KNOX and ARM®TrustZone®

As a device manufacturer, Samsung designs hardware protections that secure your applications and data. These built-in hardware protections ensure KNOX security features are not modified or disabled so those features can continue to protect your data. A critical element of our hardware protections is the TrustZone feature found on ARM-based processors. KNOX uses TrustZone to separate critical software into a Secure World while leaving less sensitive software in the Normal World.

What happens without TrustZone? The keys for encrypting and decrypting sensitive data are managed with software called the KeyStore. Without TrustZone, the KeyStore, along with all other security tools, is stored and managed by the standard Android operating system in Normal World, along with untrusted software. If an attack on the Normal World occurs, a hacker could find their way into secure software, such as the KeyStore, and access the keys protecting your data.

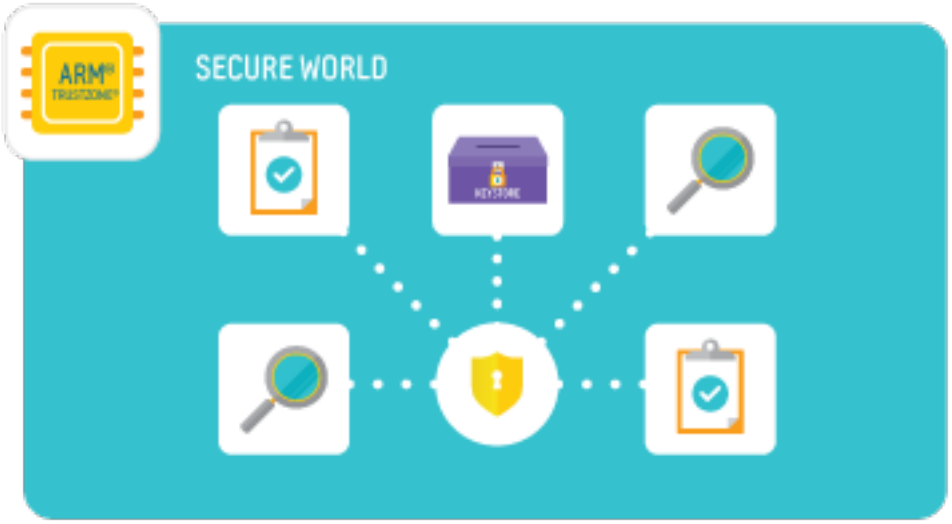
How does KNOX use TrustZone to prevent this attack?

SAMSUNG KNOX

KNOX and ARM®TrustZone®

KNOX uses the secure environment created by ARM®TrustZone® to execute its various security features, because TrustZone runs an OS other than Android. With the protection of TrustZone, the KNOX KeyStore can more securely perform cryptographic operations than Android and safely store the key away from security threats.

Each piece of security software plays a unique role in the protection of device data. See our other KNOX videos for an in depth look at how various KNOX security features work.



SAMSUNG
Knox