

UNCLASSIFIED



**SAMSUNG KNOX ANDROID 1.0  
SECURITY TECHNICAL IMPLEMENTATION GUIDE  
(STIG)  
OVERVIEW**

Version 1, Release 1

3 May 2013

**Developed by Samsung Electronics Co., Ltd.; Fixmo, Inc.;  
and General Dynamics C4 Systems, Inc. (GDC4S) in  
coordination with DISA for the DoD**

UNCLASSIFIED

### **Trademark Information**

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by DISA FSO or any non-Federal entity, event, product, service, or enterprise.

**TABLE OF CONTENTS**

	<b>Page</b>
<b>1. INTRODUCTION.....</b>	<b>1</b>
1.1 Background .....	1
1.2 Authority .....	1
1.3 Scope .....	1
1.4 Vulnerability Severity Category Code Definitions .....	2
1.5 SRG Compliance Reporting.....	4
1.6 STIG Distribution.....	4
1.7 Document Revisions .....	5
<b>2. ASSESSMENT CONSIDERATIONS.....</b>	<b>6</b>
2.1 Mobile Device Management (MDM) Configuration .....	6
2.2 Compliance via Third-party Applications and Components .....	6
2.3 Indirect Compliance .....	7
2.4 Samsung Knox Android Dual-Persona Capability .....	7
<b>3. SAMSUNG KNOX ANDROID IA FEATURES.....</b>	<b>8</b>
<b>APPENDIX A—ACRONYMS .....</b>	<b>9</b>

## LIST OF TABLES

	<b>Page</b>
Table 1-1: Vulnerability Severity Category Code Definitions .....	2

## **1. INTRODUCTION**

### **1.1 Background**

The Samsung Knox Android 1.0 Overview, along with the Samsung Knox Android Security Technical Implementation Guide (STIG), provides the technical security policies, requirements, and implementation details for applying security concepts to Samsung Knox Android 1.0.

### **1.2 Authority**

DoD Directive (DoDD) 8500.1 requires that “all IA and IA-enabled IT products incorporated into DoD information systems shall be configured in accordance with DoD-approved security configuration guidelines” and tasks Defense Information Systems Agency (DISA) to “develop and provide security configuration guidance for IA and IA-enabled IT products in coordination with Director, NSA.” This document is provided under the authority of DoDD 8500.1.

Although Security Requirements Guides (SRGs) and STIGs implement an applicable subset of IA controls for specific types of systems, all applicable IA controls must be applied to information systems. The current DoD IA controls are specified in DoDI 8500.2. Draft DoDI 8500.02aa states that “All DoD ISS and platform IT systems, including non-National Security System (NSS), shall be categorized in accordance with Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253, and implement a corresponding set of security controls that are published in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53.” SRGs and derived STIGs are based on NIST SP 800-53.

### **1.3 Scope**

This document is a requirement for all DoD administered systems and all systems connected to DoD networks. These requirements are designed to assist Security Managers (SMs), Information Assurance Managers (IAMs), Information Assurance Officers (IAOs), and System Administrators (SAs) with configuring and maintaining security controls. This guidance supports DoD system design, development, implementation, certification, and accreditation efforts.

## 1.4 Vulnerability Severity Category Code Definitions

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Code of CAT I, II, or III.

**Table 1-1: Vulnerability Severity Category Code Definitions**

	DISA Category Code Guidelines	Examples of DISA Category Code Guidelines
CAT I	Any vulnerability, the exploitation of which will directly and immediately result in loss of Confidentiality, Availability, or Integrity.	Includes <b>BUT NOT LIMITED</b> to the following examples of direct and immediate loss: <ol style="list-style-type: none"> <li>1. May result in loss of life, loss of facilities, or equipment, which would result in mission failure.</li> <li>2. Allows unauthorized access to security or administrator level resources or privileges.</li> <li>3. Allows unauthorized disclosure of, or access to, classified data or materials.</li> <li>4. Allows unauthorized access to classified facilities.</li> <li>5. Allows denial of service or denial of access, which will result in mission failure.</li> <li>6. Prevents auditing or monitoring of cyber or physical environments.</li> <li>7. Operation of a system/capability which has not been approved by the appropriate Designated Accrediting Authority (DAA).</li> <li>8. Unsupported software where there is no documented acceptance of DAA risk.</li> </ol>

	DISA Category Code Guidelines	Examples of DISA Category Code Guidelines
CAT II	Any vulnerability, the exploitation of which has a potential to result in loss of Confidentiality, Availability, or Integrity.	<p>Includes <b><u>BUT NOT LIMITED</u></b> to the following examples that have a potential to result in loss:</p> <ol style="list-style-type: none"><li>1. Allows access to information that could lead to a CAT I vulnerability.</li><li>2. Could result in personal injury, damage to facilities, or equipment which would degrade the mission.</li><li>3. Allows unauthorized access to user or application level system resources.</li><li>4. Could result in the loss or compromise of sensitive information.</li><li>5. Allows unauthorized access to Government or Contractor owned or leased facilities.</li><li>6. May result in the disruption of system or network resources degrading the ability to perform the mission.</li><li>7. Prevents a timely recovery from an attack or system outage.</li><li>8. Provides unauthorized disclosure of or access to unclassified sensitive, Personally Identifiable Information (PII), or other data or materials.</li></ol>

	DISA Category Code Guidelines	Examples of DISA Category Code Guidelines
CAT III	Any vulnerability, the existence of which degrades measures to protect against loss of Confidentiality, Availability, or Integrity.	<p>Includes <b><u>BUT NOT LIMITED</u></b> to the following examples that provide information which could potentially result in degradation of system information assurance measures or loss of data:</p> <ol style="list-style-type: none"> <li>1. Allows access to information that could lead to a CAT II vulnerability.</li> <li>2. Has the potential to affect the accuracy or reliability of data pertaining to personnel, resources, operations, or other sensitive information.</li> <li>3. Allows the running of any applications, services or protocols that do not support mission functions.</li> <li>4. Degrades a defense in depth systems security architecture.</li> <li>5. Degrades the timely recovery from an attack or system outage.</li> <li>6. Indicates inadequate security administration.</li> <li>7. System not documented in the site's C&amp;A Package/System Security Plan (SSP).</li> <li>8. Lack of document retention by the Information Assurance Manager (IAM) (i.e., completed user agreement forms).</li> </ol>

## 1.5 SRG Compliance Reporting

All technical NIST SP 800-53 requirements were considered while developing this STIG. Requirements that are applicable and configurable are included in this STIG. A compliance report marked For Official Use Only (FOUO) is available for those items that did not meet requirements. This report is available to component DAA personnel for risk assessment purposes by request via email to [disa.letterkenny.FSO.mbx.stig-customer-support-mailbox@mail.mil](mailto:disa.letterkenny.FSO.mbx.stig-customer-support-mailbox@mail.mil).

## 1.6 STIG Distribution

Parties within the DoD and Federal Government's computing environments can obtain the applicable STIG from the Information Assurance Support Environment (IASE) website. This site contains the latest copies of any STIGs, SRGs, and other related security information. The address for the IASE site is <http://iase.disa.mil/>.



## 1.7 Document Revisions

Comments or proposed revisions to this document should be sent via email to the following address: [disa.letterkenny.FSO.mbx.stig-customer-support-mailbox@mail.mil](mailto:disa.letterkenny.FSO.mbx.stig-customer-support-mailbox@mail.mil). DISA Field Security Operations (FSO) will coordinate all change requests with the relevant DoD organizations before inclusion in this document.

## 2. ASSESSMENT CONSIDERATIONS

### 2.1 Mobile Device Management (MDM) Configuration

To implement the Samsung Knox Android STIG, a security policy created on an MDM administration console must be assigned to the target devices. All devices in a specific group are assigned the same policy.

To create a STIG policy for a Samsung Knox Android device:

1. Log into the MDM Administration Console.
2. Select the appropriate menu for managing policies.
3. Create a “Knox STIG” policy group, and configure policy rules as specified in the Samsung Knox Android STIG.
4. Create a new user group named “Knox STIG Users” and assign it the “Knox STIG” policy group.

### 2.2 Compliance via Third-party Applications and Components

The Samsung Knox platform provides various APIs for third-party solution vendors to develop Knox security components that can be used to implement several Mobile Operating System (MOS) SRG IA controls. This allows for the integration of any third-party applications and components to achieve compliance to the Samsung Knox Android STIG. The APIs that are provided by the Samsung Knox platform are:

- The Samsung MDM API includes over 500 policies and 1100 interfaces that are designed to be called by any MDM agent. Using these policies and interfaces, the MDM solution vendor can implement an MDM solution that can meet or exceed the SRG requirements. Examples of MDM vendors that implement the Samsung MDM API include Mobile Iron, AirWatch, SOTI, and Fixmo.
- The Samsung Integrity Services Layer (ISL) provides an interface that allows any third-party vendor to implement an Integrity Services Agent (ISA) solution to communicate with the on-device MDM agent. The ISA will provide scanning for integrity failures on the device, and report results to the MDM server. Examples of solutions that implement the ISL include Fixmo ISA.
- The Samsung MDM API includes advanced VPN policies and interfaces that allow an MDM administrator to configure any third-party IPsec VPN solution which implements the MDM interfaces. The VPN enables the Samsung Knox Android device to connect to DoD networks and uses a FIPS 140-2 validated cryptographic module to protect data in transit. Examples of solutions that implement the MDM interface include Mocana KeyVPN and Inside Secure VPN.
- The Samsung Smart Card API provides an interface that allows any third-party vendor to implement smart card reader functionality for the Samsung Knox Android device.

Solutions implementing this interface enable Samsung Knox Android to support applications leveraging the DoD Common Access Card (CAC) for PKI-related transactions, including user authentication to DoD networks and websites, S/MIME digital signatures, and, if desired, device unlock. Examples of solutions that implement this interface include the Biometrics Associates Bluetooth Smart Card Reader.

## **2.3 Indirect Compliance**

In some cases, the Samsung Knox Android solution MOS SRG compliance is achieved through means other than direct implementation of the required IA control:

- Neither Android nor Samsung Knox Android authenticate applications through digital signature verification, but Samsung Knox Android uses an application quarantine capability that provides equivalent protection when system administrators correctly identify which applications should be permitted to exit the quarantine.
- Samsung Knox Android does not directly enforce MOS SRG Bluetooth requirements in its native Bluetooth stack, but uses a Bluetooth whitelisting capability to assure that only Bluetooth peripherals that comply with the requirements are permitted to pair with the Samsung Knox Android device.
- Samsung Knox Android meets the requirement for having a capability to log privileged text-based commands by disabling the ability to perform such commands, thereby rendering the requirement inapplicable.

## **2.4 Samsung Knox Android Dual-Persona Capability**

Samsung Knox Android can support multiple user security domains, such as separate personal and work personas. MDM software controls the creation, activation, and deactivation of these domains. However, the Samsung Knox Android 1.0 STIG does not include configuration guidance for the dual-persona use case, which DoD has not yet authorized. The dual-persona capability may be addressed in future releases of the Samsung Knox Android STIG. Until that occurs, implementing organizations must not activate personal containers or domains on Samsung Knox Android devices.

### 3. SAMSUNG KNOX ANDROID IA FEATURES

The Samsung Knox Android Platform is an extension of Android 4.1.1 (Jelly Bean) built on a SELinux-enabled kernel. It also fully incorporates Samsung SAFE, a technology used to facilitate MDM control of Samsung devices and provide additional security not found in native Android. Knox Android was designed to meet the requirements of the MOS SRG. Samsung Knox Android 1.0 currently supports the North American versions of the Samsung Galaxy S3 and Galaxy S4.

Key IA features found in Samsung Knox Android that are not present in typical Android devices are:

- Mobile application quarantine,
- Smart card support,
- Host-based firewall,
- Ability to revoke mobile application permissions,
- Over-the-air (OTA) audit log retrieval, and
- Support for PKI authentication and certificate verification in native browser.

**APPENDIX A—ACRONYMS**

API	Application Programming Interface
CA	Certificate Authority
CAC	Common Access Card
CAT	Severity Category Code
CCI	Control Correlation Identifiers
CMD	Commercial Mobile Device
CNSS	Committee on National Security Systems
CNSSI	CNNS Instruction
DAA	Designated Accrediting Authority
DISA	Defense Information Systems Agency
DoD	Department of Defense
DoDD	DoD Directive
DODI	DoD Instruction
FIPS	Federal Information Processing Standard
FOUO	For Official Use Only
FSO	Field Security Operations
IA	Information Assurance
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IASE	Information Assurance Support Environment
IPSec	Internet Protocol Security
IS	Information System
ISA	Integrity Services Agent
ISL	Integrity Services Layer
IT	Information Technology
MDM	Mobile Device Management
MOS	Mobile Operating System
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSS	National Security System
OS	Operating System
OTA	Over-the-air
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
S/MIME	Secure/Multipurpose Internet Mail Extensions
SA	System Administrator
SM	Security Manager
SP	Special Publication
SRG	Security Requirement Guide
SSP	Systems Security Plan
STIG	Security Technical Implementation Guide
URL	Uniform Resource Locator

VPN	Virtual Private Network
-----	-------------------------