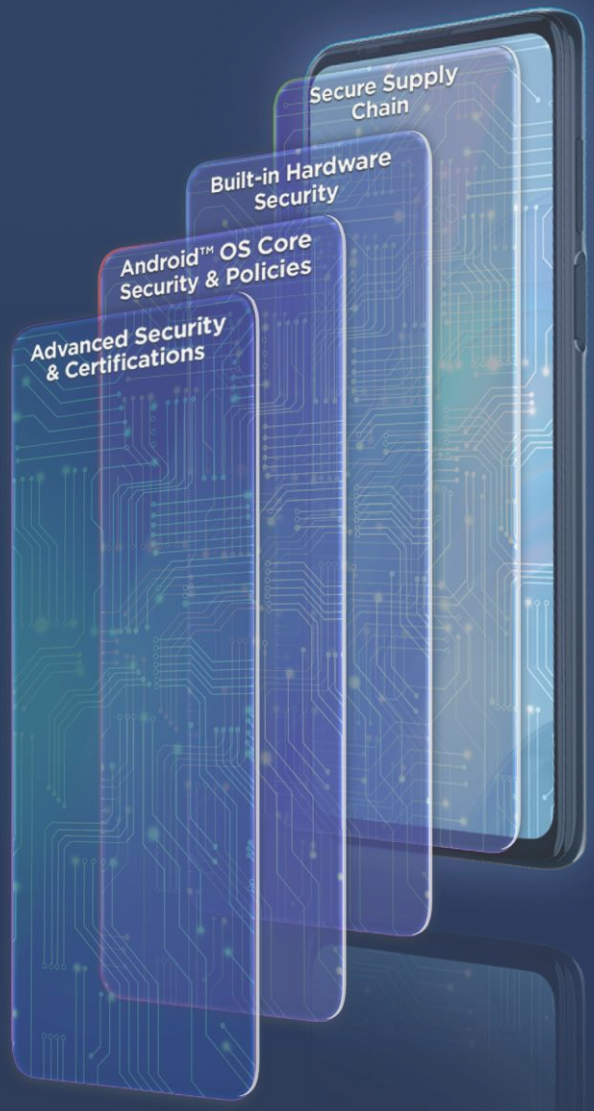
motorola
FOR BUSINESS

ThinkShield
FOR MOBILE

ADVANCED SECURITY FOR YOUR MOBILE DEVICES



motorola
FOR BUSINESS

SMARTPHONES ARE INCREASINGLY AT THE CENTER OF OUR WORK LIVES

We use them to access emails, to make voice and video calls, and to store and access various types of sensitive data, making smartphones a high value target for cyber criminals.

According to a 2020 survey, 46% of organizations reported having at least one employee who unknowingly downloaded a malicious mobile app[1], and 97% of organizations faced mobile threats that used multiple attack vectors in 2020, exposing them to increasing data and security risks.

ThinkShield for Mobile is built into our Motorola devices[2] and is designed to provide best-in-class business-grade security so that you can trust your smartphone is protected against these threats.

1Source: Check point's Mobile Security Report 2021

2 ThinkShield for mobile available on select devices. Thinkshield is a registered Trademark of Lenovo.

ThinkShield
FOR MOBILE

At the core, ThinkShield for mobile is Motorola's platform security – which is the set of underlying fundamental security policies, features, hardware, software and processes that ensure the security of the entire device including the operating system.

MULTILAYER SECURITY OVERVIEW

Motorola breaks down device protection into three main layers:

1. SUPPLY CHAIN SECURITY

Our supply chain has been recognized by Gartner as one of the Top 7 High Tech supply chains. We evaluate suppliers of intelligent components to validate that each one understands and follows proper security practices.

2. BELOW THE OS SECURITY

Securing the entire system with hardware backed security controls, trusted boot and revocation, security hardening, and secure development processes and practices.

3. OS TO CLOUD SECURITY

A clean OS with advanced security features, including additional security maintenance releases (SMRs) and OS upgrade support.

motorola
FOR BUSINESS

MULTI-LAYER SECURITY FOR END TO END PROTECTION

OS TO CLOUD

- FIPS 140-2 — FIPS CERTIFICATION
- android enterprise recommended — AER
- FACTORY RESET PREVENTION
- GOOGLE SAFETY NET
- GOOGLE PLAY PROTECT
- CHROME SAFE BROWSING
- CLEAN OS

BELOW THE OS

- SECURE BOOT
- CROSS FLASH PROTECTION
- SECURITY ENHANCED FOR ANDROID
- HSM BASED CODE SIGNING
- TAMPERPROOF IDENTITY
- USB PROTECTION
- HARDWARE BASED REVOCATION
- HARDWARE ROOT OF TRUST
- UNLOCKED BOOTLOADER FUSE

SUPPLY CHAIN

- TRUSTED SUPPLIER PROGRAM
- SECURE FACTORY PROVISIONING
- INCIDENT RESPONSE TEAM

motorola
FOR BUSINESS

SUPPLY CHAIN SECURITY

SECURE STRAIGHT OUT OF THE FACTORY

TRUSTED SUPPLIER PROGRAM

SECURE FACTORY PROVISIONING

INCIDENT RESPONSE TEAM

TRUSTED SUPPLIER PROGRAM

Today's smartphones are made up of many hardware and software components that contribute to the overall security of the device. The Trusted Supplier Program[3] is a multi-level security evaluation with zero trust policies for all Motorola component vendors who supply intelligent components.

3 https://www.lenovo.com/us/en/product-security/supply-chain/

motorola
FOR BUSINESS

TRUSTED SUPPLIER PROGRAM

Vendors of "intelligent components" must demonstrate their overall security posture, as well as the security of individual components they supply. Intelligent components include: any software or firmware program on any microprocessor; the microprocessor itself; any semiconductor device that has data processing ability, any component or device that has internal memory; any component or device that performs an input/output function. Examples of intelligent devices include memory devices and biometric sensors.

To start the process, a vendor needs to be pre-qualified by our Product Security Office. This evaluation covers the vendors IT security and overall product security practices and policies.

Following this stage, individual component offerings from the vendor are reviewed from a product security perspective to ensure they meet security requirements before business is awarded and that component is allowed to be used in a product.

SECURE FACTORY PROVISIONING

Device security must be considered from the very beginning of the manufacturing process. It ensures that devices are not tampered with and will be secured with the correct configuration. Motorola's secure provisioning process and infrastructure ensures these requirements are met. Secure servers utilizing Hardware Security Modules (HSM) are at the heart of this process.

First, the device production security policy is applied. This process includes configuring the SoC One Time Programmable fuses and Root of Trust and verifying the appropriate configuration has been applied.

Next, the device configuration is applied according to the specific model being manufactured. This configuration record is signed uniquely for the device. The device identity is then assigned and programmed, with the identity records signed in the same way. Only authorized factory stations may sign these configuration records.

The last step is device key programming; keys such as the Attestation Key must remain private and never exposed to the factory environment. Keys are delivered from our secure Key Generation Facility encrypted to the factory servers with multiple layers of encryption applied. Hardware based access controls ensure that only authorized factory test stations may connect to the factory server to receive device keys, and the keys are encrypted in such a way they are only accessible to the authorized device model being provisioned. Throughout the process, auditing records and testing ensures devices are properly configured and secured prior to being approved for shipment to a customer.

motorola
FOR BUSINESS

PRODUCT SECURITY INCIDENT RESPONSE TEAM

New threats and vulnerabilities emerge on a regular basis. A critical part of the secure product lifecycle is monitoring, analyzing, and patching security vulnerabilities before they can be exploited. Motorola's Product Security Incident Response Team (PSIRT) actively manages reports from vendors, customers, and researchers, as well as monitors the internet and dark web for threats that may impact our devices. We respond to all reported product vulnerabilities within 48 business hours. When vulnerabilities are reported or discovered, they are recorded in our vulnerability tracking system. Vulnerabilities are analyzed for product applicability, severity/impact, and patching strategy, and we coordinate with vendors and internal teams to provide the necessary patches. Patching status for affected products is tracked on a per product/model basis end-to-end to ensure devices receive the required patches on supported software releases.

motorola
FOR BUSINESS

BELOW THE OS SECURITY OVERVIEW

HARDWARE SECURITY

- HARDWARE ROOT OF TRUST
- TRUSTED EXECUTION ENVIRONMENT
- HW FIREWALLS
- ONE TIME PROGRAMMABLE FUSES
- ENCRYPTION ENGINES
- MOTO STRONGBOX

CORE PLATFORM SECURITY

- TRUSTED BOOT & REVOCATION
- HSM BASED CODE SIGNING
- ANDROID KEYSTORE & DEVICE ID ATTESTATION
- FILE ENCRYPTION
- SECURIY ENHANCED LINUX EXTENSIONS
- TAMPERPROOF IDENTITY
- USB PROTECTION
- OS HARDENING

motorola
FOR BUSINESS

INTEGRATED SECURITY IN A SINGLE CHIP

Feature rich modern smartphones are highly complex, supported by many subsystems that must work together to deliver the technology behind that the user experiences. Integrity protection, access controls, isolation, and cryptography are critical building blocks to ensure data security and privacy within the system. These functions must be built into the underlying hardware architecture, along with appropriate configuration, to ensure security guarantees are met. ThinkShield for Mobile platform not only utilizes a System on Chip (SoC) with these capabilities, but our implementation takes full advantage of these hardware features to underpin OS security features and address the mobile device threat model.

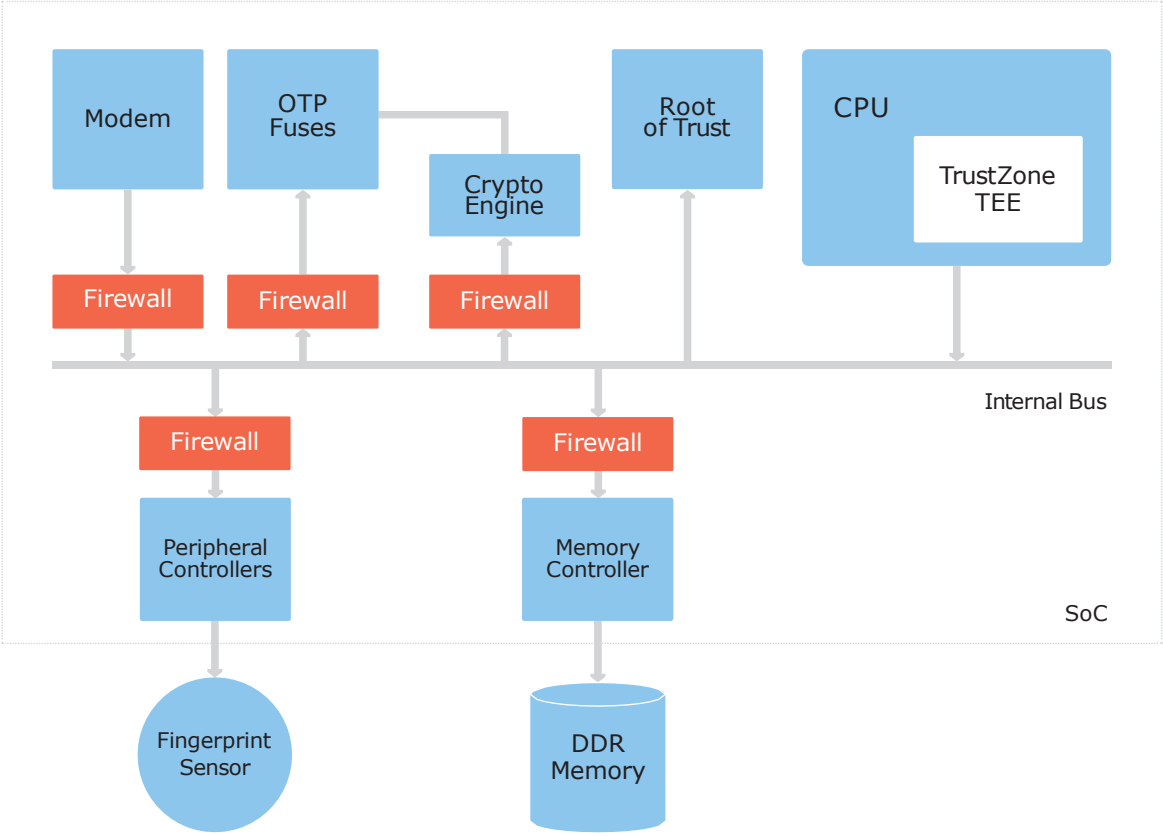


Figure 1. Conceptal view of System on a Chip (SoC)

HARDWARE SECURITY OVERVIEW

HARDWARE ROOT OF TRUST

A key aspect of platform security is verifying the integrity of each and every subsystem code before it is executed, ensuring the device can only execute software approved and released by Motorola for use on that device. SoC's used by Motorola contain embedded unchangeable boot ROMs which use a Motorola root key burned and locked into the SoC in the factory. The SoC is configured to always boot through the boot ROM. The boot ROM uses the root key to validate a 1st stage bootloader, which in turn validates the subsequent stage, continuing in a chain-of-trust fashion. In this way, trust is built and extended throughout the system.

TRUSTED EXECUTION ENVIRONMENT (TEE)

The TEE hosts a small, compartmentalized OS used for executing security critical functions. These functions include managing cryptographic hardware and associated keys, configuring hardware access controls, managing biometric data & payment credentials. Modern OS's are complex with a large attack surface. Without an isolated execution environment such as the TEE, vulnerabilities in the Android OS or kernel could be used to compromise the entire device. The TEE isolation guarantees are supported by ARM TrustZone technology, along with hardware firewalls which are used to restrict access to hardware resources owned by the TEE.

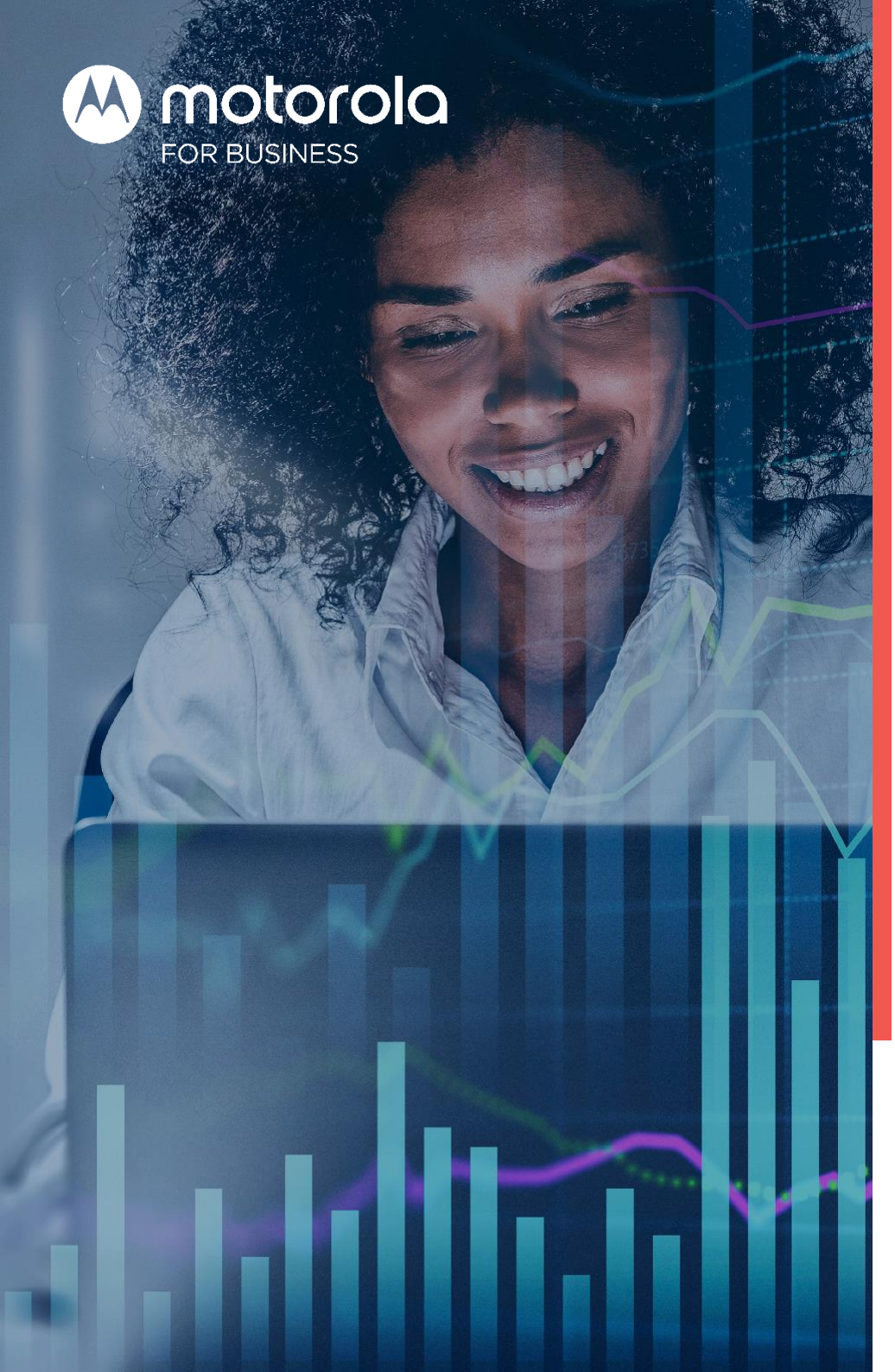
motorola
FOR BUSINESS

HARDWARE FIREWALLS

Access control within an SoC is critical to ensure that vulnerabilities in one subsystem can't affect another subsystem. A subsystem must only have access to the resources it owns or is required to interact with. Access controls may be applied to resources such as memory, IO, or other peripherals (e.g., secure element, USB). In this way, subsystems related to wireless connectivity, cellular network, power management, camera, audio, biometrics, and encryption may be isolated from each other and the main operating system. This limits the impact of a security vulnerability in any one of these systems. The hardware firewalls are implemented by the SoC vendor within the chip and configured as needed by Motorola given the product design. For example, the IO connected to the biometric fingerprint sensor is configured so that it is only accessible to the fingerprint application running inside the TEE. The Android OS, or any other subsystem, is blocked from accessing the sensor or biometric data.

ENCRYPTION ENGINES

Encryption is fundamental to data protection. Data stored on a mobile device must be protected while at rest and protected from decryption outside of the device or by unauthorized applications. SoC encryption hardware is used to protect the keys and device data, ensuring they are bound to the device and cannot be extracted.



This begins with the Root Encryption Key that is programmed into an SoC in the factory. This key is unique to each device and can only be accessed by the main cryptographic hardware module, which itself is a TEE owned resource. This key is then used to protect other keys that are used in support of file encryption, Android Keymaster, and protection of data in other subsystems. Other encryption engines, such as the inline encryption engine used for file encryption, can be used to protect keys so they are not available to the Android operating system.

ONE TIME PROGRAMMABLE FUSES

A fuse is a type of memory which is unchangeable following programming. This memory is used to store keys and security configuration on the SoC. During device manufacture, Motorola programs the security configuration fuses. These security configuration fuses restrict access to security sensitive debug interfaces and set other configuration options to ensure the SoC is configured to the highest possible security level. The device root public keys are also programmed into fuses as part of the device root of trust. Additionally, the fuses are used to store revocation data. If a software vulnerability is discovered and patched, the revocation data in the fuses is updated so the older, vulnerable software, cannot pass validation following update to the patched version. Using fuses ensures permanent revocation of the vulnerable software.

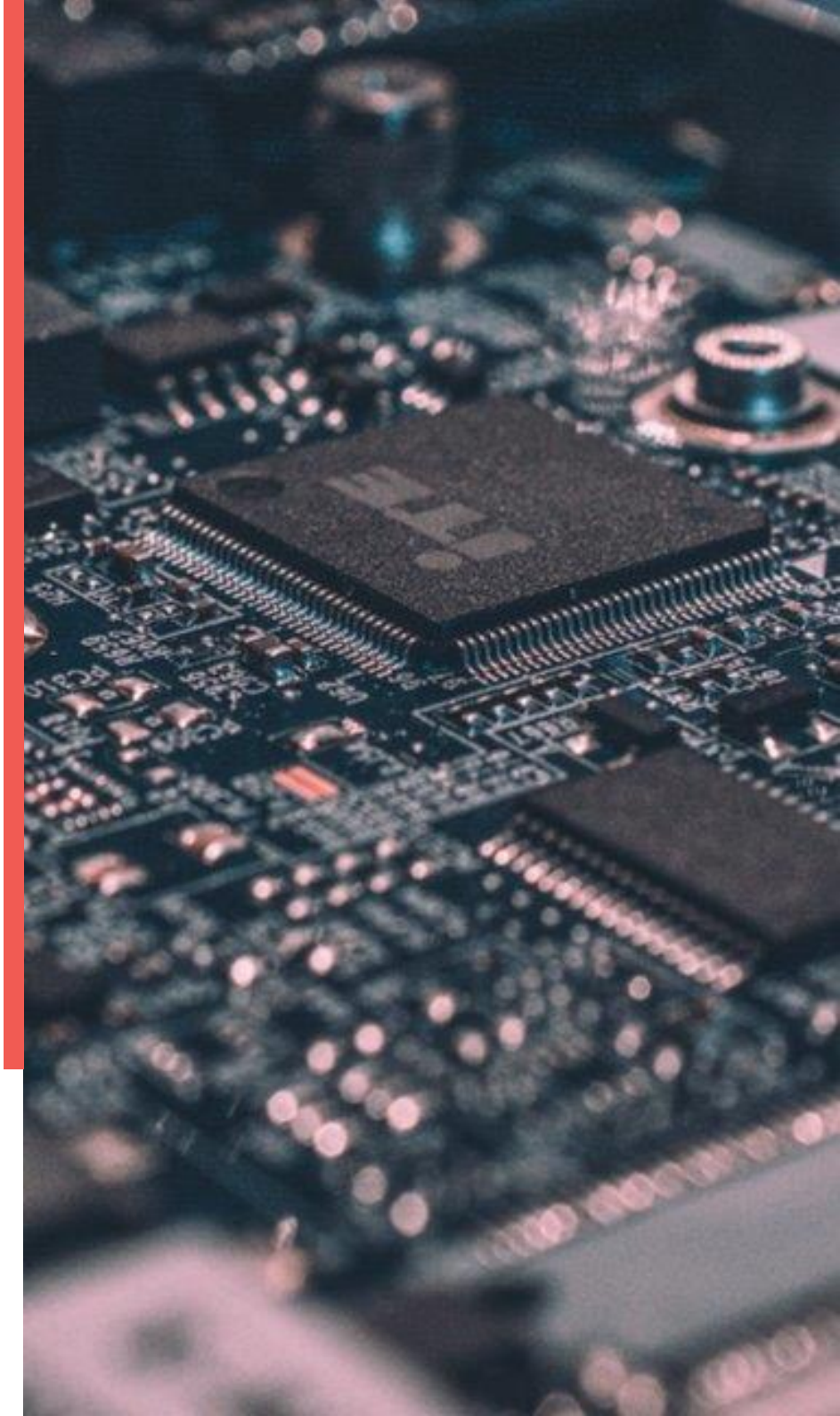
motorola
FOR BUSINESS

MOTO STRONGBOX

Moto Strongbox provides select devices with the latest device security technology. With Moto Strongbox, our devices have a physical security processor that is dedicated to running processes securely and protecting sensitive data and information.

Moto Strongbox delivers hardware-level security with tamper-resistant protection. As a physically isolated processor, Moto Strongbox can withstand any malicious attacks on the core processor. One way it provides this protection is by having its own physically separate memory location where all highly sensitive digital keys are stored. With this level of protection, sensitive processes (device unlock and file encryption) and data are better protected from advanced attacks (physical and side-channel attacks).

In addition, our devices with Moto Strongbox are ready for future solutions that will use this technology. Some of these solutions may include digital car and house keys, digital passports and driver licenses, and future payment solutions. With Moto Strongbox built-in, developers of these new solutions are able to leverage our dedicated security processor to provide their users with peace of mind that their most valuable assets are safe on a Motorola device.



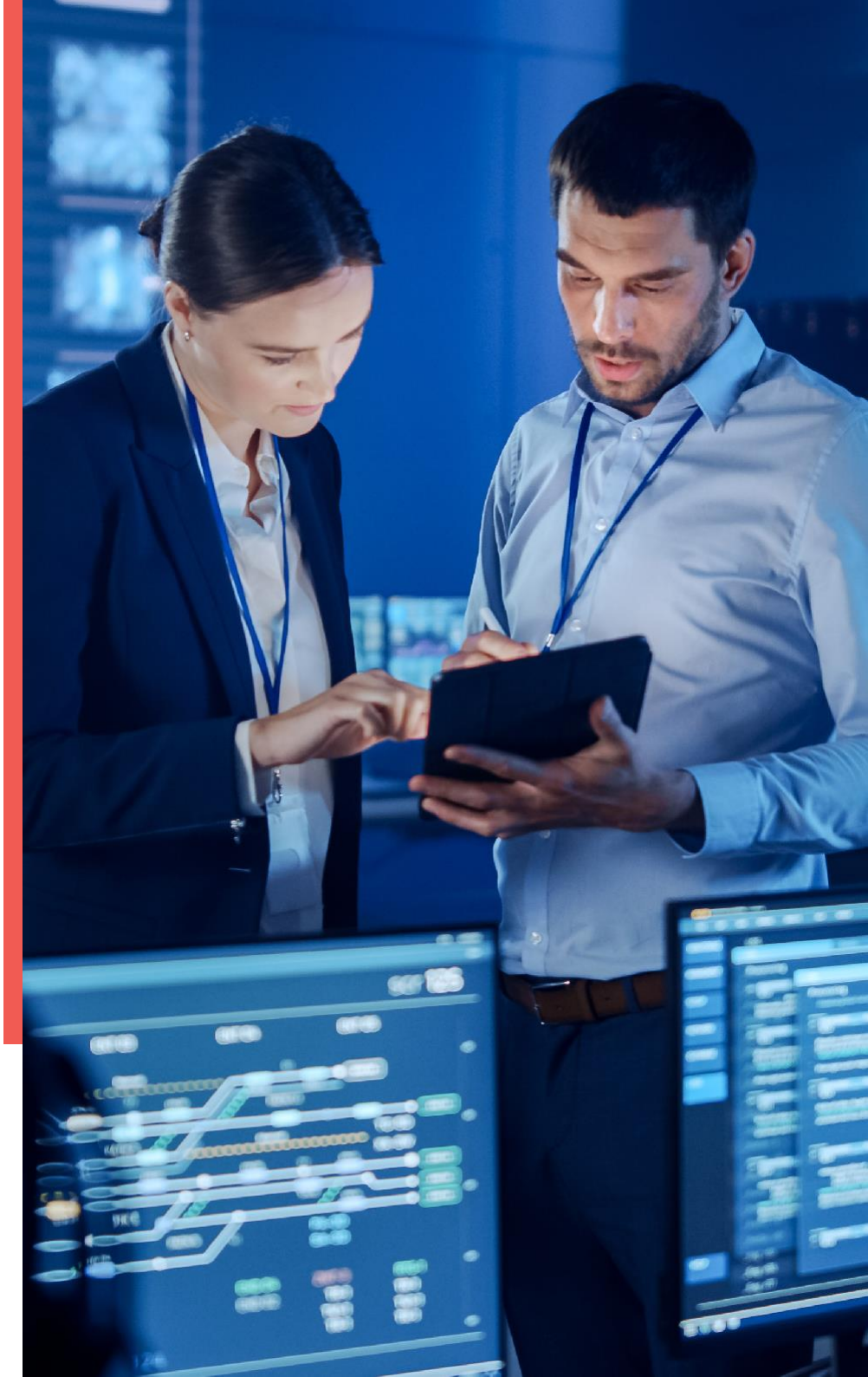
motorola
FOR BUSINESS

CORE PLATFORM SECURITY OVERVIEW

TRUSTED BOOT AND REVOCATION

In order to maintain trust and integrity, it's necessary for the device to validate all system software prior to execution. Motorola implements a Trusted Boot & Revocation mechanism whereby all system software is cryptographically signed by Motorola and validated before it's executed. This includes not only the Android operating system and kernel, but the bootloaders and firmware of each underlying hardware subsystem. This is achieved by using the SoC Root of Trust in the hardware to validate images in a chain of trust format. Cryptographic signatures are applied using industry standard algorithms and key lengths: RSASSA-PSS with SHA256 and 2048 bit keys, or ECDSA P-384 with SHA384 (varies based on product).

For Android OS secure boot, Motorola uses Android Verified Boot 2.0 and has extended it to add support for cross-flash prevention. The cross-flash prevention feature blocks software released for a given region/model/carrier from booting on a device where its factory configuration does not match. Each device is personalized in the factory for a given region/model/carrier using a factory signed record bound to an unchangeable identifier in the SoC hardware. On boot, the factory record signature and hardware identifier match are verified, and the signed OS configuration is verified against the factory configured record. If there is a mismatch, the OS will not boot.



motorola
FOR BUSINESS

"Smartphones are at the core of our business and personal lives and both companies and individuals need added security on their devices that can help protect their sensitive data and guard against online and identity-based threats. This is even more critical as our phones are used in remote working environments. Motorola is tackling this need head-on, delivering a 'breakthrough' portfolio of security features and solutions that are business-grade, but non-business users also benefit from the protection they provide as well. Congratulations to Motorola on being the clear choice for the 'Mobile Security Solution Provider of the Year' award."

James Johnson, managing director, Mobile Breakthrough.

TRUSTED BOOT AND REVOCATION (CONTD.)

This feature provides extra assurance to Enterprises/carriers that devices may not be reprogrammed with software for another SKU they did not approve. It also prevents a security exploit exclusive to one model variant from being used on a similar model that isn't affected.

Not only does Motorola's Trusted Boot solution validate each image prior to execution, but as an additional layer of defense each image is integrity validated before it is allowed to be written into the device. This policy applies to local USB programming as well as OTA updates. This step not only blocks local Denial of Service attacks if an invalid image were loaded, but also mitigates potential exploitation risks when invalid images are present in memory.

When software vulnerabilities are discovered and patched, one way malicious parties attempt to exploit the vulnerability is to revert back to a version of the unpatched software. Motorola implements a revocation mechanism to block such attempts. When a new software version is released which patches a vulnerability, the security or anti-rollback version of that image is incremented. The device security versions are held in hardware backed OTP memory (OTP fuses and/or RPMB, varies based on product), protecting them from tampering. All signed images have revocation support.

motorola
FOR BUSINESS

HSM BASED CODE SIGNING

The code signing process is only as secure as the signing keys. Without appropriate protection, private signing keys are subject to a variety of threats such as inadvertent publication, rogue employees, or a network/system intrusion. If keys are not generated in an appropriate environment, they may be weak due to improper random numbers or flawed cryptographic algorithms. To mitigate these risks, ThinkShield for Mobile products generate and store keys in a secure signing infrastructure that utilises a Hardware Security Module (HSM). HSM's are designed to securely generate and store keys in a manner where they are never exposed outside of the module and can't be extracted.

ThinkShield for Mobile product code signing utilizes HSM's that are FIPS 140-2 Level 3 and Common Criteria EAL Level 4+ certified. All code signatures are generated by the HSM in an access-controlled way; only approved secure builds are signed. Auditing ensures each signature request is traceable and within signing policy. Each product/product variant uses a new set of keys to reduce the risk of a security vulnerability affecting one product version from affecting another.

ANDROID KEYSTORE & DEVICE ID ATTESTATION

ThinkShield for Mobile products implement a hardware backed keystore that executes as an isolated application in the TEE, independent of the Android OS. The keystore offers robust generation and protection of keys such that they are bound to the device/application and blocked from extraction. It does this by using the SoC encryption hardware and Root Encryption Key. In this way, if the application which owns the keys contains a vulnerability and is exploited, an attacker may be able to use the keys but cannot extract them. Following patching of the vulnerability, the keys remain secure. The keystore receives inputs from the Trusted Boot process as well as authentication modules (e.g., Fingerprint) which control availability and access to the keys. Early in device boot, the Trusted Boot process supplies the secure boot state, software version, and anti-rollback information to the keystore system. If the software version is rolled back or the device is in a non-secure state, the keystore blocks access to the keys. Keys may also be configured to require authentication before use, where the authentication application in the TEE must securely signal the keystore system before the key is available for use.

The Motorola keystore implementation also supports the Device ID Attestation feature, where the device can attest its hardware identifiers (device name, model, manufacturer, serial numbers) to a remote party. This feature increases security for Enterprise use cases such as zero touch. The hardware identifiers are locked into secure memory during the device manufacturing process, when secure attestation key provisioning occurs.

motorola
FOR BUSINESS

FILE ENCRYPTION

The ThinkShield for Mobile file encryption mechanism[3] protects enterprise and user data against a number of advanced threats. File encryption keys are bound uniquely to the device using the keymaster, to protect against offline attacks on encrypted data. However, if the operating system were exploited through a vulnerability, the keys may become compromised. To counter this threat, the encryption keys are never presented to the operating system by the TEE in cleartext form; a wrapped ephemeral key mechanism is used.

The operating system loads the wrapped key to the hardware crypto accelerator using a TEE service. The operating system is blocked from decrypting the wrapped key or extracting it from the hardware accelerator. Enterprise work profiles may use separate authentication, and the work profile is uniquely encrypted from the personal profile. When the work profile is not in use, the encryption key is evicted from the hardware so files can no longer be decrypted. The wrapped key held by the OS is also invalidated, and authentication is required to obtain a new wrapped key before files can be decrypted in the profile. (varies based on device model)

3 Encryption mechanisms may vary by product and chipset

"We applaud Motorola for taking this proactive step to keep its devices secure by certifying an array of its smartphones with our industry-backed standards. Motorola has always built its devices with the consumers' safety in mind and this certification further validates the manufacturer's commitment to security, privacy and transparency, providing an enhanced peace of mind and confidence to end-users."

Brad Ree, ioXt Alliance, CTO.

ioXt alliance

motorola
FOR BUSINESS

SECURITY ENHANCED LINUX EXTENSIONS (SELINUX)

SELinux is an access control mechanism used to enforce security policy on the Android platform. Following the principle of least privilege, it sandboxes Android applications and services, only allowing them to access resources they were intended to access. Should the app or service contain a vulnerability, or attempt to act maliciously, it will be blocked from accessing any resource outside of its sandbox. Access control rules are defined in an SELinux policy. While AOSP provides a reference SELinux policy covering the AOSP system, SoC vendors and OEMs supply the remaining required policy necessary to support the SoC and OEM feature set. Policy writers must be careful to avoid opening security holes by adding overly broad access to resources, executing within an inappropriate domain, including debug/unused policy, etc. Motorola security reviews all vendors' policies to limit risk in these areas. All Motorola defined policy undergoes security and design reviews to ensure security best practice, least privilege, and adherence to the Android architecture. Motorola applications and services execute in isolated domains according to security best practices.

TAMPER PROOF IDENTITY

The device serial number is an identifier expected to be constant and unchangeable for the life of the product. Such identifiers, e.g., International Mobile Equipment Identifier (IMEI), must be protected from tampering following device manufacture. Tampered identifiers may lead to spoofing or cloning, or defeat measures to block the use of stolen goods.

motorola
FOR BUSINESS

During the secure device provisioning process, Motorola assigns device identifiers to a particular device and signs the record uniquely bound to the SoC, using the unique ID burned into the fuses. This prevents the record from being used on any other device except the one it was created for. Signatures are generated using an in-factory HSM with access controls and auditing and may only be requested by authorized test stations. The device validates the signed record on boot and prior to any use, including the binding to the SoC unique ID. If the record does not validate or match the SoC, the modem will not go online and register with the network.

USB PROTECTION

Devices that are lost or stolen are at risk of physical attacks which may be used to exploit the device and gain access to user data. To limit this risk, Motorola blocks any new USB connection on a device with a secure lock screen. This includes Android Debug Bridge (ADB), if it has been enabled by the user. This mitigates the risk of an attacker being able to exploit any vulnerabilities in the USB protocol stack or services utilizing USB, which has the potential to lead to user data compromise.

OS HARDENING

Motorola takes a number of steps to harden the Android OS which includes the underlying board support package and preloaded applications/services. Board support packages as delivered from the component vendors often include drivers, services, and test functionality that increase the attack surface and may introduce product security vulnerabilities. Motorola conducts a security review and removes such unrequired features/functionality from the product.

Preloaded applications also represent a potential risk to the device or user data. Motorola security reviews all preloaded applications/services for security and privacy. We work to eliminate excessive permissions and privilege, unsafe API usage, appropriately protect interfaces, and enforce best security practices such as using https secure connections. This reduces the risk of a privileged preloaded application being used to compromise OS security or user data. In addition to internal security reviews, Motorola periodically engages 3rd party security consultants to review critical security areas in the system and conduct pen-testing. Select products have been formally evaluated in Google's Advanced Assurance Program (AAP) and passed audit meeting or exceeding all requirements.

Motorola has obtained FIPS FIPS 140-2 Level 2 CAVP certification for application-level cryptography using Motorola BoringCrypto Android.

motorola
FOR BUSINESS

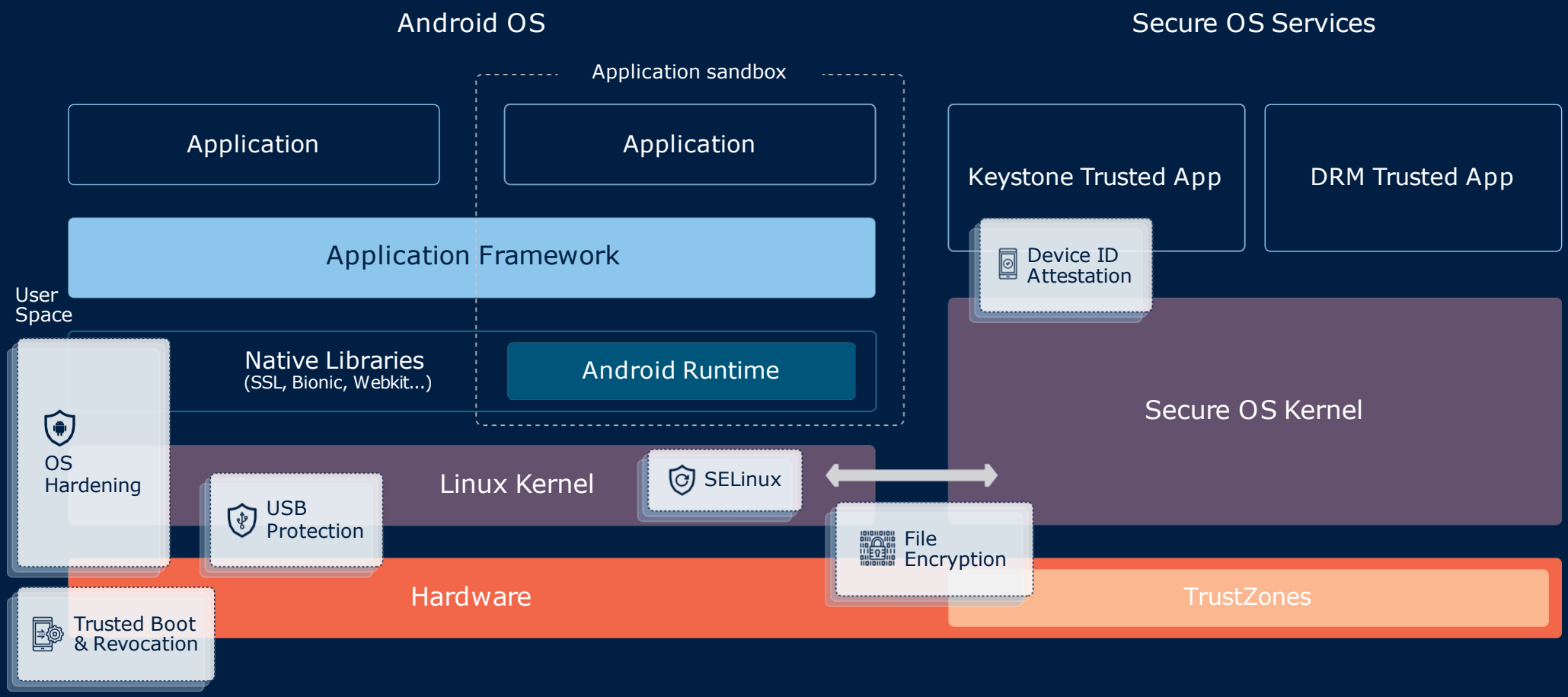


Figure 2. Android security architecture on ARM with TrustZone support

Ref: https://static.googleusercontent.com/media/www.google.co.il/iw/IL/work/android/files/android-for-work-security-white-paper.pdf

motorola
FOR BUSINESS

IN CONCLUSION

With the rise of hybrid work environments, smartphone security has become even more relevant for enterprises. Today, smartphones can access the same type of company information that was traditionally reserved for laptops. As a result, mobile devices account for ~60% of endpoints containing or accessing enterprise data[4]. These devices are always connected and exposed to both attacker and user risks. ThinkShield for mobile provides our devices the business-grade protection that your company needs against today's emerging threats.

4 https://www.zimperium.com/enterprise-mobile-security/

motorola
FOR BUSINESS