CSfC & NIAP CERTIFIED

SECURE MOBILE ENVIRONMENT

A HARDENED MOBILE DEVICE SUPPORTING MULTIPLE CLASSIFIED SECURITY ENCLAVES

MOTOROLA SOLUTIONS

To succeed in today's asymmetrical mission environments, government executives, command leadership, military personnel, and members of the law enforcement and intelligence community, must be able to access and share information with mission partners across the globe. As a result, encrypted voice and data communications in the field are crucial to enabling tactical access to timely information and making more informed decisions in critical moments.

Motorola Solutions' Secure Mobile Environment (SME) is designed specifically to NSA's CSfC standards allowing federal personnel to access classified voice and data from anywhere, at any time, using the LEX L11 smart device.

LEX L11 is a purpose-built device for your agency's most challenging operations. It's a rugged, LTE-based smart device built to military drop and shock standards. It ensures teams receive the right information at the right time while bringing more actionable, real time intelligence directly into the hands of field personnel. It pairs the best-in-class voice and audio capabilities of our mission critical radios with smart device functionality so you can use modern applications, send and receive multimedia, and instantly connect with dedicated push-to-talk functionality.

LEX L11 : FEATURES

- Intuitive Controls for Head Up, Hands Free Operation
- Best-In-Class Audio Quality and Performance
- Push-To-Talk Experience with a Dedicated Button
- End-To-End Mobile Security
- Rugged Construction, Purpose-Built to Outperform Even in the Harshest Environments
- Remote Management and Control with Device Management Wall
- Standard and High-Capacity Battery Options

LEX L11

LEX L11 has been enhanced with accredited software and hardware security components to meet the highest information assurance and integrity standards. Now, federal and military users have an unprecedented opportunity to capitalize on advanced mobile computing and communications in the field.

SECURE MOBILE ENVIRONMENT

ENTERPRISE

GOVERNMENT AND MILITARY IT NETWORK

SECURITY MANAGEMENT

- OTA Device Management
- OTA Key Management
- Define and Manage Security Policies
- Supports OTA Secure Device

NETWORK

- Public Broadband Networks
- Wi-Fi Internet
- FirstNet Band 14
- Private Cellular Networks

SECURE TUNNEL

- Data in Transit Protection With CSfC VPN
- Mandatory Secure Connectivity
- End-to-End Authentication

LEX L11

MISSION CRITICAL BROADBAND DEVICE

ASSURED DEVICE

- Redwall Multiple Modes and Persona's
- Meets Latest Data-at-Rest (DAR) Capabilities Package as defined by the NSA CSS

CSfC HIGHLIGHTS

Motorola Solutions SME leverages the National Security Agency (NSA) cryptography standards that promote the Commercial Solutions for Classified (CSfC) protection profiles for secure sharing of classified information over wireless mobile networks. It specifies a common suite of public standards, protocols, algorithms and modes to meet stringent NSA directives for classified information up to TOP SECRET level.

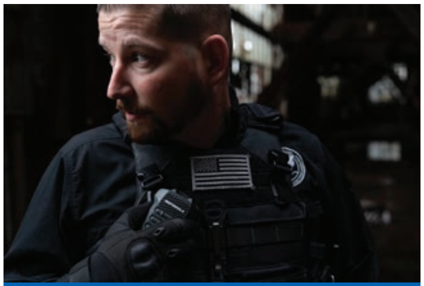
ADDITIONAL ELEMENTS OF SECURE MOBILE ENVIRONMENT

- Supports but is not limited to AES-256, ECDSA, ECDH, SHA-256, SHA-384
- Supports any CSfC Approved VPNs without modification to the device build
- End-to-End Encrypted Voice, Video and Messaging packets
- Security Enhanced OS with Modes Capability

ENABLING A GLOBAL FEDERAL WORKFORCE

Federal missions, operations and personal logistics are constantly changing. Motorola Solutions believes federal agencies need flexible, secure and scalable mobility solutions that enable the exchange of classified and sensitive information between disparate user groups. From military personnel to law enforcement officers to the broader federal workforce, the operation of government requires access to classified or sensitive information. SME streamlines these operations by enabling secure, mobile access to information, across multiple security domains, from a single device.

SECURE ACCESS TO CRITICAL INFORMATION & COMMUNICATIONS



WARFIGHTER SPECIAL OPERATIONS COVERT PERSONNEL

Securely access sensitive/ classified data from garrison to battlefield

INTELLIGENCE COMMUNITY LAW ENFORCEMENT FIRST RESPONDERS

Securely share information and collaborate among teams

The focus on COTS-based high assurance mobile security solutions allows Motorola to deliver both classified and unclassified protection in a single COTS homogeneous system (clear up to TS). As a trusted integrator, Motorola is dedicated to leveraging enhanced software security feature sets to extend classified-enabled communications capabilities to federal overt and covert personnel running on a purpose-built, mission-critical handheld LTE device supporting CONUS or OCONUS coverage needs.

FEDERAL BENEFITS

NSA's Commercial Solutions for Classified (CSfC) Program "enables commercial products to be used in layers protecting classified National Security System data." The CSfC Program provides the ability to securely communicate based on commercial standards in solutions that can be fielded in months, not years, ensuring users are equipped with devices at the cutting edge.

- Hardened Device
- Protecting Data at Rest and In Transit
- End-to-End Encrypted Voice, Video and Messaging packets
- Control, Manage and Enforce Mobile Security Policies

DEFENSE IN DEPTH

PROTECTING INFORMATION AT REST AND IN TRANSIT

The LEX L11 meets all defined DAR requirements in the latest NSA CSS Capabilities Package and the MDFPP, then goes further. It contains features that are novel enough to merit an NSA Innovations BAA to study the technology's ability to strongly separate multiple personas or security levels on-device, while resisting first-world forensics. The team that developed our DAR solution has extensive expertise in offensive key extraction and designed new defenses for the LEX L11 with that experience in mind, adding an additional layer on top of what CSfC requires, with no performance overhead.

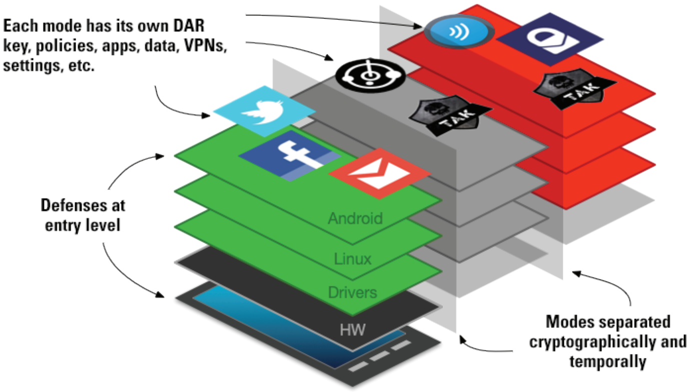
The LEX L11 has a unique feature that allows for authenticated and cryptographically signed trusted daemons and privileged system services without modifying the firmware. These become part of the system's boot and run-time integrity checks. This allows support for multiple VPN applications, while controlling VPN state, IP tables, geofences, and more. All from a signed security policy that is compatible with any commercial EMM, without requiring one. In this way, the LEX L11 is not tied to a single VPN solution or management platform. It can be easily updated without an OTA or reflash, but still offers the same level of assurance as if the VPN services were baked into the firmware.

KEY BENEFITS OF SME

- Ease-of-use: Enables a user-friendly experience. The enhanced security features are transparent to the user. Interface enhancements provide visual cues to help users identify the security status in which they are operating.
- Encrypted voice and messaging: Enables AES-256, VoIP and messaging communications to other SME-enabled devices. Supporting the NSA's CSfC protection profiles.
- Secure data: Provides access to a protected enclave through integrated AES-256, IPsec VPN, and Data at Rest protection. Supports many 3rd party applications for situational awareness, realtime video, and email.
- Security control: Lets you define and control security policies from the secure enclave; delivers Over-the-Air support for key management and device management.
- End-to end integrated solution: Leverages commercially available 3rd party vendors' security products and applications as part of the SME ecosystem, delivering a complete end-to-end solution for secure mobility.
- Built-in firewall: Allows for real-time configuration of kernel-level packet firewall (IPv4 and IPv6)

CONTROL, MANAGE AND ENFORCE MOBILE SECURITY.

All of the functions of the SME Solution operate without any connectivity, EMM/MDM, or any proprietary tools or services. While the LEX L11 is compatible with CSfC approved Android MDMs, none are required to sign or manage the devices. All policies and files, as well as device wiping and more, may be managed remotely over email, MMS, in the device's Web browser, and a myriad of other ways, or locally via microSD cards or USB. No special software is required.



Each mode has its own DAR key, policies, apps, data, VPNs, settings, etc.

Defenses at entry level

Modes separated cryptographically and temporally

UNIQUE MULTI-MODE TECHNOLOGY

This architecture allows for a unique method of providing multiple operational modes on the device. Each mode has its own authentication, data, policies and apps. Unlike multiple accounts, hypervisors, or TrustZone-based systems, modes are never co-resident in memory nor executing simultaneously. Multiple security levels may safely run on a single device, and even an operating system, baseband, or processor-level exploit cannot cross the boundary between modes.

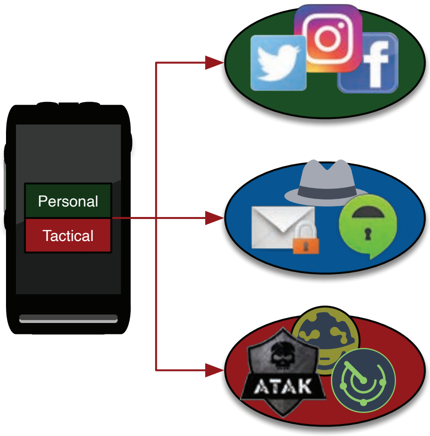
GMS AND APP COMPATIBILITY

The SME's Google Mobile Services provide a richer and more complete Android experience, and gives the user access to millions of apps. But for those times when you need to lock down a mode or even the entire device, modes can also selectively be GMS or non-GMS. Disabling GMS results not only in a more "vanilla" or AOSP-like mode, but it goes much further to remove Google keyboards, browsers, time servers, SE policy, remote font usage by apps, and dozens more deeply embedded APIs. It also removes the steady stream of marketing, location, ID, and analytics data which GMS devices sends to Google, who subsequently sells that data to third parties. And while side-loading and downloading apps can be disabled along with the Play Store, properly signed APK files ranging from ATAK to WAVE PTT install and work without the need to re-compile, use any particular API, special app store, or whitelists and blacklists (unless desired).

Any combination of modes and policies is possible. One mode could be zero-emit (all radios off, even BLE), and accessed only via a non-obvious trigger operation. Another could allow LTE data, but disable SMS and LTE voice calling outside a geofence. Modes and policies can be managed by Motorola, or by the end user, in a flexible and intuitive manner enabling custom ROMs without the typical cost of customization.

POLICIES

A simple JSON file defines the modes and policies for each mode, and allows an admin to enable and disable not only GMS, but every feature and function of the phone on a per-mode basis, as shown in the example. The policies control low-level features such as individual system calls, baseband functions, and IP firewall settings, as well as high-level functions like VPN geofences, cameras, and radios such as Bluetooth. When the LEX L11 disables a feature, it does much more than the Android (or iOS) APIs could; drivers for disabled features are not loaded and access - even by the kernel - is blocked, disabled chipsets are not initialized, and not even an exploit could enable the feature.



MOTOROLA SOLUTIONS

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, Il 60661 U.S.A. **motorolasolutions.com**