THE ASSURED MOBILE ENVIRONMENT

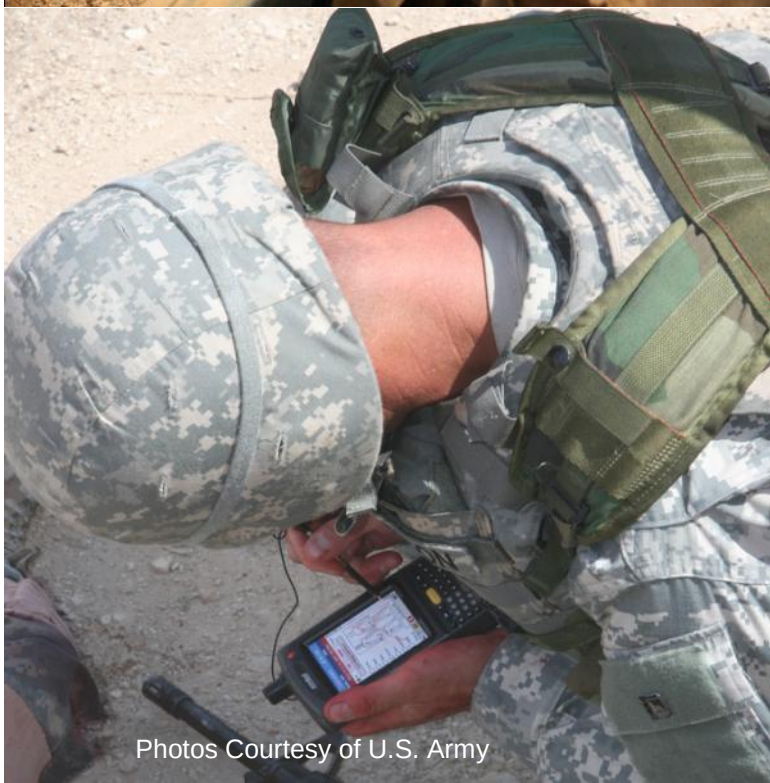
Randy Siegel
Director
U.S. Federal Government Markets Division
Motorola Solutions
Randy.Siegel@motorolasolutions.com

Photo courtesy of U.S. Army
Inset photo courtesy of Cpl. Ryan Tomlinson

AGENDA

- Introduction
- Solution Overview
- Solution Components
- Implementation
- Conclusion


Photo Courtesy of Cpl. Ryan Tomlinson


Photos Courtesy of U.S. Army

THE NEED IS REAL

Traditional high assurance solutions are lacking for contemporary defense communications applications

*"[Commercial Mobile Devices] CMD (e.g. smartphones, e-readers, tablets, etc.) offer unprecedented opportunities for advanced mobile computing and communications." **

*"The increasing use of social media, smartphones and tablet computers has made information sharing an expectation. This expectation requires new capabilities, particularly in the "edge" or tactical environments that have limited availability to persistent, high speed connections." **

Contemporary Commercial Off the Shelf (COTS) Devices are not secure

*"The Defense IA Security Accreditation Working Group (DSAWAG), which adjudicates community risk and approves Security Technical Implementation Guides (STIGs), recently reviewed a CMD Operating System and determined these devices are not yet suitable for wide-scale DoD deployment." **

**Use of Commercial Mobile Devices (CMD) in the Department of Defense (DoD)*
T. M. Takai, DoD CIO April 06, 2011

THE THREAT IS REAL

Mobile phones are the primary communications device for many

- Especially true for high ranking officials and executives

Vulnerabilities to mobile phones are increasing

- *Practical Cellphone Spying*, (DEFCON 18, Jul 30 - Aug 1, 2010), http://defcon.org/html/links/dc-archives/dc-18-archive.html
- Live demonstration of GSM phone call interception for <$1500

Technology for adversaries is ever more readily available

- *Secret Mobile Phone Codes Cracked: A German computer scientist has published details of the secret code used to protect the conversations of more than 4bn mobile phone users.* (BBC News Dec-09)

Monday, January 31, 2011

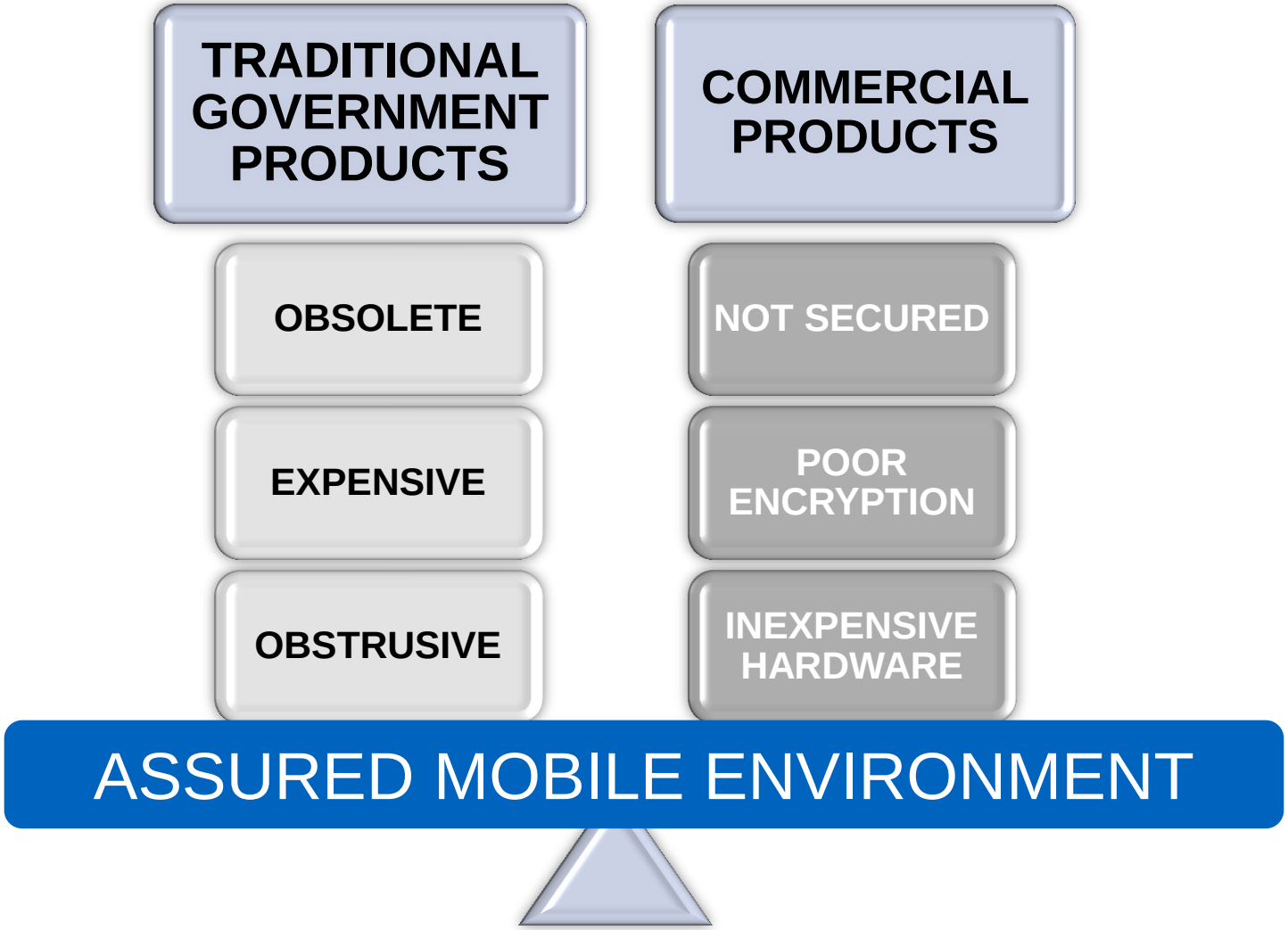
The Cell Phone Security Threat

The majority of large and medium businesses are failing to adequately protect themselves against the growing threat of mobile voice call interception;…

"Effective email security has become routine but our research shows most businesses do not apply anything like the same level of robust security to cell phone calls. Companies that do not respond are exposing themselves to attack."

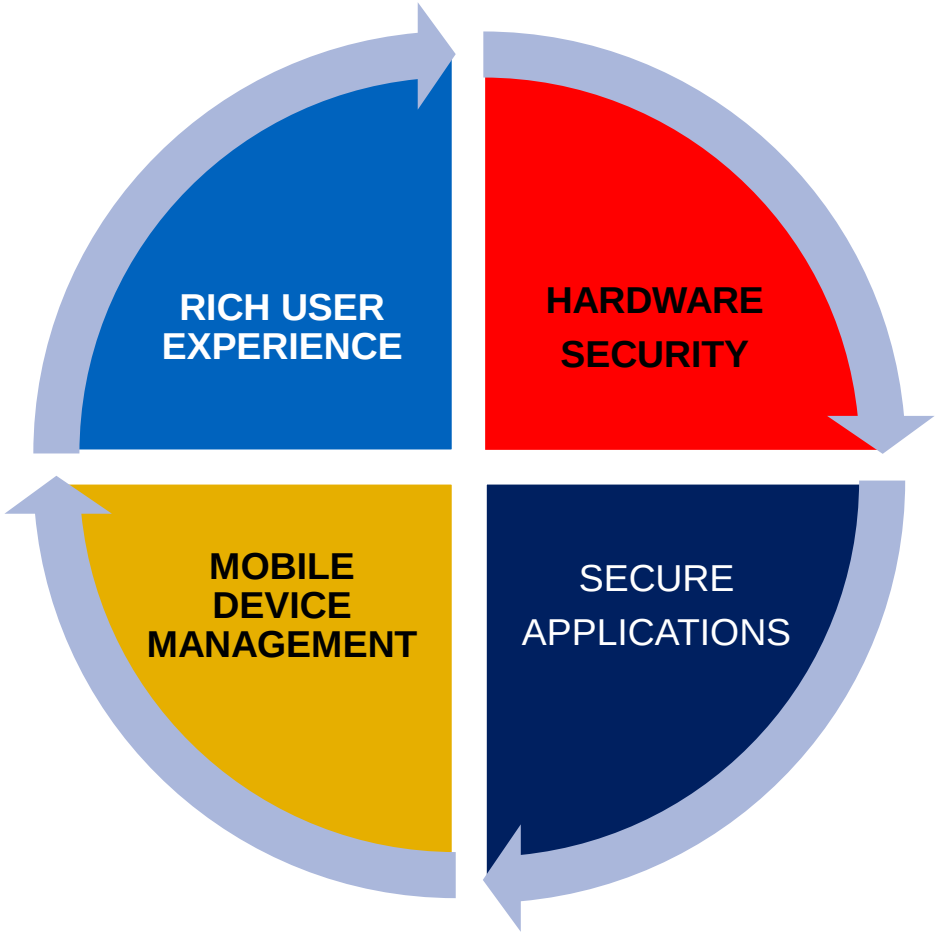
Source: ABI Research

FINDING THE BALANCE



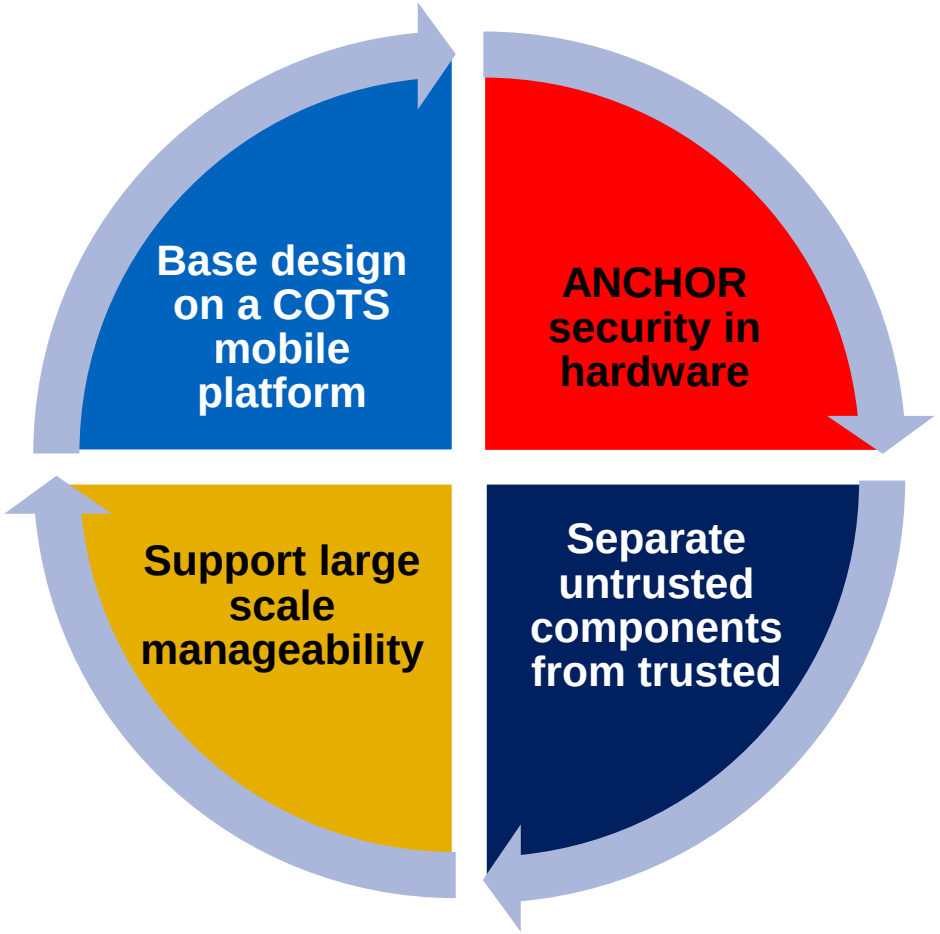
ASSURED MOBILE ENVIRONMENT

A COMPLETE SOLUTION



ASSURED MOBILE ENVIRONMENT

FOUR FOUNDATIONAL TENETS

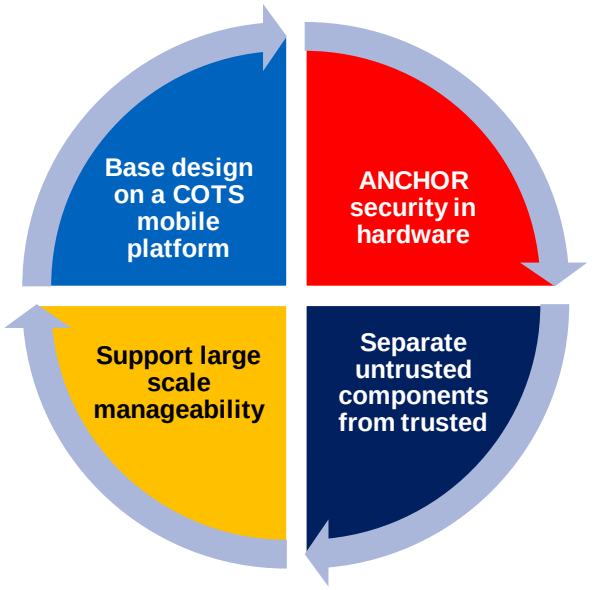


2010 FEASIBILITY STUDY

Is there an optimal commercial platform or OS?

Is it feasible to implement a high assurance Suite B crypto-processor in a micro SD format?

Which commercial platform or OS offers the richest user experience?



Is it feasible for the module to be non-CCI?

Can PKI be used effectively in spite of the potential size of a mobile network?

Can the OS be trusted to keep applications separated and protect I/O streams?

Can mobile devices be securely managed from a control center in the network?

Is virtualization needed? What is the optimal virtualization technology?

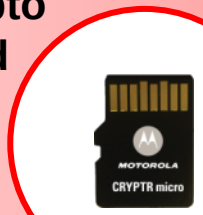
ASSURED MOBILE ENVIRONMENT

Not Just an Encryption Module or Application Software!

Commercial platform agnostic

Base design on a COTS mobile platform

Micro SD Crypto Processor and keystore



ANCHOR security in hardware

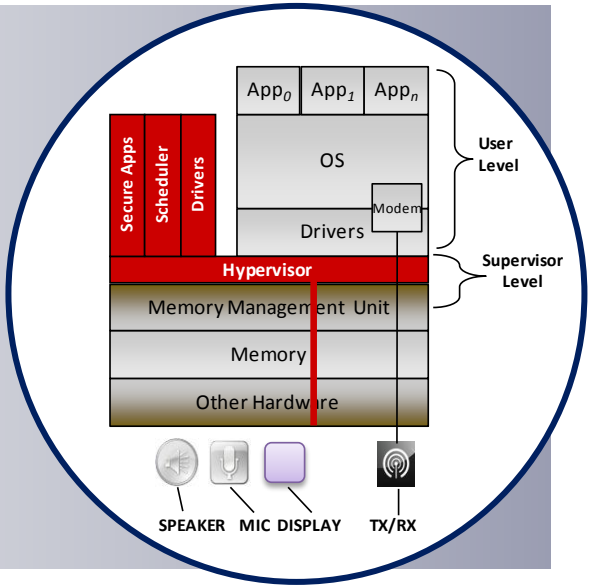
Support large scale manageability

Standards based protocols and APIs

Remotely Manageable

Separate untrusted components from trusted

Bare-metal hypervisor



ASSURED MOBILE ENVIRONMENT

DRIVING THE REQUIREMENTS

Functionality:

- ✓ *Secure VoIP Phone Calls*
- ✓ *Secure Data Connectivity*
- ✓ *Secure Voice and Email Apps*
- ✓ *Security API for Customer Apps*
- ✓ *Support for Non-Secure Voice and Apps*
- ✓ *Secure Device Management*

One Phone – Two Domains

Primary Security Considerations:

- ✓ *Software Integrity*
- ✓ *Fail-Safe Design – Virtualized Process Separation*
- ✓ *Design Assurance – Security Critical Components Evaluated*
- ✓ *Physical Security –*
  Tamper-Resistant Key and Algorithm Storage
  Environmental Exception Detectors
- ✓ *Secure Key Management*

Environment:

- ✓ *Latest COTS Devices*
- ✓ *COTS-like Product Cost*
- ✓ *Open Platform for Secure Applications*
- ✓ *High Assurance Crypto*

ASSURED MOBILE ENVIRONMENT

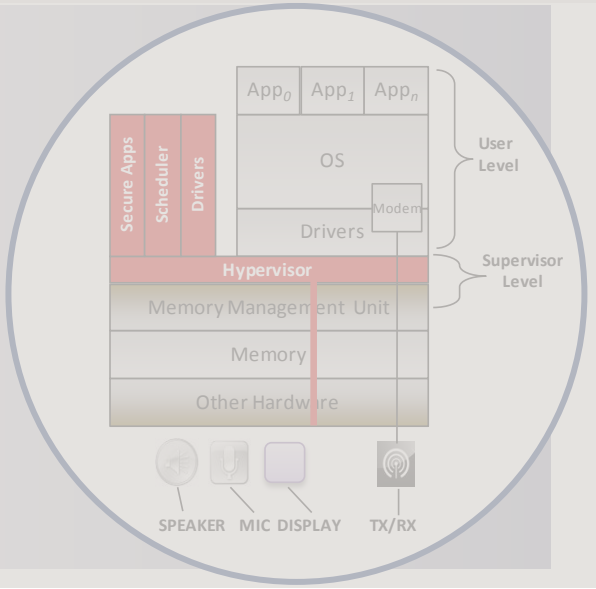
Commercial platform agnostic

Base design on a COTS mobile platform

Micro SD Crypto Processor and keystore

ANCHOR security in hardware

Separate untrusted components from trusted



Bare-metal hypervisor

Support large scale manageability

Standards based protocols and APIs

Remotely Manageable

ENTERPRISE GRADE DEVICES

- **Windows Mobile**
- **Biometric Reader, GPS**
- **CDMA plus GSM in one device**
- **IP42, MIL810G**
- **Extended lifecycle support**

KNOWLEDGE USER
Secure Voice and Data Mobility

- **Enhanced Android™ OS**
- **Extended accessory ecosystem**
- **IP54 sealed, MIL810G**
- **Replaceable battery**
- **Extended lifecycle support**

TASK ORIENTED USERS
Secure Application Access

ASSURED MOBILE ENVIRONMENT

Commercial platform agnostic

Base design on a COTS mobile platform

Micro SD Crypto Processor and keystore

ANCHOR security in hardware

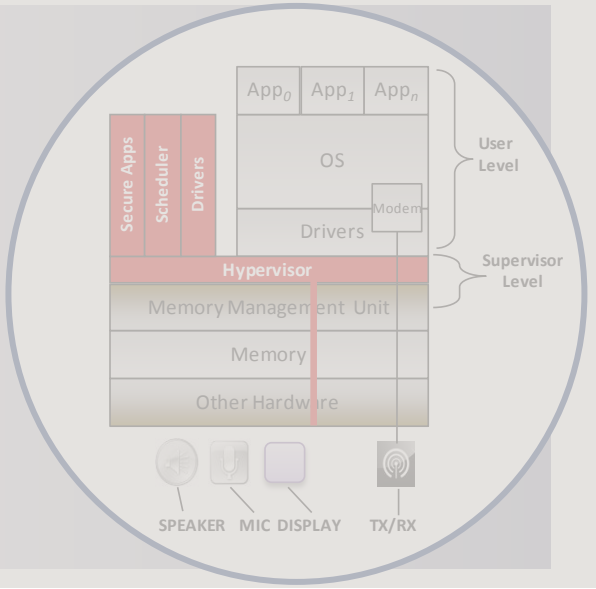
Support large scale manageability

Standards based protocols and APIs

Remotely Manageable

Separate untrusted components from trusted

Bare-metal hypervisor



CRYPTR micro OVERVIEW

Micro-SD Form Factor

- Designed for use in Commercial-off-the-Shelf Smartphones

Hardware Based Security

- Tamper Protection
- Supports Encryption & Key Management
- Secure Credential Store
- Hardware based Random Number Generation (RNG)

FIPS 140-2 and Suite B Cryptography

- FIPS 140 Planned Complete 4Q11
- Designed with high assurance requirements in mind

CRYPTR micro CAPABILITIES

Capabilities

- Encipher/decipher – symmetric
- Encipher/decipher – asymmetric
- Cryptographic Enveloping
- Sign data/verify signatures
- X.509v3 Certificate and key pair storage
- Key Generation
- X.509v3 Certificate and Key Pair Update
- X.509v3 Certificate Validation
- Random Number Generation
- Key Establishment Operations
- Key Derivation
- Hashing and HMAC

CRYPTR micro MANAGEMENT

Certificate/Key Management

- Generates and stores a device-unique signed X.509v3 Elliptic-Curve certificate.
- No private key import functionality.
- Validates another device's unique public key during an authentication process
- Supports import of the root CA certificate
- Supports export of the public key for certification
- Supports importing of device-unique certificate
- Supports certificate revocation.

CRYPTR micro ACCESS

Policy Management

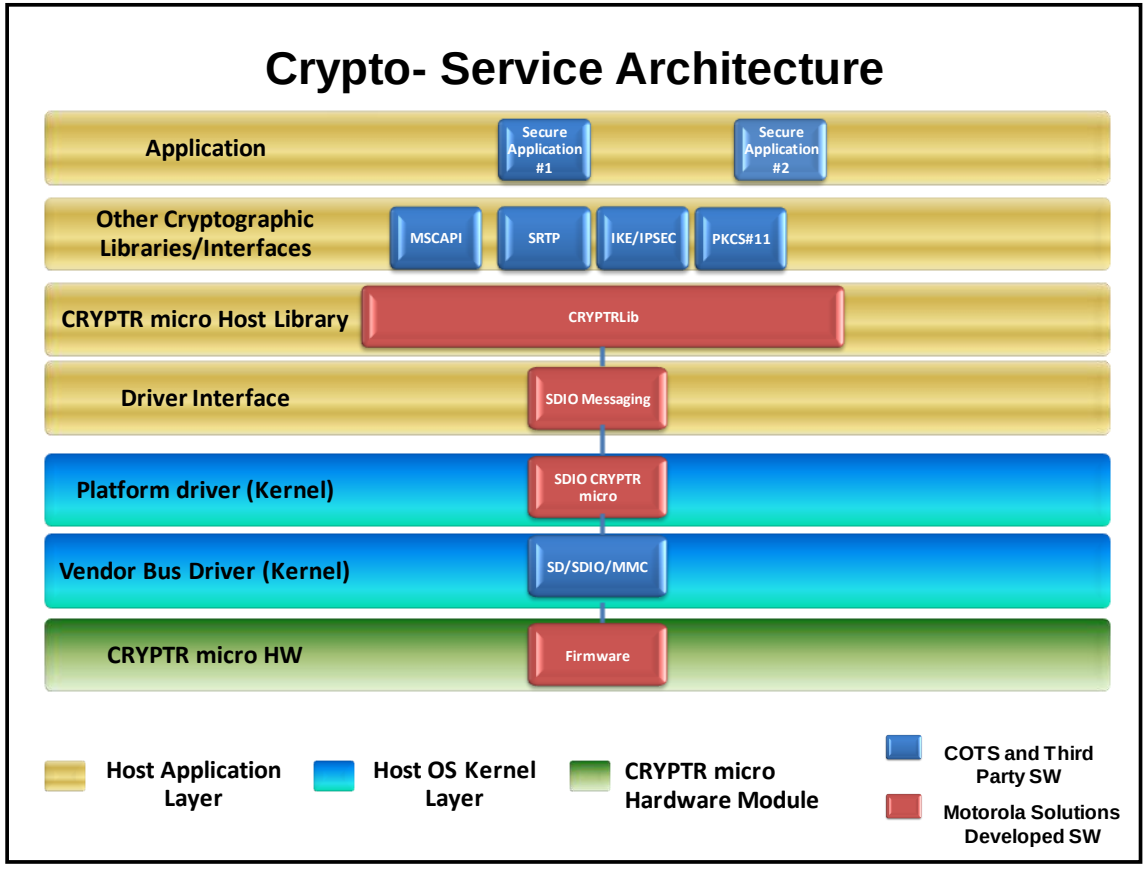
- Policy is enforced through configuration of the CRYPTR micro
- All configuration data stored in the CRYPTR micro is stored in a single database under an administrator password
- The privileges are not configurable by either the user or the administrator

PIN/Token

- Administrator access is allowed via an external host connected through the SDIO interface (factory device, Smartphone)
- The CRYPTR micro has one Administrator and one User account with configurable passwords.
- Strong passwords are enforced

CRYPTR micro EMBEDMENT

- The software stack exposes the CRYPTR micro's functions and services through a crypto library API.
- Usable directly with little change to applications currently using industry standard APIs and toolkits.



ASSURED MOBILE ENVIRONMENT

Commercial platform agnostic

Base design on a COTS mobile platform

Micro SD Crypto Processor and keystore

ANCHOR security in hardware

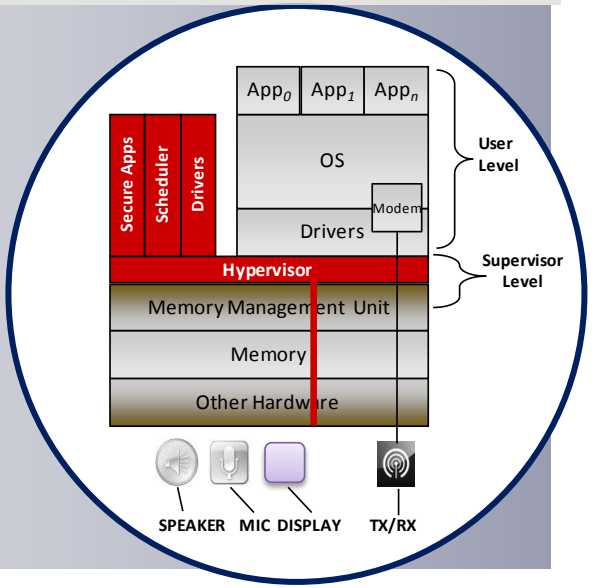
Support large scale manageability

Standards based protocols and APIs

Remotely Manageable

Separate untrusted components from trusted

Bare-metal hypervisor



AME HYPERVISOR

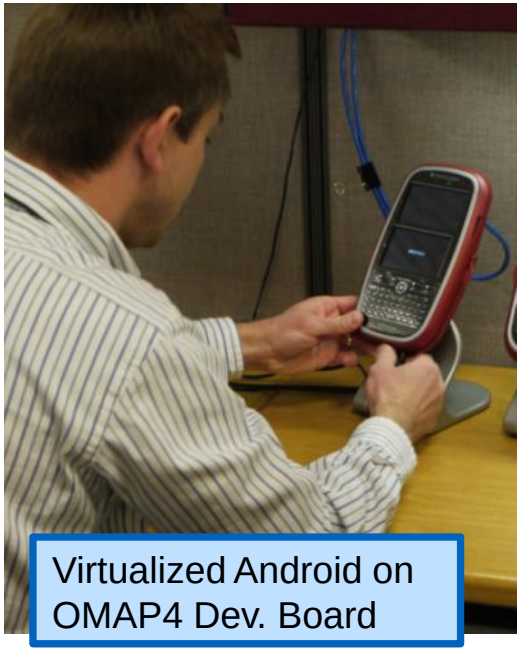
DOMAIN SEPARATION

Separates untrusted components from trusted ones.

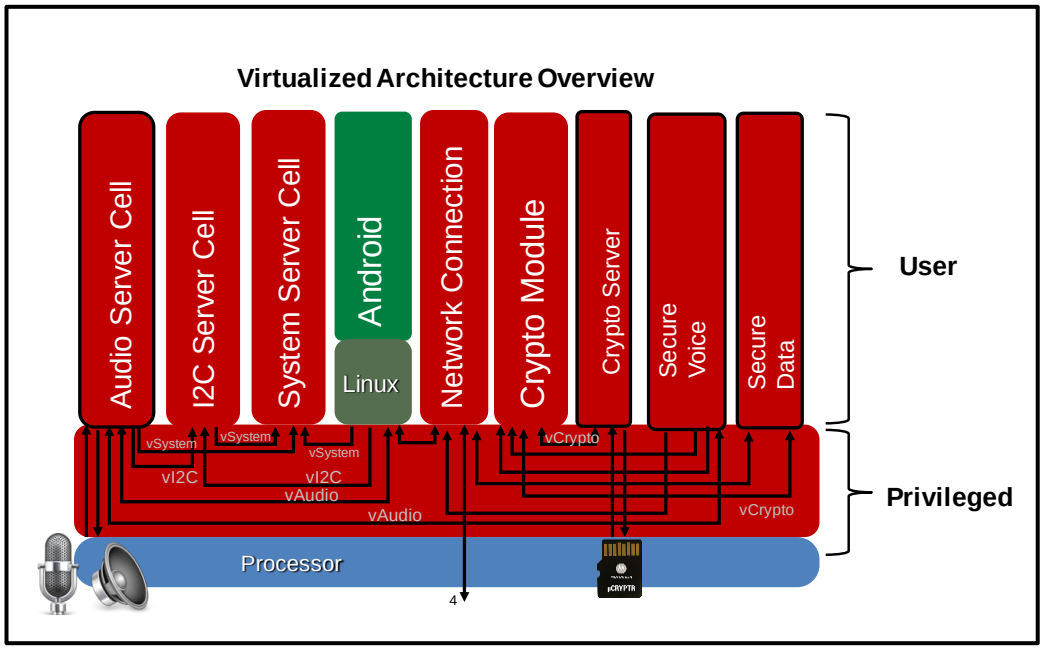
The hypervisor is proven to work on several ARM processors.

The hypervisor is small, (about 80Kbytes) making it amiable to analysis.

Based on academic work focused on a provable security model.



Virtualized Android on OMAP4 Dev. Board

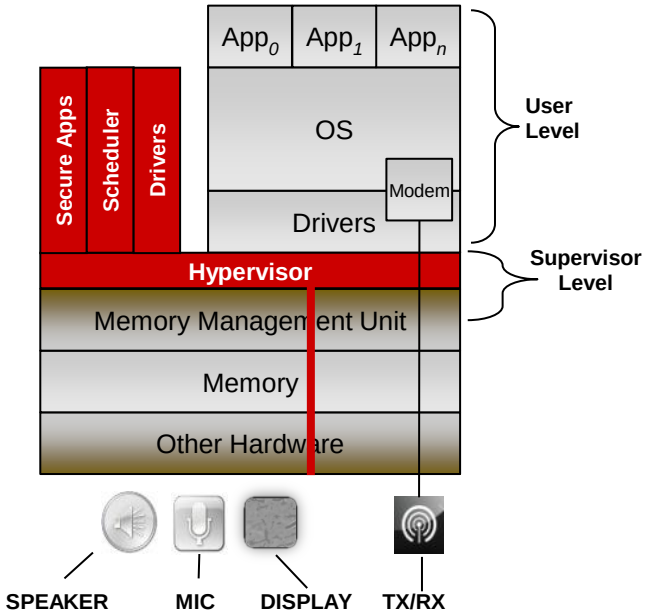


Trusted Computing Base TCB

ASSURED MOBILE ENVIRONMENT

Motorola Solutions' Secure Mobile Architecture

- **Virtualization solution ("Hypervisor") separates the OS from hardware to enable a trusted COTS device for secure applications**
  - Isolates red and black cells-- applications environments
  - Controls access to peripherals
- **CRYPTR micro Crypto engine provides trusted crypto operation and key storage**
  - Secure key handling methods
  - Data at rest protection provisions
  - Real-time integrity checking & tamper protection



CRYPTR micro Module

ASSURED MOBILE ENVIRONMENT

Commercial platform agnostic

Base design on a COTS mobile platform

Micro SD Crypto Processor and keystore

ANCHOR security in hardware

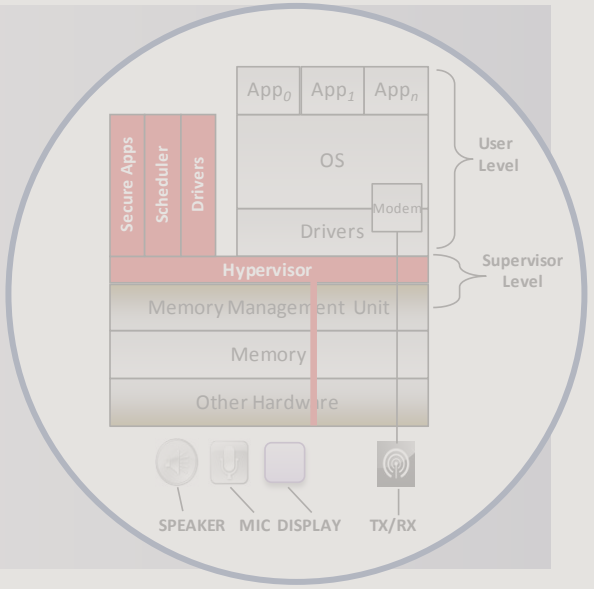
Support large scale manageability

Standards based protocols and APIs

Remotely Manageable

Separate untrusted components from trusted

Bare-metal hypervisor



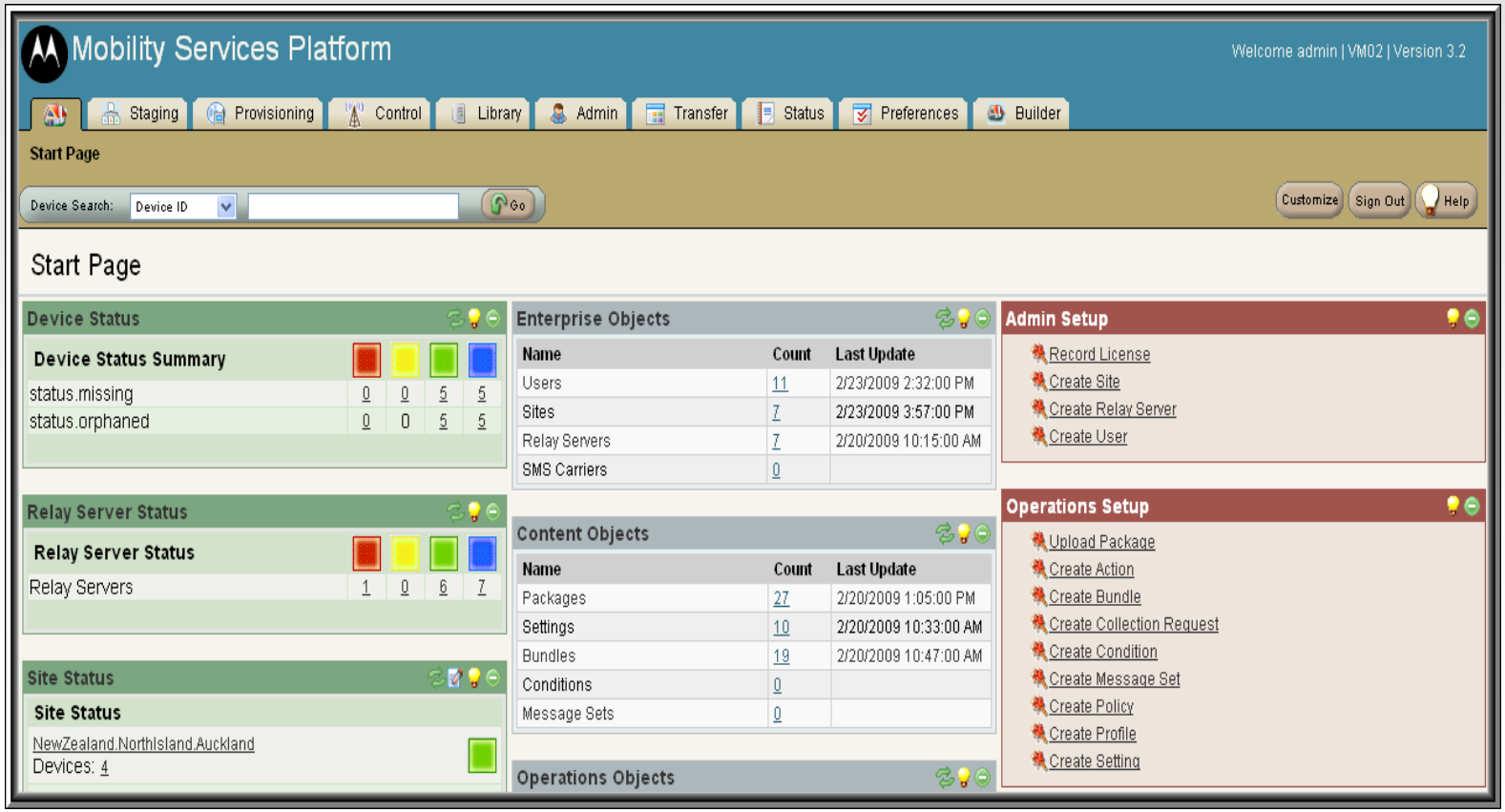
AME DEVICE MANAGEMENT

Mobility Services Platform v3

AME DEVICE MANAGEMENT

Designed for easy navigation and workflow

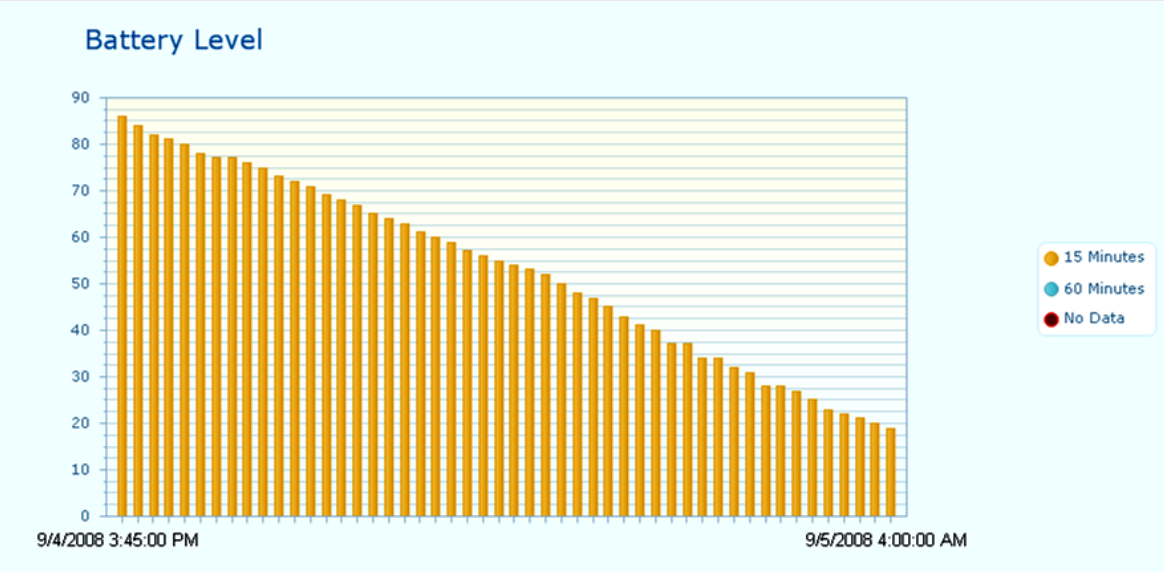
Wizard-like tools help answer: “What’s the next logical step in the workflow?”



AME DEVICE MANAGEMENT

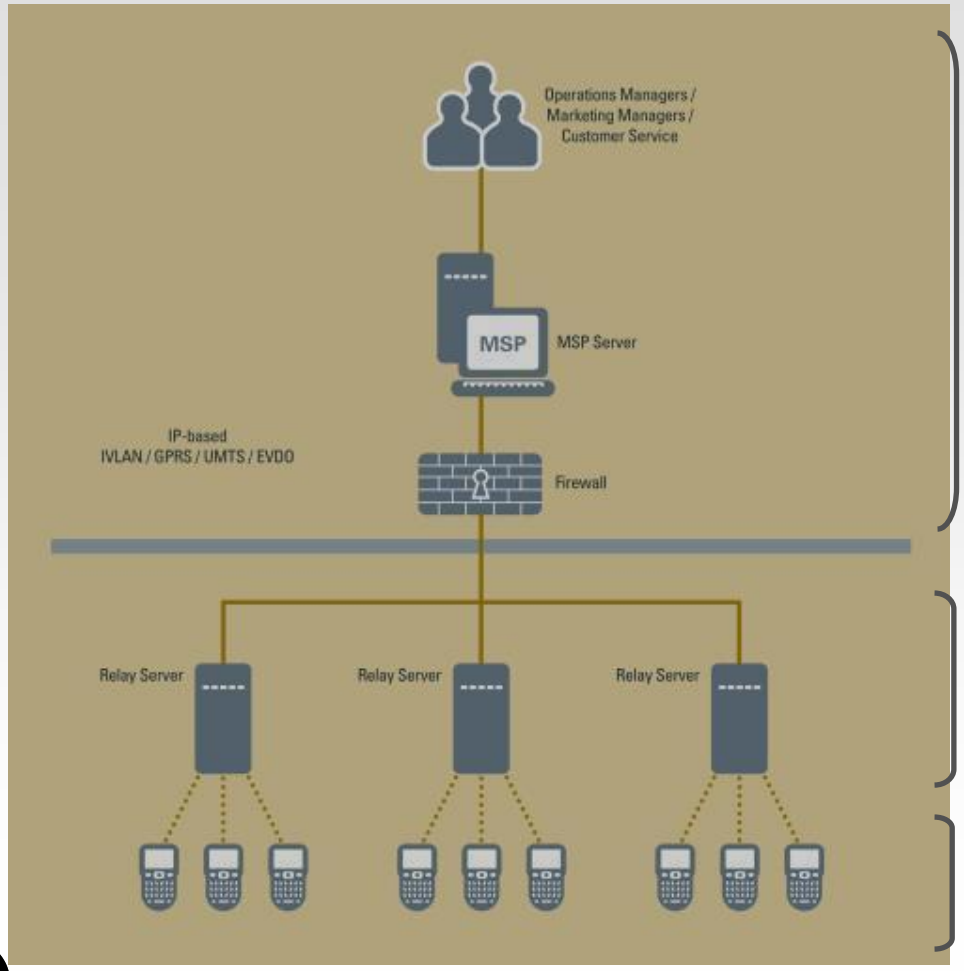
CONTROL

Proactive management and optimization allows IT to identify potential application, network or device issues — before your users are affected



AME DEVICE MANAGEMENT

POWERFUL AND SIMPLE IT ARCHITECTURE

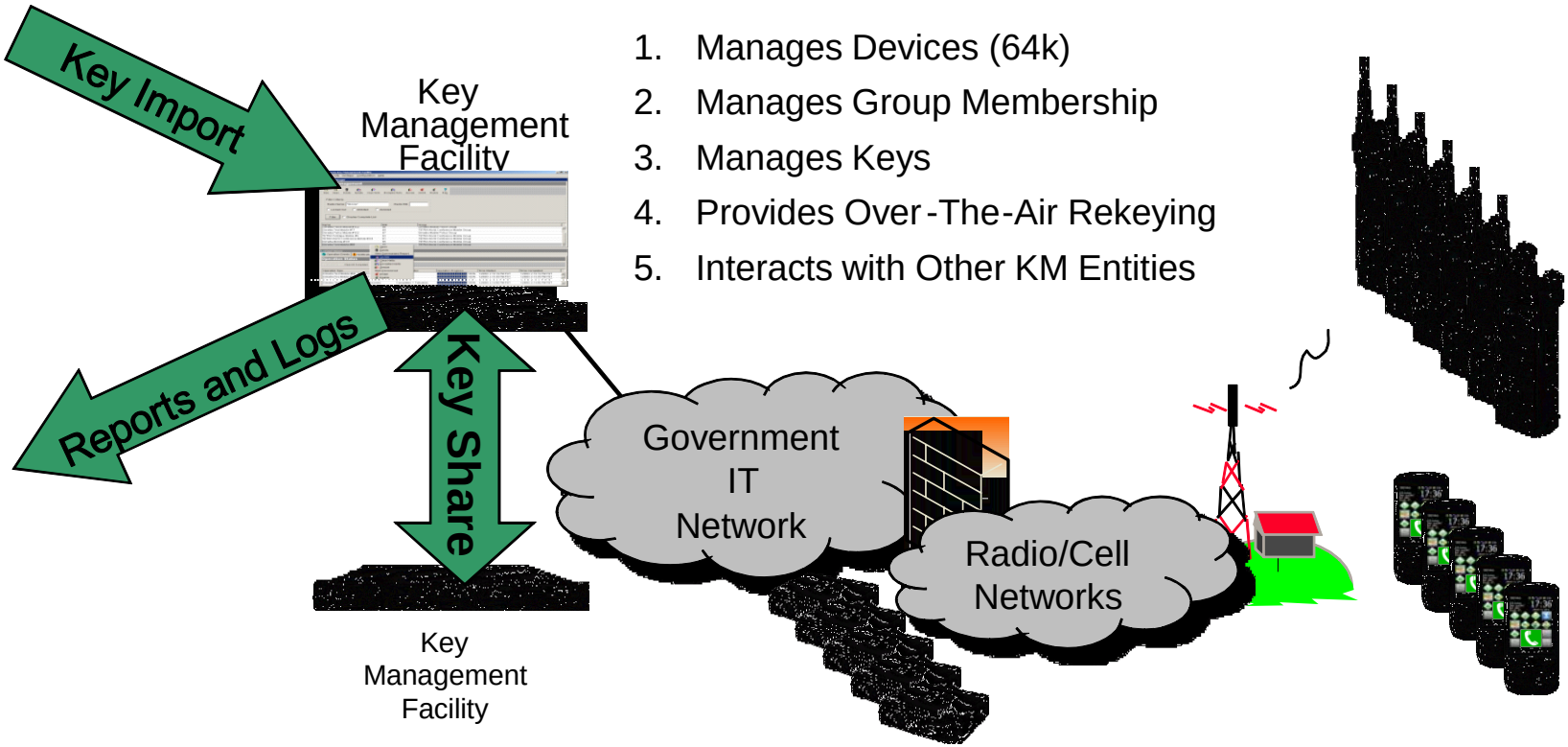


Distributed 3-tier architecture offloads processing to Relay Server — ideal for large distributed environments

Single point of management — one server to maintain and manage

KEY MANAGEMENT SYSTEM

PROVEN CAPABILITY



1. Manages Devices (64k)
2. Manages Group Membership
3. Manages Keys
4. Provides Over-The-Air Rekeying
5. Interacts with Other KM Entities

AME SOLUTION

IMPLEMENTATION

- Demos with CRYPTR micro
- Analyis
- Whitepaper

- Voice Only
- Windows Mobile 6.5 + CRYPTR micro

- Voice, Data, Apps
- Android + Hypervisor + CRYPTR micro

Feasibility Study | **AME Secure Voice** | **ANDROID AME**

2010 ***2011*** ***2012***

AME SECURE VOICE

ES400 Enterprise Digital Assistant	CRYPTR micro Crypto Module	Apriva Voice
• A modern, secure, commercial smartphone • GSM + CDMA World-phone. • Windows Mobile 6.5.3	• Hardware based cryptography • FIPS140-2 and Suite B capable	• VoIP over Packet Data • SCIP and DTLS/SRTP • Interoperable with existing SCIP secure devices & terminals

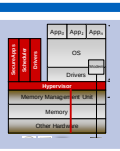
ANDROID AME

Android Devices

Secure VOIP

Secure Applications

CRYPTR micro Library



AME Hypervisor

CRYPTR micro

MEETING THE REQUIREMENTS

COMMERCIAL MOBILE DEVICES REQUIREMENTS*	ASSURED MOBILE ENVIRONMENT
ACCESS CONTROL	
• DoD approved identification and authentication to the mobile is required • CMDs should employ approved user credentials to authenticate to DoD web servers, collaboration tools and data files.	✓CRYPTR micro hardware based user identification / authentication. ✓Standard CRYPTR micro API allows authenticated users to make use of trusted applications and secure web access.
DATA PROTECTION	
•All sensitive DoD data both in transit and at rest is required to be encrypted using a FIPS validated module. •Decryption requires successful entry of a password. •When a screen lock occurs (user initiated or due to inactivity timeout) all data will be re-encrypted. •The system administrator shall have Remote Data protection capability though the use of a Data Wipe or Data Obfuscation command to the handheld.	✓ Cryptography and key storage supplied by CRYPTR micro hardware. ✓ Hardware based password protection of all cryptographic services. ✓ Trusted User Interface and data management applications. ✓ Data storage protected by the hypervisor. ✓ MSP3 provides full remote management capability.

**Use of Commerical Mobile Devices (CMD) in the Department of Defense (DoD) T. M. Takai, DoD CIO April 06, 2011*

MEETING THE REQUIREMENTS

COMMERCIAL MOBILE DEVICES REQUIREMENTS*	ASSURED MOBILE ENVIRONMENT
ENTERPRISE MANAGEMENT	
•Devices must be managed and controlled by an enterprise management system. This includes capability to configure the device browser during provisioning; capability of performing a device audit. •Devices must prevent user override of security configurations.	✓ Base security policy on the CRYPTR micro set at the factory and can not be changed. ✓ Mobile device policies set and managed remotely by MSP3 ✓ Hypervisor prevents unauthorized user access.
DoD PUBLIC KEY INFRASTRUCTURE (PKI) CREDENTIALS	
• Devices must implement DoD PKI standards or approved authentication credentials. • Email on CMDs will be capable of using public key enabled digital certificates for authentication between devices and the server.	✓CRYPTR micro can store credentials and act as an embedded CAC. ✓Standard CRYPTR micro API allows authenticated users to make use of approved email applications.

**Use of Commerical Mobile Devices (CMD) in the Department of Defense (DoD) T. M. Takai, DoD CIO April 06, 2011*

MEETING THE REQUIREMENTS

COMMERCIAL MOBILE DEVICES REQUIREMENTS*	ASSURED MOBILE ENVIRONMENT
SOFTWARE APPLICATIONS	
•Software and applications must be installed from an approved source •A trusted loading process including Over The Air (OTA) provisioning must include mutual authentication, data confidentiality, integrity and availability between the provisioning server and device.	✓Hardware based signature validation ✓Hypervisor protects trusted load process ✓Standard CRYPTR micro API allows full hardware based cryptographic services to be used by a trusted load application
TRAINING	
• The rapid evolution of new CMDs and the current dependence on user-based security controls introduces risks to the environment requiring more robust system administrator and user training and awareness.	✓Commercial based technology leverages the advanced intuitive UI capabilities of Android , thus streamlining training and awareness

**Use of Commerical Mobile Devices (CMD) in the Department of Defense (DoD) T. M. Takai, DoD CIO April 06, 2011*

ASSURED MOBILE ENVIRONMENT

Commercial platform agnosti

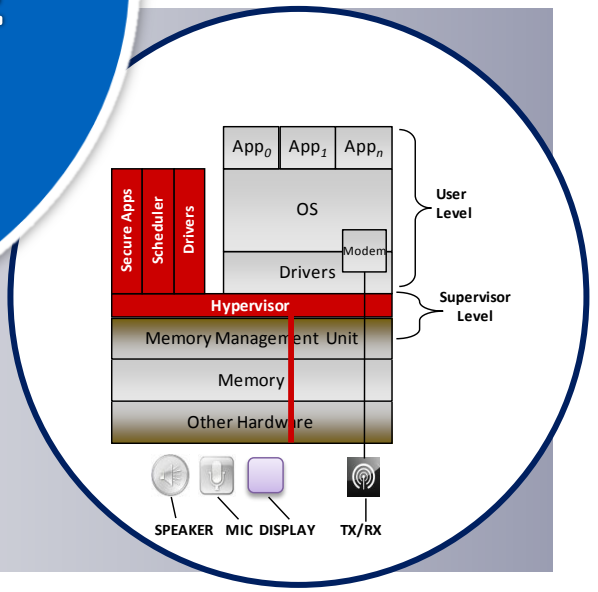
Micro SD Crypto
cessor and

LEADING EDGE SOLUTIONS FOR SECURE MOBILE COMMUNICATIONS

Sta
based
protocols and
APIs

Remotely Manageable

Bare-metal hypervisor



THANK YOU