFixit, at 605 (emphasis added); OSNH_00000422-OSNH_00000430, *Galaxy S23 Ultra Chip ID*, *supra*, at 424 (emphasis added).	OSNH_00000675-OSNH_00000677, *Deep Dive Teardown of the Samsung Galaxy S24*, at 675 (emphasis added).

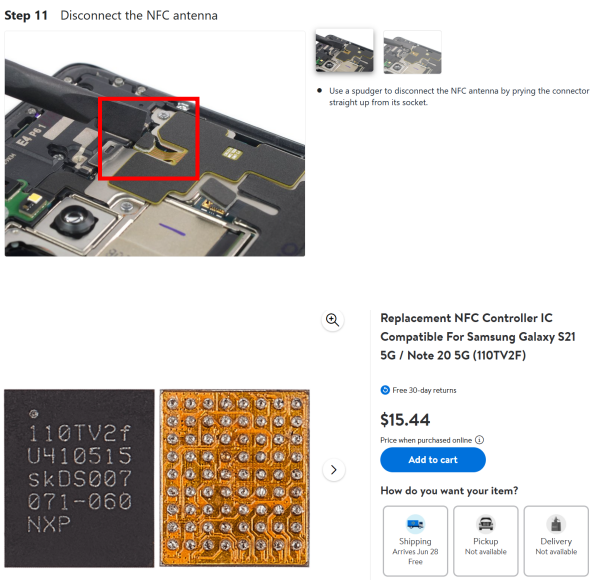
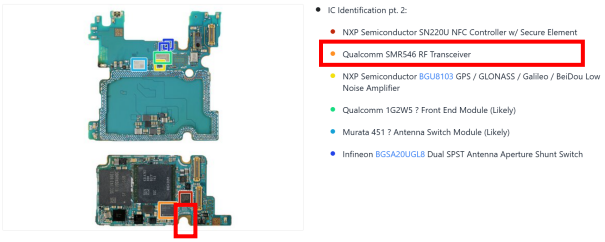
	 OSNH_00000647-OSNH_00000654, *Knox Documentation, Knox Vault*, *supra*, at 650. **The digital data encoder/decoder and a wireless transceiver module is in communication with the Processor (identified on pgs. 21-24)**.
said integrated digital data encoder/decoder and a wireless transceiver being configured to communicate with any of a group of external devices including RF operated credit card readers, ATM machines, and remotely operated electronic locks gates and doors opener using RFID based techniques.	**All the accused Galaxy S devices include Samsung Wallet/Pay.** 

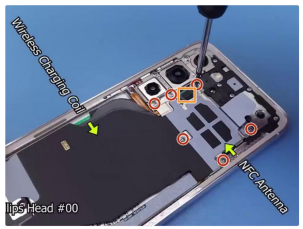
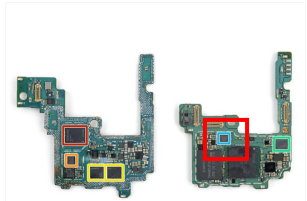
	OSNH_00000613-OSNH_00000615, *Use Samsung Wallet on Your Galaxy Phone*, at 613. **During the Samsung Wallet/Pay process, an encoder/decoder and transceiver (*e.g.*, NFC Controller) is used to access communication with, at least, point-of-sale terminals.**  OSNH_00000616, *Samsung Wallet* (emphasis added).



OSNH_00000589-OSNH_00000591, *Samsung Pay SDK Programming Guide*, at 589.

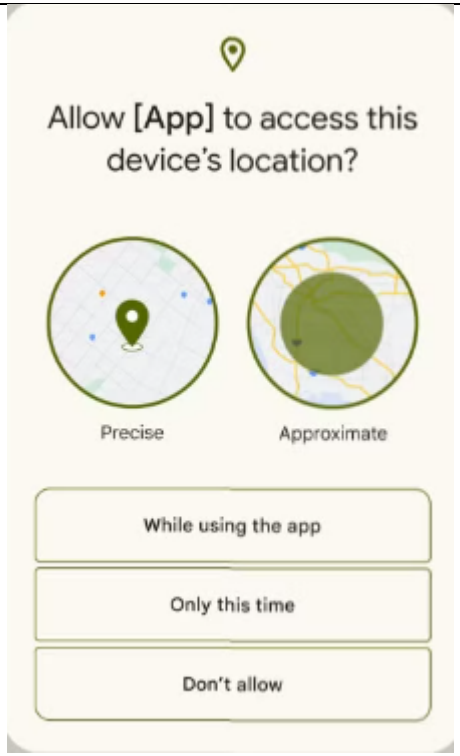
	User Authentication Ensures Control Another important part of maintaining Samsung Pay security is the user authentication process. All transactions also require that the user confirm the purchase, either by a PIN or a fingerprint. Payments must be authorized with the user's PIN or fingerprint so their mobile device only allows payments with the user's consent. **Samsung KNOX, the Most Certified Solution** With multiple levels of security right out of the box, down to the hardware level, Samsung KNOX offers unprecedented security for mobile devices. Samsung KNOX constantly monitors devices, scanning for any malware or suspicious activity, providing defense-grade security from the moment a device is first turned on. With its series of security features, Samsung KNOX has the most certifications and authorizations by governments, militaries and enterprises among Android manufacturers, ensuring Samsung Pay is the safest solution possible. OSNH_00000617-OSNH_00000621, *Multilayer Security and Convenience Make Samsung Pay a Winning Choice*, Samsung Newsroom, at 618 (emphases added). **An extra layer of security with Samsung Knox** Samsung Wallet is protected by Samsung Knox, Samsung's mobile security platform. Samsung Knox includes fingerprint recognition and encryption of your data to make sure your it is secure. OSNH_00000616, *Samsung Wallet*, *supra* (emphasis added).

	Galaxy S21 line	Galaxy S22 line
		
	OSNH_00000592-OSNH_00000601, *Samsung Galaxy S21 Ultra NFC Antenna & Charging Coil Assembly Replacement*, iFixit Repair Guide, at 599, (emphasis added); OSNH_00000602-OSNH_00000603, at 602 (last visited July 26, 2024).	OSNH_00000573-OSNH_00000578, *Samsung Galaxy S22 Ultra Chip ID*, *supra*, at 575 (emphasis added).

	Galaxy S23 line	Galaxy S24 line
	Step 2 Remove the Wireless Coil and NFC Antenna  • Unscrew the 6 Phillips #00 screws that weld the wireless charging base and the NFC antenna. • Disconnect the connector connecting the two antennas and remove everything. **Step 3** Main Board Side 1 - Connectivity  • Qualcomm WCN7851-101 FastConnect 7800 WiFi 7, 6, & 6E & Bluetooth 5.3 transceiver • NXP Semiconductor SR200T ? ultra-wideband transceiver • Qualcomm SDR735-001 RF transceiver • Qualcomm SMR546-002 RF transceiver • NXP Semiconductor SN220U ? NFC controller w/ secure elemen	The manufacturer with the main cost is Samsung. It supplied the Applications/Baseband Processor, DDR5X SDRAM, 3D TLC V-NAND Flash, RF Transceiver + GPS, NFC Controller, 8x Power Management, Camera Powe Management, 3x Envelope Power Tracker, and Clock Buffer. Samsung supplied a total of 18 chips for this device.
	OSNH_00000604-OSNH_00000612, *Galaxy S23 Teardown*, iFixit, at 605 (emphasis added); OSNH_00000422-OSNH_00000430, *Galaxy S23 Ultra Chip ID*, *supra*, at 424 (emphasis added).	OSNH_00000675-OSNH_00000677, *Deep Dive Teardown of the Samsung Galaxy S24*, at 675 (emphasis added).
Claim 18. The apparatus according to claim 1, further comprising an integrated GPS module in communication with the processor to precisely locate the geographical position of the apparatus.	**The Accused Instrumentalities include integrated GPS modules in communication with their processors (identified on pgs. 21-24) to precisely locate their geographical positions.**	

Galaxy S21 line	Galaxy S22 line
COMMS WLAN: Wi-Fi 802.11 a/b/g/n/ac/6, dual-band, Wi-Fi Direct Bluetooth: 5.0, A2DP, LE Positioning: GPS, GLONASS, BDS, GALILEO NFC: Yes Radio: FM radio (Snapdragon model only; market/operator dependent) USB: USB Type-C 3.2, OTG	COMMS WLAN: Wi-Fi 802.11 a/b/g/n/ac/6, dual-band, Wi-Fi Direct Bluetooth: 5.2, A2DP, LE Positioning: GPS, GLONASS, BDS, GALILEO NFC: Yes Radio: No USB: USB Type-C 3.2, OTG
OSNH_00000657-OSNH_00000659, at 658 (emphasis added).	OSNH_00000660-OSNH_00000662, at 661 (emphasis added).
Galaxy S23 line	**Galaxy S24 line**
COMMS WLAN: Wi-Fi 802.11 a/b/g/n/ac/6e, tri-band, Wi-Fi Direct Bluetooth: 5.3, A2DP, LE Positioning: GPS, GLONASS, BDS, GALILEO NFC: Yes Radio: No USB: USB Type-C 3.2, OTG	COMMS WLAN: Wi-Fi 802.11 a/b/g/n/ac/6e, tri-band, Wi-Fi Direct Bluetooth: 5.3, A2DP, LE Positioning: GPS, GLONASS, BDS, GALILEO, QZSS NFC: Yes Radio: No USB: USB Type-C 3.2, DisplayPort 1.2, OTG
OSNH_00000663-OSNH_00000665, at 663 (emphasis added).	OSNH_00000666-OSNH_00000669, at 667 (emphasis added).

The GPS modules allow the precise geographical position of the Accused Instrumentalities to be located:

	 Android request location permission.