



Unisoc Confidential For hiar

CTA 入网安全能力测试指导手册

文档版本
发布日期

V1.2
2020-11-06

版权所有 © 紫光展锐（上海）科技有限公司。保留一切权利。

本文件所含数据和信息都属于紫光展锐（上海）科技有限公司（以下简称紫光展锐）所有的机密信息，紫光展锐保留所有相关权利。本文件仅为信息参考之目的提供，不包含任何明示或默示的知识产权许可，也不表示有任何明示或默示的保证，包括但不限于满足任何特殊目的、不侵权或性能。当您接受这份文件时，即表示您同意本文件中内容和信息属于紫光展锐机密信息，且同意在未获得紫光展锐书面同意前，不使用或复制本文件的整体或部分，也不向任何其他方披露本文件内容。紫光展锐有权在未经事先通知的情况下，在任何时候对本文件做任何修改。紫光展锐对本文件所含数据和信息不做任何保证，在任何情况下，紫光展锐均不负任何与本文件相关的直接或间接的、任何伤害或损失。

请参照交付物中说明文档对紫光展锐交付物进行使用，任何人对紫光展锐交付物的修改、定制化或违反说明文档的指引对紫光展锐交付物进行使用造成的任何损失由其自行承担。紫光展锐交付物中的性能指标、测试结果和参数等，均为在紫光展锐内部研发和测试系统中获得的，仅供参考，若任何人需要对交付物进行商用或量产，需要结合自身的软硬件测试环境进行全面的测试和调试。

Unisoc Confidential For hiar

紫光展锐（上海）科技有限公司



前言

概述

本文档主要描述了展锐 CTA 入网安全能力方案、安全能力功能开启、不支持权限的移除和安全能力功能自测。

读者对象


本文档主要适用展锐智能机平台维护 CTA 入网安全能力方案或负责 CTA 入网安全能力测试的相关人员。

缩略语

缩略语	英文全名	中文解释
CTA	China Testing Alliance	中国质量检验联盟
TAF	Telecommunication Terminal Industry Forum Association	电信终端产业协会

符号约定

在本文中可能出现下列标志，它所代表的含义如下。

符号	说明
 说明	用于突出重要/关键信息、补充信息和小窍门等。 “说明”不是安全警示信息，不涉及人身、设备及环境伤害。

变更信息

文档版本	发布日期	修改说明
V1.0	2019-10-09	初稿。
V1.1	2020-04-08	更新文档模板和内容优化。

文档版本	发布日期	修改说明
V1.2	2020-11-06	1、更新文档模板。 2、更新 1.2 安全能力等级。 3、更新 4.3 Android 6.0 至 4.6 Android 9.0 节。 4、增加 4.7 Android 10.0 节。

关键字

CTA、安全能力、入网安全。

Unisoc Confidential For hiar

目 录

1 概述.....	1
1.1 测试背景	1
1.2 安全能力等级	1
2 方案介绍.....	3
2.2 架构	3
2.2.1 安全防护主系统	3
2.2.2 自启动管理系统	4
2.2.3 权限数据库	5
2.3 代码结构	5
3 Sample Code 说明	7
3.1 结构	7
3.2 合入说明	7
4 功能开启.....	9
4.1 Android 4.4	9
4.2 Android 5.1	9
4.3 Android 6.0	10
4.4 Android 7.0	10
4.5 Android 8.1	11
4.6 Android 9.0	12
4.7 Android 10.0	13
5 不支持的权限移除.....	15
6 功能自测.....	17
7 常见问题.....	22
8 附录.....	23

图目录

图 2-1 通讯类功能受控机制	3
图 2-2 安全防护主系统架构图	4
图 2-3 自启动管理系统架构图	5
图 2-4 代码结构图	6
图 3-1 Sample Code 结构	7
图 3-2 代码路径	8
图 6-1 功能开启提示界面	17
图 6-2 权限配置界面	18
图 6-3 Test 界面	19
图 6-4 拨号权限确认对话框	20
图 6-5 短信权限确认对话框	21
图 7-1 权限配置日志界面	22

表目录

表 1-1 芯片平台及其支持的安全能力等级	1
表 5-1 权限数据库	15
表 8-1 移动智能终端安全能力分级表	23
表 8-2 移动智能终端安全能力等级标识	25
表 8-3 移动智能终端功能丰富度标识	25

Unisoc Confidential For hiar

1 概述

1.1 测试背景

依据 2013 年工信部电管[2013]120 号《关于加强移动智能终端进网管理的通知》：“申请进网许可的移动智能终端应当符合通信行业标准有关移动智能终端安全的基本要求，检测机构在进网检测时应该依据相关标准进行检测”，泰尔终端实验室目前在进行测试。

移动智能终端安全能力技术要求由电信终端产业协会提出并归口，对应的标准为：TAF-WG4-AS0015-V1.0.0:2018 移动智能终端安全能力技术要求。

该技术要求将移动智能终端的安全能力自低到高划分为 5 个等级（最低等级 1 级，最高等级 5 级），在不同的等级中分别定义了移动智能终端需要支持的安全能力集合，移动智能终端必须支持该集合中所约束的所有安全能力才能标识为该级别。具体的等级划分和安全能力标识请详见 8 附录。

在现阶段：

- CMCC 要求 Level 4。
- CUCC 要求 Level 1。
- CTA 要求 Level 1，同时鼓励厂家主动提高安全能力级别。

1.2 安全能力等级

目前展锐取得认证的芯片平台及其支持的安全能力等级如表 1-1 所示

表1-1 芯片平台及其支持的安全能力等级

Android 版本	芯片平台	支持的安全能力等级
Android4.4	SC7731G/SC9830	LEVEL 4
Android5.1	SC9830	LEVEL 4
Android6.0	SC9832A/SC9860	LEVEL 4
Android7.0	SC9832A	LEVEL 5
Android8.1	SC9850K	LEVEL 5
Android9.0	UMS312	LEVEL 4

说明

- 平台侧的策略是每个 Android 大版本选择一个芯片平台送测，在其他没有列出的相同 Android 版本的芯片平台上，该功能同样支持。

- 从 2018 年 3 月 1 日开始实施了新规范 (TAF-WG4-AS0015-V1.0.0:2018)，按照新规范的技术要求，目前展锐平台的最高支持能力为 Level 4（按照 2018 年 3 月 1 日之前的旧规范，展锐平台的最高支持能力为 Level 5）。
- Android 10.0 版本，目前展锐芯片平台未送测，但最高支持能力为 Level 4。

Unisoc Confidential For hiar

2 方案介绍

依据移动智能终端安全能力技术要求，展锐平台开发了 CTA 入网安全能力功能，用以支撑展锐平台 CTA 入网安全能力送测。基于此功能，当第三方应用在使用某种敏感权限时，将会给用户相应的提示。以通讯类功能受控机制中的发送短信和拨打电话为例，如图 2-1 所示：

图2-1 通讯类功能受控机制



2.2 架构

CTA 入网安全能力方案架构包含安全防护主系统、自启动管理系统和权限数据库三部分。

2.2.1 安全防护主系统

安全防护主系统包含安全策略配置应用和安全策略实施层，其架构如图 2-2 所示。

图2-2 安全防护主系统架构图

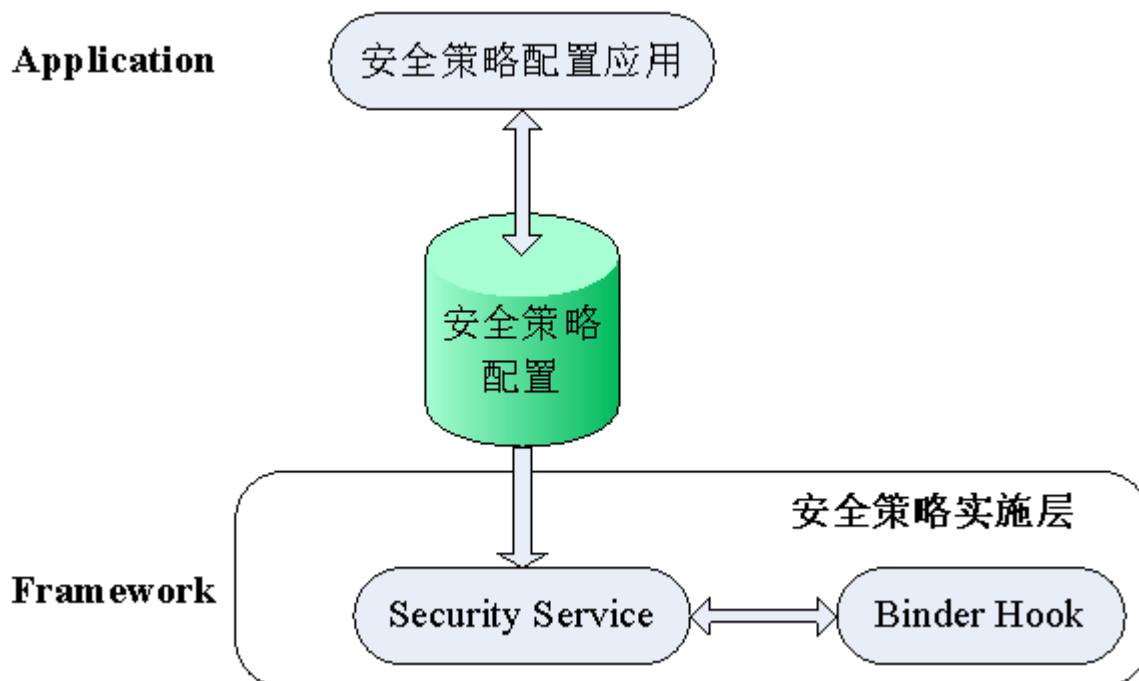


图 2-2 中说明如下：

- 安全策略应用：向用户提供配置界面。
- 安全策略实施层：实施所配置的安全策略。

2.2.2 自启动管理系统

自启动管理系统包含自启动管理应用和广播拦截，其架构如图 2-3 所示。

图2-3 自启动管理系统架构图

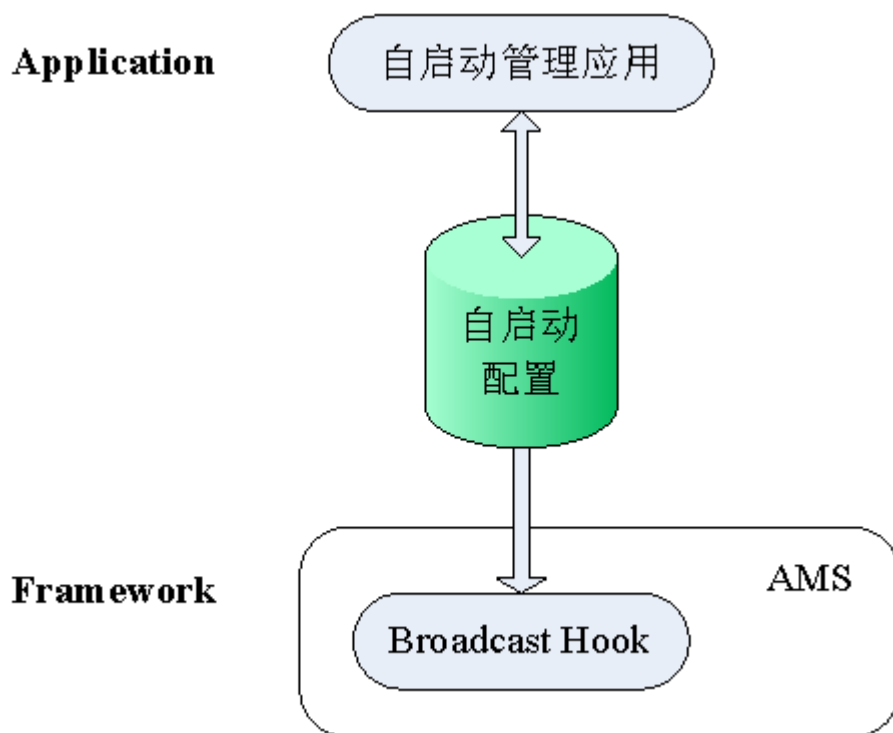


图 2-3 中说明如下：

- 自启动管理应用：向用户提供配置界面。
- Broadcast Hook：拦截广播，实施所配置的自启动策略。

2.2.3 权限数据库

权限数据库存储了 CTA 入网安全能力功能所对应的权限策略，与安全防护主系统中的 Security Service/Binder Hook 对接。

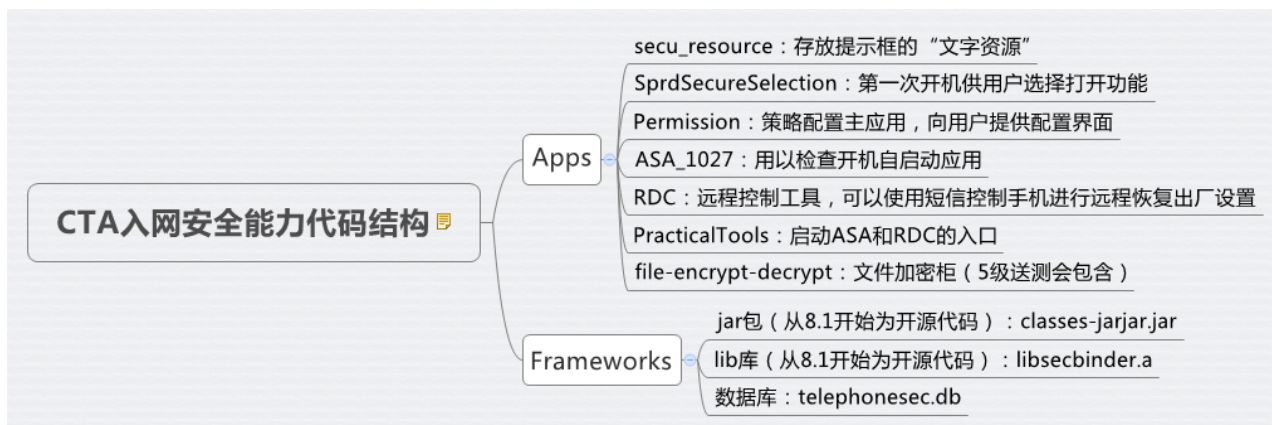
2.3 代码结构

CTA 入网安全能力方案代码结构包含 7 个 apk，以及核心实现部分所对应的 jar 包、lib 库和数据库，如图 2-4。

说明

- Android7.0 之前的版本为 6 个 apk。
- Android7.0 及之后版本为 7 个 apk。

图2-4 代码结构图



Unisoc Confidential For hiar

3 Sample Code 说明

平台侧在送测通过后，会将结果合入平台版本，但是由于版本在不断迭代，同时泰尔实验室测试环境也会存在更新，客户侧在送测时，请在展锐 CQ 支持系统中提交对应的问题单（Android_Security_CCSA/FDE/DmVerity）以获取最新状态的 Sample Code，本章对 Sample Code 结构和合入方法进行说明。

3.1 结构

CTA 入网安全能力方案 Sample Code 结构如图 3-1 所示

图3-1 Sample Code 结构



3.2 合入说明

请参考图 3-2 中的路径说明以及 Sample Code 中的 readme，将 Sample Code 中的 APK、Jar 包和 Lib 库合入，详细如下：

- **APKs:** 请按不同的 Android 版本，分别取对应的版本路径下的 APK。
- **Code:** 该部分的修改请按 Sample Code 路径下的 readme 中的说明进行合入。
- **Jar 包:** Android 4.4 是单独的文件，其他版本请使用 Common 路径下的文件。
- **Lib 库:** 请按项目的实际配置（ARM 架构下的 32 位或是 64 位，X86 架构下的 32 位或是 64 位）分别取对应路径下的库文件，配置信息可以通过 Board 中的 TARGET_ARCH 参数来确认。

图3-2 代码路径



Unisoc Confidential For hiar

4 功能开启

CTA 入网安全能力功能默认关闭，在制作送测版本时，需手动开启，本章对各个 Android 版本下如何开启该功能进行说明。

4.1 Android 4.4

以 sp9820a_refh10_native.mk 为例，请参考下面红色框标识。

```
# Overlay touch screen features, and all core feature should edit here, not modify directly
PRODUCT_COPY_FILES := \
    $(BOARD_DIR)/handheld_core_hardware.xml:system/etc/permissions/handheld_core_hardware.xml \
    $(BOARD_DIR)/android.hardware.touchscreen.multitouch.xml:system/etc/permissions/android.hardware.touchscreen.multitouch.xml \
    $(BOARD_DIR)/android.hardware.touchscreen.xml:system/etc/permissions/android.hardware.touchscreen.xml \
    $(PRODUCT_COPY_FILES)

# add security build info
$(call inherit-product, vendor/sprd/open-source/security_support.mk)

WCN_EXTENSION := true

# PRODUCT_REVISION := multiuser
# include $(APPLY_PRODUCT_REVISION)

CHIPRAM_DEFCONFIG := sp9820a_refh10
KERNEL_DEFCONFIG := sp9820a_refh10_defconfig
DTS_DEFCONFIG := sprd-scx35l_sp9820a_refh10
UBOOT_DEFCONFIG := sp9820a_refh10
```

4.2 Android 5.1

以 sp9830aed_5m_h100_dt_cmcc.mk 为例，请参考下面红色框标识。

```
diff --git a/sp9830aed_5m_h100/sp9830aed_5m_h100_dt_cmcc.mk b/sp9830aed_5m_h100/sp9830aed_5m_h100_dt_cmcc.mk
index 8ed7219..b289e2f 100644
--- a/sp9830aed_5m_h100/sp9830aed_5m_h100_dt_cmcc.mk
+++ b/sp9830aed_5m_h100/sp9830aed_5m_h100_dt_cmcc.mk
@@ -24,6 +24,9 @@ VOLTE_SERVICE_ENABLE := true
# add animation resource.
$(call inherit-product, vendor/sprd/open-source/res/boot/boot_res_cmcc_4g_fwvga.mk)

+# add security build info
+$(call inherit-product, vendor/sprd/open-source/security_support.mk)
+
# Overrides
PRODUCT_NAME := sp9830aed_5m_h100_dt_cmcc
PRODUCT_DEVICE := $(TARGET_BOARD)
```

增加
security_support.mk

4.3 Android 6.0

以 sp9820a_refh10_native.mk 为例，请参考下面红色框标识。

```
$(PRODUCT_COPY_FILES)

# add security build info
$(call inherit-product, vendor/sprd/open-source/security_support.mk)

WCN_EXTENSION := true

# PRODUCT_REVISION := multiuser
# include $(APPLY_PRODUCT_REVISION)

CHIPRAM_DEFCONFIG := sp9820a_refh10
KERNEL_DEFCONFIG := sp9820a_refh10_defconfig
DTS_DEFCONFIG := sprd-scx35l_sp9820a_refh10
UBOOT_DEFCONFIG := sp9820a_refh10
```

说明

针对泰尔实验室测试新需求，会使用到第三方定位 APP 测试定位权限，如百度地图、美团外卖、360 天气等，而展锐 CTA 入网安全能力的整体方案只是针对系统定位 API 的，并不能拦截内置了定位 sdk 的应用。因此针对这种情况，展锐更新了解决方案，客户需要申请 SampleCode。

4.4 Android 7.0

以 sp9832a_3h10_cmcc.mk 为例，请参考下面红色框标识。

```
include device/sprd/scx35l/sp9832a_3h10_volte/sp9832a_3h10_5mvolte.mk
include vendor/sprd/operator/cmcc/configs/spec2.mk

#ccsa test on
$(call inherit-product, vendor/sprd/operator/ccsa/prebuilds/security_support.mk)
PRODUCT_REVISION := common cmcc
include $(APPLY_PRODUCT_REVISION)
include device/sprd/scx35l/common/5mod.mk

# Override
PRODUCT_NAME := sp9832a_3h10_cmcc

# add animation resource.
$(call inherit-product, vendor/sprd/operator/cmcc/configs/res/boot/boot_res_cmcc_4g_hd.mk)
```

说明

针对泰尔实验室测试新需求，会使用到第三方定位 APP 测试定位权限，如百度地图、美团外卖、360 天气等，而展锐 CTA 入网安全能力的整体方案只是针对系统定位 API 的，并不能拦截内置了定位 sdk 的应用。因此针对这种情况，展锐更新了解决方案，客户需要申请 SampleCode。

4.5 Android 8.1

由于从 Android 8.1 开始编译系统发生了变化，所以在 Android 8.1 上开启 CTA 入网安全能力的方式也有所变化，在修改.mk 文件的同时，还需要修改.bp 文件，参考步骤如下：

步骤 1 在主 mk 中增加 include security_support.mk，同时打开 ccsa 开关，如下所示。

```
#ccsa test on
$(call inherit-product, vendor/sprd/operator/ccsa/prebuilts/security_support.mk)
PRODUCT_REVISION := ccsa
```

步骤 2 在 frameworks/native/libs/binder/Android.bp 中打开 USE_PROJECT_SEC，如下面红色字体。

```
cflags: [
    "-Wall",
    "-Wextra",
    "-Werror",
    "-DUSE_PROJECT_SEC"
],
```

步骤 3 在 frameworks/av/media/libmedia/Android.bp 中打开 USE_PROJECT_SEC，如下面红色字体。

```
cflags: [
    "-Werror",
    "-Wno-error=deprecated-declarations",
    "-Wall",
    "-DUSE_PROJECT_SEC"
],
```

步骤 4 在 frameworks/av/camera/Android.bp 中打开 USE_PROJECT_SEC，如下面红色字体。

```
cflags: [
    "-Werror",
    "-Wall",
    "-Wextra",
    "-DUSE_PROJECT_SEC",
    "-DSPRD_FRAMEWORKS_CAMERA_EX",
    "-DSPRD_FEATURE_BRIGHTNESS",
    "-DSPRD_FEATURE_ISO",
    "-DSPRD_FEATURE_CONTRAST",
    "-DSPRD_FEATURE_SATURATION",
    "-DSPRD_FEATURE_METERING_MODE",
    "-DSPRD_FEATURE_SLOW_MOTION",
    "-DSPRD_FEATURE_3GVT",
    "-DSPRD_FEATURE_BEAUTY",
    "-DSPRD_FEATURE_EIS",
]
```

说明

- 从 Android 8.1 开始，针对自启动管理功能，已由 Android 原生的自启动管理功能来支持，CTA 入网安全能力功能中包含的 ASA.apk 已不再使用。
- 针对泰尔实验室测试新需求，会使用到第三方定位 APP 测试定位权限，如百度地图、美团外卖、360 天气等，而展锐 CTA 入网安全能力的整体方案只是针对系统定位 API 的，并不能拦截内置了定位 sdk 的应用。因此针对这种情况，展锐更新了解决方案，客户需要申请 SampleCode。

---结束

4.6 Android 9.0

在合入 Android 9.0 对应的 Sample Code 的基础上，开启 CTA 入网安全能力功能请参考如下步骤：

步骤 1 在主 mk 中增加 include security_support.mk，同时打开 ccsa 开关，如下所示。

```
#ccsa test on
$(call inherit-product, vendor/sprd/operator/ccsa/prebuilts/security_support.mk)
PRODUCT_REVISION := ccsa
```

步骤 2 在 frameworks/native/libs/binder/Android.bp 中打开 USE_PROJECT_SEC，如下面红色字体。

```
cflags: [
    "-Wall",
    "-Wextra",
    "-Werror",
    "-DUSE_PROJECT_SEC"
],
```

步骤 3 在 frameworks/av/media/libmedia/Android.bp 中打开 USE_PROJECT_SEC，如下面红色字体。

```
cflags: [
    "-Werror",
    "-Wno-error=deprecated-declarations",
    "-Wall",
    "-DUSE_PROJECT_SEC"
],
```

步骤 4 在 frameworks/av/media/libmediaplayerservice/Android.bp 中打开 USE_PROJECT_SEC，如下面红色字体。

```
cflags: [
    "-Werror",
    "-Wno-error=deprecated-declarations",
    "-Wall",
    "-DUSE_PROJECT_SEC"
],
```

步骤 5 在 frameworks/av/camera/Android.bp 中打开 USE_PROJECT_SEC，如下面红色字体

```
cflags: [
```

```

    "-Werror",
    "-Wall",
    "-Wextra",
    "-DSPRD_FRAMEWORKS_CAMERA_EX",
    "-DSPRD_FEATURE_BRIGHTNESS",
    "-DSPRD_FEATURE_ISO",
    "-DSPRD_FEATURE_CONTRAST",
    "-DSPRD_FEATURE_SATURATION",
    "-DSPRD_FEATURE_METERING_MODE",
    "-DSPRD_FEATURE_SLOW_MOTION",
    "-DSPRD_FEATURE_3GVT",
    "-DSPRD_FEATURE_BEAUTY",
    "-DSPRD_FEATURE_EIS",
    "-DSPRD_FEATURE_ZSL",
    "-DSPRD_FEATURE_3DNR",
    "-DUSE_PROJECT_SEC",
],

```

----结束

4.7 Android 10.0

开启 CTA 入网安全能力功能请参考如下步骤：

步骤 1 在主 mk 中打开 ccsa 开关，如下所示。

```

#ccsa test on
PRODUCT_REVISION := ccsa

```

步骤 2 在 frameworks/native/libs/binder/Android.bp 中打开 USE_PROJECT_SEC，如下面红色字体。

```

cflags: [
    "-Wall",
    "-Wextra",
    "-Werror",
    "-DUSE_PROJECT_SEC"
],

```

步骤 3 在 frameworks/av/media/libmedia/Android.bp 中打开 USE_PROJECT_SEC，如下面红色字体。

```

cflags: [
    "-Werror",
    "-Wno-error=deprecated-declarations",
    "-Wall",
    "-DUSE_PROJECT_SEC"
],

```

步骤 4 在 frameworks/av/media/libmediaplayerservice/Android.bp 中打开 USE_PROJECT_SEC，如下面红色字体。

```
cflags: [  
    "-Werror",  
    "-Wno-error=deprecated-declarations",  
    "-Wall",  
    "-DUSE_PROJECT_SEC"  
],
```

步骤 5 在 frameworks/av/camera/Android.bp 中打开 USE_PROJECT_SEC，如下面红色字体。

```
cflags: [  
    "-Werror",  
    "-Wall",  
    "-Wextra",  
    "-DSPRD_FRAMEWORKS_CAMERA_EX",  
    "-DSPRD_FEATURE_BRIGHTNESS",  
    "-DSPRD_FEATURE_ISO",  
    "-DSPRD_FEATURE_CONTRAST",  
    "-DSPRD_FEATURE_SATURATION",  
    "-DSPRD_FEATURE_METERING_MODE",  
    "-DSPRD_FEATURE_SLOW_MOTION",  
    "-DSPRD_FEATURE_3GVT",  
    "-DSPRD_FEATURE_BEAUTY",  
    "-DSPRD_FEATURE_EIS",  
    "-DSPRD_FEATURE_ZSL",  
    "-DSPRD_FEATURE_3DNR",  
    "-DUSE_PROJECT_SEC",  
],
```

---结束

📖 说明

针对泰尔实验室测试新需求，会使用到第三方定位 APP 测试定位权限，如百度地图、美团外卖、360 天气等，而展锐 CTA 入网安全能力的整体方案只是针对系统定位 API 的，并不能拦截内置了定位 sdk 的应用。因此针对这种情况，展锐更新了解决方案，客户需要申请 SampleCode。

5 不支持的权限移除

CTA 入网安全能力功能默认支持规范中规定的所有权限的拦截，如果一个项目的硬件配置不支持 WLAN 或 GPS，那么不支持的权限也应在 CTA 入网安全能力功能中移除。移除权限配置应用中的某项权限，可通过删除 telephonesec.db 数据库中的相应权限来实现，该数据库中各权限对应的 policy_id 以及所在的 TABLE 如表 5-1。

表5-1 权限数据库

权限	policy_id	TABLE
拨打电话	101	opr2policy, opr2keywords
发送短信	102	opr2policy, opr2keywords
发送彩信	103	opr2policy, opr2keywords
发送邮件	104	opr2policy, opr2keywords
开启移动数据	105	opr2policy, opr2keywords
开启 WLAN	106	opr2policy
调用定位功能	201	opr2policy, opr2keywords
开启录音或通话录音	202	opr2policy
开启摄像头	204	opr2policy
写入/删除电话本	205	opr2policy
写入/删除通话记录	206	opr2policy
写入/删除短信数据	207	opr2policy
写入/删除彩信数据	208	opr2policy
读电话本数据	209	opr2policy
读通话记录	210	opr2policy
读短信数据	211	opr2policy
读彩信数据	212	opr2policy
读被保护文件	213	opr2policy
开启蓝牙	301	opr2policy
开启 NFC	302	opr2policy, opr2keywords

以移除定位权限为例，移除时需要执行如下操作：

步骤 1 删除 telephonesec.db 中 policy_id = 201 的行。

```
delete from opr2policy where policy_id = 201;  
delete from opr2keywords where policy_id = 201;
```

步骤 2 用修改后的数据库替换原版本中的 telephonesec.db，重新编译版本。

📖 说明

- 移除某个权限，也可使用工具 sqlitebrowser 删除 telephonesec.db 数据库中的相应权限来实现。
- telephonesec.db 中有 opr2policy 和 opr2keywords 两张表，如果需要删除的权限在两张表中都存在，则需要同时删除两张表中的数据。
- 调试阶段可通过将 telephonesec.db push 到 /system/etc/telephonesec.db 目录，验证修改是否生效。但此时需要同时删除手机中的 /data/data/com.spreadst.security.permission/databases/permission.db 文件，重启手机后再验证，以确保权限配置应用的数据库与 telephonesec.db 同步。

---结束

Unisoc Confidential For hiar

6 功能自测

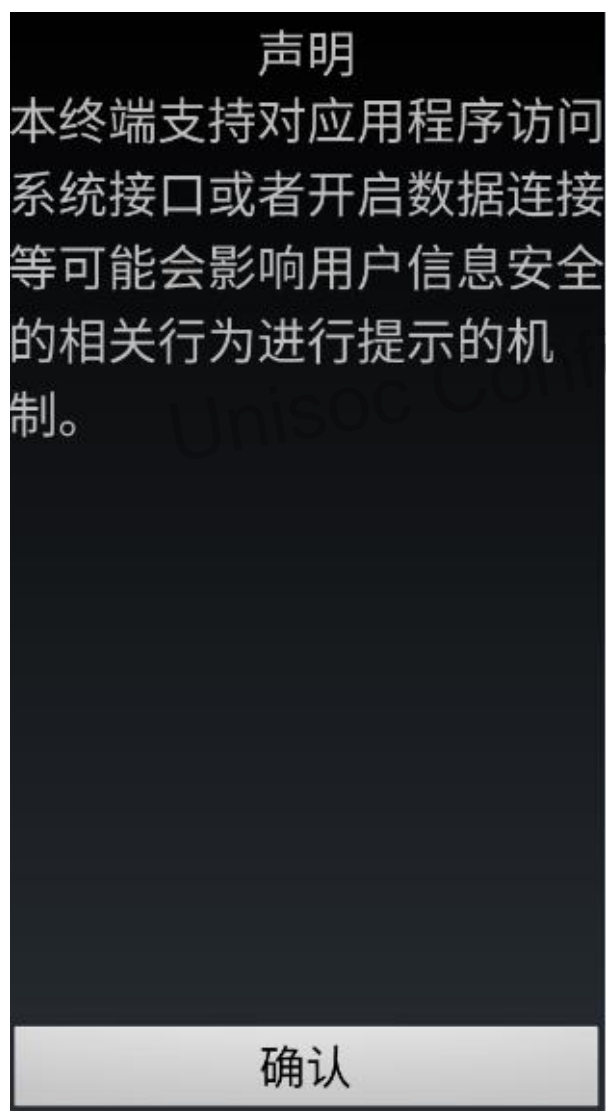
CTA 入网安全能力功能是否开启，以及权限配置是否生效，可以通过如下步骤进行自测检查：

步骤 1 第一次开机时，出现如图 6-1 所示的提示界面，则表示 CTA 入网安全能力功能已开启，单击“确认”键。

说明

若没有出现如图 6-1 所示的提示界面，请联系展锐 CTA 入网安全能力支持工程师。

图6-1 功能开启提示界面



步骤 2 在桌面打开“权限配置”应用，会进入权限配置界面，如图 6-2 所示。

图6-2 权限配置界面



步骤 3 在 Sample Code 根目录找到 test_ccsa.apk 文件，通过 adb install 方式进行安装，完成安装后会在桌面新增“Test”应用。

步骤 4 在桌面打开“Test”应用，会显示如图 6-3 所示的 Test 界面。

图6-3 Test 界面



步骤 5 这里以拨打电话和发送短信为例，查看是否会弹出对话框请用户确认。

- 拨号

在图 6-3 中单击“拨号”按钮，输入电话号码后单击“拨打电话”，会弹出弹出如图 6-4 所示的权限确认对话框。

图6-4 拨号权限确认对话框



- 短信
在图 6-3 中单击“短信”按钮，输入发送电话号码和短信内容后单击“发送”，会弹出弹出如图 6-5 所示的权限确认对话框。

图6-5 短信权限确认对话框



步骤 6 自测结果确认

- 各步骤结果正常：则说明 CTA 入网安全能力功能已经开启，权限配置已生效，可以有效拦截。
- 某步骤结果异常：请联系展锐 CTA 入网安全能力支持工程师进行技术支持。

---结束

7 常见问题

1. **问题描述：**如果合入了 Sample Code，但按照 6 功能自测所述的步骤检查后，发现功能没有生效。

分析及解决方法：可以通过检查开机 LOG 来分析 Security Service 是否被成功加载：

```
01-01 00:06:06.271 636 636 I SystemServer: Security Service
```

如果出现此条 log 输出，则说明安全服务已被注册到系统服务中。

2. **问题描述：**如何判断 Security Service 是否生效。

分析及解决方法：adb shell 进入手机，使用 getprop 去查看 service.project.sec 和 persist.support.securetest 两个属性值。

- getprop persist.support.securetest

返回值说明：

- 1 -- security service enable
- 0 或空 -- security service disable

- getprop service.project.sec

返回值说明：

- 1 -- 安全拦截生效
- 0 -- 安全拦截不生效

3. **问题描述：**虽然 CTA 入网安全能力功能在展锐平台上已通过测试，但是客户侧的版本状态与平台送测时的版本状态并不完全相同，在实际送测时，可能会由于版本状态的不同而出现个别失败项。

分析及解决方法：需要请前方测试人员在泰尔实验室环境下抓取问题场景对应的 Log，然后提交对应的 CQ 到模块 Android_Security_CCSA/FDE/DmVerity，展锐会提供对应的技术支持。抓取 Log 的操作流程：

- a. 在权限配置应用->日志下，将“打开 LOG”开关勾选上，如图 7-1 所示。

图7-1 权限配置日志界面



- b. 使用 adb logcat 抓取问题场景对应的 LOG。

8

附录

表8-1 移动智能终端安全能力分级表

安全能力		安全能力等级				
		一级	二级	三级	四级	五级
1	5.2.2 移动智能终端硬件远程控制安全能力	NA	NA	NA	NA	√
2	5.3.1.1.1 拨打电话	√	√	√	√	√
3	5.3.1.1.2 三方通话	NA	√	√	√	√
4	5.3.1.1.3 发送短信	√	√	√	√	√
5	5.3.1.1.4 发送彩信	√	√	√	√	√
6	5.3.1.1.5 发送邮件	NA	NA	NA	NA	√
7	5.3.1.1.6a) 移动通信网络数据连接—开关	√	√	√	√	√
8	5.3.1.1.6b) 移动通信网络数据连接—应用调用时的确认	√	√	√	√	√
9	5.3.1.1.6c) 移动通信网络数据连接—连接状态提示	√	√	√	√	√
10	5.3.1.1.6d) 移动通信网络数据连接—数据传送状态提示	NA	√	√	√	√
11	5.3.1.1.7a) WLAN 网络连接—开关	√	√	√	√	√
12	5.3.1.1.7b) WLAN 网络连接—应用调用时的确认	√	√	√	√	√
13	5.3.1.1.7c) WLAN 网络连接—连接状态提示	√	√	√	√	√
14	5.3.1.1.7d) WLAN 网络连接—数据传送状态提示	NA	NA	√	√	√
15	5.3.1.2.1 定位功能	√	√	√	√	√
16	5.3.1.2.2 通话录音功能	√	√	√	√	√
17	5.3.1.2.3 本地录音功能	√	√	√	√	√
18	5.3.1.2.3 拍照/摄像功能	√	√	√	√	√
19	5.3.1.2.5 a) 对用户数据的操作—修改/删除	NA	NA	NA	√	√
20	5.3.1.2.5 b) 对用户数据的操作—读	√	√	√	√	√

21	5.3.2 操作系统的更新	√	√	√	√	√
22	5.4.1.1 无线外围接口开启/关闭受控机制	√	√	√	√	√
23	5.4.1.2 无线外围接口连接建立的确认机制	√	√	√	√	√
24	5.4.1.3 无线外围接口连接状态标识	√	√	√	√	√
25	5.4.1.4 无线外围接口数据传输的受控机制	NA	NA		√	√
26	5.4.2.1 有线外围接口连接建立的确认机制	NA	NA	√	√	√
27	5.4.2.2 U 盘模式的安全机制	NA	NA	√	√	√
28	5.5.1 应用软件安全配置能力要求	NA	NA		√	√
29	5.5.2.1 非认证签名要求	√	√	√	√	√
30	5.5.2.2 认证签名要求	NA	NA	√	√	√
31	5.5.3 开机自启动程序监控能力	NA	NA	√	√	√
32	5.5.5.1 收集用户数据	√	√	√	√	√
33	5.5.5.2 修改用户数据	√	√	√	√	√
34	5.5.5.3.1 流量耗费	√	√	√	√	√
35	5.5.5.3.2 费用损失	√	√	√	√	√
36	5.5.5.3.3 信息泄露	√	√	√	√	√
37	5.6.1 移动智能终端的密码保护	√	√	√	√	√
38	5.6.2 文件类用户数据的授权访问	NA	NA	NA	NA	√
39	5.6.2 用户数据的加密存储	NA	NA	NA	NA	√
40	5.6.3 用户数据的彻底删除	NA	NA	√	√	√
41	5.6.4 用户数据的远程保护	NA	√	√	√	√
42	5.6.5 用户数据的转移备份	NA	√	√	√	√
43	6 移动智能终端功能限制性要求	√	√	√	√	√

表8-2 移动智能终端安全能力等级标识

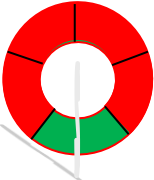
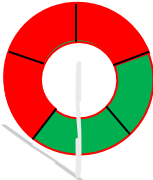
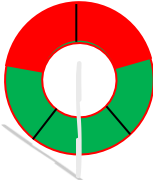
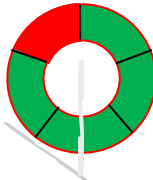
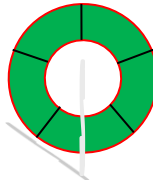

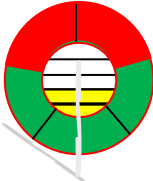

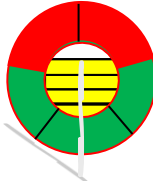
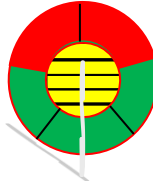
				
一级	二级	三级	四级	五级

表8-3 移动智能终端功能丰富度标识

				
支持一种功能	支持两种功能	支持三种功能	支持四种功能	支持五种功能

说明

圈内黄色线条的个数代表了终端所支持的功能的个数，本处以三级安全功能覆盖等级为例。

Unisoc Confidential For hiar