https://verifone.cloud/docs/application-development-kit-version-50/Release_Notes_ADK_5.0.1.1
Updated: 29-Apr-2025

Release_Notes_ADK_5.0.1.1

Release Notes ADK 5.0.1.1

Released: 2025-04-16

Verifone, Inc.
817 Broadway, Suite 1100
New York, NY 10003 USA
www.verifone.com

Introduction

This document describes the content and changes in the ADK 5.0.1.1 release. It includes details about supported hardware,
components used, major changes and bug fixes as well as known issues and updates to procedures.

A summary of planned or implemented incompatible changes, which may require changes to applications, are provided as an annex.

Please check the installations section, to understand restrictions on downgrading to older ADK versions.

Content

This release provides files as follows:

Product Name	Package Name	Component identifies as
ADK VOS3 download file	adk-vos3-load-prod-5.0.1.1-33.zip adk-vos3-load-dev-5.0.1.1-33.zip	SLP-secure ADK-5.0.1.1 SLP-debug ADK-5.0.1.1
ADK VOS2 download file	adk-vos2-load-prod-5.0.1.1-33.zip	SLP ADK-5.0.1.1
ADK VOS download file	adk-vos-load-prod-5.0.1.1-33.zip	SLP ADK-5.0.1.1
ADK tools	tools-5.0.1.1-33.zip	N/A
ADK Documentation	adk-overview-programmers_guide-5.0.1.1-33.zip adk-doc-5.0.1.1-33.zip	N/A
ADK V/OS SDK	adk-sdk-vos-5.0.1.1-33.zip	N/A
ADK V/OS2 SDK	adk-sdk-vos2-5.0.1.1-33.zip	N/A
ADK V/OS3 SDK	adk-sdk-vos3-5.0.1.1-33.zip	N/A
ADK ANDROID NDK for payment applications	adk-sdk-android-5.0.1.1-33.zip	N/A

Installation

Important note: On any Engage device with battery, please calibrate the battery after installing the new version. Go through a complete discharge-charging power cycle at least once.

To install the new ADK 5.0.1.1, please follow the instructions below:

- **VOS3 on NEO and Vegas devices:**
    - **Installing applications**:
        - To install user applications for ADK 5.0, you must sign download files on the online portal before installing them on the device.
    - **Field update**
        - Please use the download file **dl.adk-5.0.1.1-33-vos3-(neo|vegas)-prod.tgz**.
        - Low bandwidth updates: In case your bandwidth is limited, please check the packman documentation about differential packages. These can be created using this tool only and will result in a smaller download file, which can be used on top of one specific starting version.
    - **Deployment**
        - Please use the download file **dl.adk-5.0.1.1-33-vos3-(neo|vegas)-prod.tgz**.
        - **Passwords:** Verifone recommends to enable passwords during deployment to limit access to control panels and the MAC desktop. Please read the programmers guide sections about passwords.

          Password management requires a password key to be installed on the device, which can be done through VRK or other key loading means.
    - **Development**
        - Please use the download file **dl.adk-5.0.1.1-33-vos3-(neo|vegas)-dev.tgz** to update development devices.
        - For additional debug functionality, use the file **dl.adk-5.0.1.1-33-vos3-(neo|vegas)_debug-dev.tgz**. Note that the behavior of the device may differ from the production version, when running the debug variant.
        - **Note:** VOS3 uses the term "appdev", you can check the state of your device in the info control panel. Development devices are usually provided as devkits and are controlled by dev tokens.
- **VOS2 on Engage devices:**
    - **Installing applications**:
        - To install user applications for ADK 5.0, you must sign its download files on the online portal before installing on the device.
        - In a case you are using license token, you must install these before starting the installation process for applications.
        - Please check the appendix "New user signing for V/OS2" below, and the chapter "Guidance for new user signing feature" in the ADK programmers guide for details.
    - **Field update**
        - **Field update:** Please use the installation file used during deployment for field updates, the default package for payment terminals is **dl.adk-5.0.1.1-33-vos2-engage-prod.tgz**.
        - Low bandwidth updates: In case your bandwidth is limited, please contact Verifone support to provide a trimmed down download file. Be aware, that these are point-to-point version

updates and only work on the requested starting version.
        - **Bases:** Please use the download file **dl.adk-5.0.1.1-33-vos2-base-prod.tgz** to update bases.
    - **Deployment**
        - Please use the download file **dl.adk-5.0.1.1-33-vos2-engage-prod.tgz** to update to this ADK version.
            - Please use the SDI and related download files for other types of devices, or for solutions, which require SDI.
            - **Bases:** Please use the download file **dl.adk-5.0.1.1-33-vos2-base-prod.tgz** for bases.
    - **Important note: We advise to not cut the power during software updates.**
    - **Development**
        - Please use the download file **dl.adk-5.0.1.1-33-vos2-engage-prod.tgz** to update "CP dev" development devices.
        - **Note:** You can check the state of your device in sysmode, development devices are usually referred to as "CP dev" devices.

- **V/OS on Trident devices:**

    - **Important note: Downgrading the SBI boot loader will tamper your device.**
    - **For ADK 5.0 there are two types of buildall files for Ux.**

        - **Original buildall (with SBI included) and no_SBI (new additional buildall). If you use the original buildall file, the latest SBI 3.17.1 or higher will be installed. If you try to downgrade to a build with an older SBI your device will tamper. If you want to keep the old SBI, pre 3.17.1, please use the no_SBI buildall file.**

        - **The Ux diff update package will not update the SBI.**

    - **Deployment and field update**

        - Please use the regular UX download file for both initial deployment and field updates
        - Low bandwidth updates: In case your bandwidth is limited, please contact Verifone support to provide a trimmed down download file. Be aware, that these are point-to-point version updates and only work on the requested starting version.
    - **Important note:**
        - **For better behavior of software installs in case of unexpected power failures, we strongly advice to install software in form of compressed tar download files '.tgz' instead of '.tar' files. This note only applies to the top most layer, the download file, no other changes are required.**
        - **We advise to not cut the power during software updates.**

Solution Package Overview

ADK 5.0.1.1 provides solution files, which combine the operating system, middleware components and EMV kernel in one single loading image.

Please review the supported kernel version list and update your desired file accordingly. You must only enable kernel versions, which are certified for your device, country and customer.
In some cases, due

to included user components, solutions might need to be resigned before loading into a unit.

For more details, please check the ADK programmers guide, chapter "ADK Packages and Update Procedure", in particularly "System Installation Download Files".

Documentation

For detailed information on using any of the ADK features, please refer to comprehensive documentation at adk-overview-programmers_guide-5.0.1.1-33.zip.

Additional files referred to in the programmers guide can be found in the "doc" archive.

Prerequisites/Requirements

Hardware Requirements

This ADK release is for use on production and application development terminal units specified in section "Supported Platforms".

Software Requirements

No special software is required to use this software on a Verifone device. This release provides all required software to operate a terminal, except a payment application.

VHQ server dependencies

- ADKTMS 5.1.5.2 or higher is compatible with the VHQ Server 3.27.01.19
- VHQ XSD version 04.01.0009 is used in this Agent

Application development:

- VOS2 & VOS1: The use of Verifone Development Environment (VDE) is recommended when creating new applications (VOS1 & VOS2 support only).
- VOS3: Please check chapter Developing Applications and in particular the section Development Toolkit VOS3 in the programmers guide for an instruction for compiling applications.

Release Overview

ADK 5.0.1.1 is an intermediate release on top of ADK 5.0.1. This release is focused on VOS3 NEO1 products to provide changes in the payment area.

The release is based on ADK 5.0.1 and is in parity with ADK-4.7.43, ADK-4.8.35 and ADK 4.10.6, as well as ADK-VOS3 2.1.7.

Branch maintenance policy: ADK 5.0 is the new main production branch for VOS1, VOS2 and VOS3 devices and is updated with new features and bug fixes regularly. Please use this branch when creating new customer solutions.

Supported platforms and devices

This ADK release targets the following Verifone products:

- NEO PinPad: P630
- NEO Countertop: M425, M450
- NEO Unattended: UX700, UX700 ML
- VEGAS Unattended: UX302
- Engage: PIN Pad: P200, P200 Plus, P400, P400 Plus, P400 Dual MSR
- Engage Countertop: V200c, V200c Plus, V200, V400c, V400c Plus, M400
- Engage Portable: V200t, V205c, V210, V240m, V240m Camera, V400m
- Engage Mobile: E280 Speaker, E285, E235
- Engage secure devices: CM5, M440, M424
- Engage based full-featured bases: V210, V240m, V400m, T650p, V660p, CM5
- Trident Unattended: UX300, UX301, UX410 and Ux115

Important note: Use CM5, M440 and M424 only in combination with an approved Android OS version. The same requirement applies to Carbon 8 and Carbon 10 using ADK 4.6.

Component Versions

This ADK Release provides following component versions:

- Abstraction:
  - Crypto Abstraction 1.5.0
  - Reader Abstraction 1.7.10
  - Reader Synchronous Cards 1.0.6
- ADK Fonts 1.6.1
- AUTHMAN 0.1.10 - VOS3 Authentication Manager
- Agent - System remote management (e.g. VHQ):
  - AGT 5.1.5.2 - System Remote Agent for VOS1 & VOS2 devices
  - AGT-SUBDEV 4.3.40.2 - System Remote Agent for Android Subdevices (e.g. CM5, M424 and M440)
  - AGT-VOS3 7.5.1 - System Remote Agent for VOS3 devices
- AST 1.9.3 - Anti Skimming Tool
- Base Updater 1.0.2 - Updating base software
- CDD 1.0.3 - Compromise Detection Daemon
- Communication:
  - CCP 1.84.0 - Communication Control Panel
  - COM 2.139.0 - Communication service
  - COMSVC 3.41.0 - Communication Daemon for VOS3
- CPL 2.8.3 - Commerce Platform Library
- EMV CT, CTLS and MSR Card Services:
  - CRD 5.2.144 - EMV service
  - CRD-SYNC 1.3.1 CRD-SYNC service
  - MSR 2.10.5 - MSR service
  - TEC 2.9.6 - Technology selection service
- Certificates:
  - KLDCERTS 1.2.1 - Key Loading Certificates

    - RKLCERTS 1.2.1 - Remote Key Loading Certificate
    - ROOTCERTS 2.0.0 - Root Certificate
- CTLS L1:
    - CTLS L1 Library 1.2.51
    - CTLS L1 K81 Library 1.0.35
- EVT 2.6.18 - Event service
- FPS 1.3.3 - Fingerprint Sensor Library
- GDA 1.0.5 - Global Diagnostic Application
- GUIPRT 2.60.3 - Graphical User Interface service
- INF 1.16.13 - Information Database service
    - SQLITE 1.3.7
    - EXPAT 1.1.9
- INSTALLER 1.3.3.1 - Installer
- IPC 1.31.0 - Inter Process Communication
    - IPC-CFG 1.0.17 - IPC configuration
- ISO8583 1.6.1 - ISO8583 protocol Communication
- KLDLIB 1.3.7 - Key loading library
- LAUNCHER 1.1.1 - Launcher
- LOG 2.21.4 - Logging service
- MDB 0.2.3 - Multi-Drop Bus protocol
- NAV 1.1.0 - Navigator Gateway
- NAVLib 1.6.11 - Navigator Library
- NETLOADER 1.5.7 - Netloader Daemon
- NFC 1.21.4
    - NFC VAS 1.11.2
    - NFC Applepay 1.13.4
    - NFC VWI 1.14.3
- PAWMAN 0.4.4 - VOS3 Password Manager
- PC REGEX 8.41.3
- PERSO 1.3.0 - Ux Personalization
- PP1000 1.3.0.3 - Pinpad communication library
- PRX 3.8.0 - Cloud proxy
- SCP 2.4.2 - Secure Control Panel
- Secure Data Interface - SDI:
    - SDI 4.32.0-258-P2PE-1.6.39 - Secure Data Interface
    - SDI-API 1.18.0 - High level C++ client library
    - SDI-CLIENT 1.33.5 - Compatibilty layer
    - SDI-PAL 4.17.1 - Platform Abstraction Layer for Android and VOS3 platforms
- SEC 2.5.5 - Security service
- SKIMMERDETECT 1.1.0 - Anti Skimming Tool Library
- SLP ADK-5.0.1.1 - Solution package version
- SOUND
    - SOUND 1.2.8 - Sound library
    - SOUND-REC 0.0.0 - Sound Record library
- SSTD 1.2.0 - Secure Service Tool Daemon
- SYSTEM SERVICES components:
    - SYSPROP 1.1.14 - System properties
    - SYSINFO 3.106.6 - System Services
    - SYSMAC 3.85.12 - Multi application controller

    - SYSPM 1.44.27 - ADK Power management
    - VFISYSD 1.1.0 - System Daemon
- VCCI 1.0.5 - Verifone Customizable Cryptographic Interface
- VeriShield Crypto Library:
    - VCL 12.7.6 - VeriShield Crypto Library
    - VCL-VOS3 12.7.7 - VeriShield Crypto Library
    - VCLCP 1.0.2 - VeriShield Crypto Library Control Panel
- VERIFIER 1.0.0 - Verifier
- VFIDIAG 1.0.15 - Verifone Diagnostic
- VOS-MSR 1.3.7 - MSR Decoder Library
- VRK-Agent 1.0.5 - Key Injection Service

Secure Processor (K81):

- SECPROCAPI 1.22.2 - Secure Processor Client API
- SECPROCFW 1.3.16 - Secure Processor Firmware
- SECPROCTOOLS 0.4.19 - Secure Processor Tools
- GPIO 1.2.0 - Secure Processor GPIO API

V/OS:

- SBI 3.17.1 - Secure Boot Image
- OS 32411100

V/OS2:

- OS 32411100-A100

V/OS3:

- Neo NON-HLOS 1.0.0 - Neo non-hlos (non-high level operation system) for modem processor
- ABOOT 1.0.18 - VOS3 NEO Bootloader
- U-BOOT 1.0.0 - VOS3 VEGAS Bootloader
- BSP
    - NEO 2.0.9
    - VEGAS 1.0.0
- OSS 2.2.0 - Open-Source-Software

CTLS:

- **V/OS**
    - VOS_CTLS-4-01.30.03
        - Subversion A4/A5/A6: With Visa MSD and Interac (suitable for the Americas and Europe)
        - With ExpressPay 3.0 / 3.1 and PayPass 3.0.2 / MCL 3.1.1 - Combinations according to release notes
    - VOS_CTLS-4.01.16.13
        - Subversion A4: With Visa MSD and Interac (suitable for the Americas and Europe) - With ExpressPay 3.0 and PayPass 3.0.2
        - Subversion B4: With Visa AP and ePAL (suitable for Asia-Pacific) - With ExpressPay 3.0 and PayPass 3.0.2

- **V/OS2 - CTLS L1**
  - ctls-l1-full-1.2.51 CTLS level 1 library for Engage

Tools:

- PACKMAN 1.7.2 - Tool for managing archives
- Windows USB driver (for Trident, Engage) 5.0.5.2 Build 7

Important Notes

- **From ADK 4.10.0 and ADK 4.8.24 onwards if you downgrade to any older ADK 4.8, 4.7 or 4.6 version you will lose any keys on your device.**

New Features

New features in ADK 5.0.1.1:

- No new features

New features in ADK 5.0.1:

- EMV: Added new CTLS kernel versions for UX410 and V210. Please check the EMV documentation for details.
  EMV: Allow fetching tag 9F09 even for CTLS specifications, which have not defined it.

- Battery: Improve/Refine battery capacity % reporting and removed some redundant charger settings

- Battery related changes:
  - Battery: Charging mode changed to meet specification of power management chip on e235 (applicable only on releases it is supported).
  - Battery: Improved error debugging when dealing with battery temperature.

New features in ADK 5.0.0:

- SEC: Hardened the implementation of file access and use of compression libraries when used by system services; removed telnet library from the default solution

- MSR: Refine MSR reading to support Magnetic Secure Technology (MST) on Samsung S23 and newer models. Note, that this change requires an update of both the SecProc SW and the main controller SW for devices other than Engage.

- Packaging: A new packaging structure for ADK package was introduced, which separates SDK, DOC and download archives. Please check the programmers guide package overview for details. The original full-

ext package is still provided for VOS1 and VOS2 devices

- DOC: The programmers guide now includes a chapter about how to best make use of random functions

- COM: CCP now provides an additional firmware version to identify the radio related software on the main controller

- DOC: The programmers guide has been extended by various chapters from the VOS3 user guide.

- VOS3: VOS3 devices P630, UX700, M425, M450 and UX302 are now supported in regular ADK releases, including an SDK, download files, documentation and tools. Please check the programmers guide for details. In addition the Verifone support team offers a user guide and training.

Fixed Issues

Fixed Issues in ADK 5.0.1.1:

- All VOS3 and Android 10
    - SDI: Delivering DFA138 tag when card is whitelisted in the whitelist.json file with fetchTrxTags (29-02)

    - SDI: getKeyInventory() - returns correct data when ADE KeyAddressTable encryptData list contains 12 or more labels

- Multi-lane
    - Netloader: Added vfi::installer::get_bundle_list() to retrieve bundle information with the "WHO2" command in libnetloader

Fixed Issues in ADK 5.0.1:

- All Engage
    - RADIO: Two new rows have been added to the "Status monitor" table located in "Sysmode - Supervisor - Administration - Communications - GSM" tab.
      The first one shows the name of the currently selected network operator and the second one shows the current network registration status. In the case of roaming, the status will be set to "Registered to foreign network" or "Registered to home network" otherwise.

    - BT: To prevent implicit pairing, the retry mechanism for missing keys is now disabled.

- Sec/VRK: VRKv2 TR31 blocks with filetype "opt hdr ID 02" are now allowed for VOS2 devices, if the filetype matches the one in VRKv2 KBPK
- EMV: Improved handling of the tag DFA13A of EMV_ADK_FETCHTAGS_GET_DATA. Please check the programmers guide for details.
- MSR: Fixed issue that blocked VCL from encrypting MSR data. (Issue occurs with ADK 4.10.5, ADK 4.10.6 and ADK 5.0.0)

- Portable and Mobile
  - VOS-RADIO: Modifications have been made in the case of LTE Attach #11, #12, #13, #14, #15, #22, #35, #42 to ensure compliance with the 3GPP standards.
  - COM:
    Fixed rare cases where COM stack would deadlock during Wifi interface setup
    Enhanced registration status waiting logic in GSM stack
  - SYS: Updated the version of libssh2.so to 1.10.0
  - RADIO: added support for new radio firmware version EC200AAUHAR01A13M16_01.200.01.200
  - PTR: Corrected printer driver issue where it reads an out of range voltage that then caused a printer error message and blocked printing.
  - CP apps: Fixed an issue on VOS2, where MAC becomes unresponsive, if all CP apps are stopped
  - PTR: Improve print quality for V210

- PinPad
  - COM: CCP now allows to configure static DNS servers for dynamic connections
  - COM: Added ability to set user-defined DNS server IP when using PPP with dynamic IP assignment.
  - TOUCH SCREEN: touch config is updated for P630 to support Stylus Pen PN "PPL435-010-01-A"
  - SDK: Expat headers and libraries are now part of the SDK.

    - COM-WiFi: Implementation: After terminal's reboot country domain is set automatically to world regulatory domain 00, which is used to select a behavior (1) or (2).
        - (1) Country Code isn't changed/specified by user. World regulatory domain is configured.
        - Behavior: Country Code can be set automatically during scan procedure or upon a connection to wireless Access Point, if AP is transmitting Country Code information element in Beacon/Probe Response/etc. frames.
        - (2) Country Code is changed/specified by user via ADK-COM API. Then svc-net automatically sets this Country Code upon power on of WLAN module.
        - Behavior: WLAN stack is ignoring Country Code, which is transmitted by wireless AP.
- Desktop
    - RADIO: Fixed an issue, which prevented reading of radio capabilities for a BGS2-W radio module.
- Unattended
    - VCL: Fixed an issue with configuring encryption in VCL.
    - Touch based PIN entry: Improved the switching mechanism for touch based PIN entry to prevent the loss of the initial touch event after returning to normal mode.
- Multi-lane
    - MAC: Fix sporadic issue with MAC init that resulted in UI styling errors including very large button icons

Fixed Issues in ADK 5.0.0:

- All platforms
    - DOC: Fixed issue with VHQ section of Programmers Guide
- All Engage
    - VHQ: Added reporting for AES and 3DES DUKPT online keys to VHQ
    - VHQ: Agent will send AgentReboot only once and subsequent reboots are considered as SystemReboot
    - VHQ: Fixed issue where Agent not handling SIG TERM signal in all cases.
    - VHQ: Fixed issue where scheduling an installation at a later time from download wasn't working.

    - EMV: Fixed the falllback handling for EMV_CTLS_GetCandidateData() in case IIN(E) is not provided by candidate

- All Trinity
    - SDI: Add check for minPanLength and maxPanLength when loading cardranges.json.
- All VOS3 and Android 10
    - SDI: SDI now allows to encrypt card data also for manual card data entry when using VCL
    - SDI: Add check for minPanLength and maxPanLength when loading cardranges.json.
    - CP on appdev: Fixed an issue, which prevented CP apps from starting on appdev Devices
    - VOS3 SDK: Duplicate NFC shared libraries and header files in the SDK have been removed, as VOS3 user application have to make use of SDI instead. For user application migration we recommend to use libsdiclient.a which provides the interfaces for SDI and compatibility to VOS-2 for NFC, TECSEL and MSR. For More details please check the VOS3 Migration Guide and the ADK-SDI-Client Programmers Guide
- Portable and Mobile
    - VHQ: Fixed issue where Agent not handling SIG TERM signal in all cases.
    - BAT: Fixed a bug that has prevented to receiving event on low battery on mobile devices.
    - COM: Fixed an issue where the WiFi interface is not disabled when the last saved network is deleted from CCP database.
    - VHQ: Fixed an issue which prevented installation of JSONKeyBlobs provided by the VHQ server.
- PinPad
    - VHQ: Fixed a sporadic issue in the VOS3 VHQ agent, which prevented SW installation after it's downloaded
- Unattended
    - VHQ: Remove watchdog timer to eliminated reported deadlock situation
- Multi-lane
    - VHQ: Fixed issue where Agent not handling SIG TERM signal in all cases.

- SDI: PAN obfuscated is now added for control request BF01 and BF02 in case VCL is disabled

Known Issues, Limitations and Restrictions

Known Issues:

- No known issues

Restrictions:

- **Hardware support:** Please check the official PCI web page for support of any given hardware.
  This is a new release line and certifications may still be in progress.
  - **In particularly support for UX300, UX301 and UX410 is not available at this point.**
- **From ADK 4.10.0 and 4.8.24 onwards, if you downgrade to any older ADK 4.8, 4.7 or 4.6 version you will lose any keys on your device.**
- **VHQ Agent 5.1.3.x or above should be used with VHQ server 3.24.01.19 or higher.**
- **VHQ Agent 5.1.4.x or above should be used with VHQ server 3.26.01.17 or higher.**
- **VHQ Agent 5.1.5.x or above should be used with VHQ server 3.27.01.19 or higher. Please**
  - Check server version before recommending device software updates (especially on-premise clients).
  - Check version of Agent that will be included in any device software update.
  - Check version of software embedded on any devices before distributing to clients.
- V200t: You must use the latest PVT-3 battery. **Low power modes cannot be used on V200t. The unit may hang**
  sporadically and needs to be rebooted.
- When upgrading to ADK-4.4.17/ADK-4.6.4/ADK-4.7.x/later versions from older versions, it is recommended
  to go through a complete discharge-charge power cycle atleast once after the SW update.
  For later updates,
  example moving from ADK-4.6.12 to ADK-4.7.6 this step is not required.
  If battery is removed and
  re-inserted, it is recommended to go through a complete discharge-charge power cycle at least once.
- The presence of countries with WLAN channels supporting in the list does not indicate that the product is fully approved for use or sales in all listed countries.

Please follow the update procedure above strictly. There are several limitations in older releases regarding the update of units:

- **Engage automated update**: In some cases, the unit may not automatically restart after an install. Please reboot the unit manually in that case.

Appendix:

General notes:

- **For all Base devices:**
    - Devices without user signed VHQ Config - in the field:
        - will receive a sys6 signed VHQ config with current ADK release. This config will set the operating mode to "Direct". Once user decided to install a user signed VHQ Config, a package "dl.VHQconfig-remove-prod.tgz" needs to be installed first. Please contact Verifone service team for assistance.
    - Devices without user signed VHQ Config - out of the box scenario:
        - While installing user signed VHQconfig pointing to customer server, please do not use "ADK operating mode", but "Direct mode" instead.
    - Devices with user signed VHQ Config package:
        - Must ensure that **VHQ config is set to use Direct mode** before installing this version of ADK.
        - During installation of this ADK will see an error message where sys6 signed VHQ config will fail to overwrite existing user signed VHQ config. Please ignore error message.

- **VOS2:**
    - Radio auto-start must be used if the radio needs to be turned off for any reason. Auto-start is the default and it should be retained in this release.

SW Update Capabilities

- **Buildall**

1. Surgical removal - removed OS+sys apps - but not usr apps or keys or OS config; however, network settings will be reverted to default (package "cdgnetcfg").
2. Loaded via USB or as a package i.e. downloadable file via VHQ, netloader, etc...
3. Used at deployment center to change factory VOS into that required by customer.
4. VHQ:
    1. In the past, VHQ device-specific session key was deleted, but fixed in Agent R6 and later.
    2. Currently
        1. Using the normal build all will erase all settings for VHQ.
        2. However, we can technically generate a “upgrader”, (see below) which only erases downgraded components. This should be reviewed in advance for any security breaches (usually there is none), and then be used in VHQ.
        3. However, this is a one off process, i.e. a usual updater request.
5. In most cases, can downgrade, i.e. change to earlier VOS release. Note on MX9, downgrading from release-3014 to something earlier requires special magic, contact i_mx_T3SW for details.
6. This does NOT wipe Warrantied Keys / VRK key.
7. VCL:
    1. in the past, VCL Keys, Configuration Data, and the BIN Table file was deleted with a build-all.
    2. Starting with VCL 9.1.001S (in OS release-31040101) VCL now stores the VCL Keys, Configuration Data, and the Bin Table file into a new folder location so the build-all will not delete these files.

- **Removeall**

    1. Remove file in a bundle - list off what you want to remove. Can remove everything that was loaded via a
       bundle (anything part of manifest) i.e. not anything that apps created.
    2. Secure Installer API - remove bundle names, users (same limitations as remove file via bundle).
    3. Never do a removeall on its own of OS (without OS as part of buildall) because then you'd have no OS.

- **Crtreset**

    1. Tool that uses customer signer card to be able to remove customer app sponsor. Required when device is
       no longer being used by customer.
    2. (info) this is used by customers for their devices (works with customer specific app sponsor only).
    3. Passwords are set to pre-expired such that user is forced to enter new passwords.

- **Upgraders**

    1. Use a script to determine if upgrade applicable, based on current software installed, e.g. VOS release/build string.
    2. "Upgrades", so changes nothing if already on final VOS build, or applied accidentially to a later VOS release/build, i.e. "upgrade to release-30250600" downloaded when release-30410400 running on device.
    3. Script can remove specific files or packages if no longer relevant. E.g. MX9 VOS ADK 2 and ADK 3, FLTK
       and Nano-X were optional packages in their own bundle. For release-3041 it was moved into the core.
    4. During upgrade, a package can be replaced with more-recent version, or altered using **bsdiff** (does binary patching of package). However, **bsdiff** requires a
       specific package version to start with.
    5. Overhead is (at least) one extra reboot that a build-all does not need. This is when the upgrader script runs to decide what to do.
    6. MX9 Upgraders must not change VCL, VHQ and its certificates, CTLS, and not touch vos-syslog-flash
       package.

- **Tamper / VCL Key**

  Note about VCL keys specifically and key versus config in bold below

  In AES DUKPT mode the keys are now handled and stored by the OS so the keys shouldn't be lost during a buildall. But the other VCL configuration settings would be lost temporarily disabling encryption until another VCL config package is installed on the device.

As documented above in the VCL section, configuration data and the keys used in DDK mode have been moved to a new location under VOSCOR-21681 which will be integrated into the OS after QA completes testing. The new location will persist keys and data after a build-all.

- **Permanent Tamper**
  - AKA: TANC (tampered and not cleared) is a tamper that is still physically active e.g. a normally closed tamper switch is open, or a security mesh is broken.
    The source of the tamper must first be fixed in hardware before the terminal can be detampered.
- **Transient Tamper**
  - AKA: TAC (tampered and cleared) is a tamper that was physically active e.g. a normally closed tamper switch opened and then closed, or a security mesh was temporarily open but is now closed.
    By definition, for a transient tamper the source of the tamper has first been fixed in hardware, so the terminal can be detampered.
- **Tamper Handling**
  - Tamper detection and response are done entirely by the hardware, when a tamper event occurs the vault code that deals with the tamper events manages the tampering logs messages and deliver these log messages to the public world.
    A tamper will always reboot the terminal. All secret or private keys, or the key that is encrypting them, are deleted.
    On every boot up, the software determines the tamper status.
    There are two ways the terminal software can respond if the terminal is tampered:
    - Not run any third party applications.
    - Run third party applications but disable all payment interfaces such that payment (or processing of cards MSR, Contact, Contactless, or card data) is not possible.

A terminal may support either one or both of these methods. The configuration of which methods are supported is done at manufacture time by setting a signed Secure Installer variable.

- **Detamper device**

There are two methods to detamper a device, it may support either one or both of these methods.

- Detamper with passwords / direct key load operation.
- Detamper with SST (Secure Service Tool TRSM) / Keyloading via KLD.

The configuration of which methods are supported is done at manufacture time in a MIB (Message Information Block) file. This configuration cannot be changed once set.

Tables:

- **Key Wiping Scenarios**

Symbol	Meaning

? The keys will not be affected in this scenario

? The keys will either be deleted or rendered unreadable and unusable

?? The keys will be replaced with new versions

Key/SW vs Scenario	War-ranty Keys	Cus-tomer Key IPP	Cus-tomer Key ADE 3*	Cus-tomer Key VSP	Cus-tomer Key AES DUKPT	VSS Script Key	Apple/ Google Wallet Key 2*	App	ADK (USR)	ADK (SYS)	OS config	OS	VSS Scripts	Pass-words
Buildall	?	?	?	? 1*	?	?	?	?	?	?	?	?	?	?
Buildall + Remove all User	?	?	?	? 1*	?	?	?	?	?	?	?	?	?	?
Remove all	?	?	?	?	?	?	?	?	?	?	?	?	?	?
Remove all users	?	?	?	? 1*	?	?	?	?	?	?	?	?	?	?
CrtReset	?	?	?	?	?	?	?	?	?	?	?	?	?	?
O/S Upgrade	?	?	?	?	?	?	?	?	?	?	?	??	?	?
ADK Upgrade	?	?	?	?	?	?	?	?	??	??	?	?	?	?
Application Upgrade	?	?	?	?	?	?	?	??	?	?	?	?	?	?
Tamper Event	?	?	?	?	?	?	?	? 4*	?	?	?	?	? 4*	?
CP Dev	Replaced with test keys	?	?	?	?	?	?	?				Replaced with test keys	?	

Notes:

1. In the past VHQ device-specific session key was deleted, but fixed in Agent R6 and later.
2. This is a app key transported via VSS key.
3. Note that ADE requires a FeatureEnablement license token to enable it (in addition to an ADE key).
4. For Brazil ABECS it is a requirement to delete the applications on tamper.
5. Diagnostic counters are always maintained as long as coincell is good (they are in Battery Backed sram).

ADK re-packaging

Status of change

Type of change	Repackaging of full-ext zip archive
New behavior available	ADK 5.0
Planned Deprecation version	ADK 5.1
ADK components	ADK integration and packaging
Changes	The ADK-full-ext zip archive is replaced by SDK archives, a doc archive and platform specific load archives.
Impacts	As a solution provider you may need to update build scripts to use the new zip archives instead of the full-ext zip archive. Transition: The original full-ext zip archive is still available and can be used to simplify the transition.
Reasons for change	With the introduction of VOS3, the size of the ext-full bundle becomes unmanageable large. As some parts are already provided separately, the remaining files will be split, too.
References	Packaging documentation in the programmers guide.

PCI version check

Status of change

Type of change	Add ability verify consistency of PCI versions from sysmode and via API
New behavior available	ADK 4.10 / ADK 4.9
Planned Deprecation version	N/A
ADK components	Installer and sysmode for VOS1 and VOS2
Changes	A new API was added to verify, if the combination of installed components match the expected and certified combination and reported a "tainted" status, if they do not match. The same check is added to sysmode and the PCI version splash screen shown during start up. In addition a NAG screen is implemented on devices with color screens, which will be shown during regular operation, indicating a tainted state.

Impacts	Terminal users should check for tainted status of terminals in the field in a similar way as checking PCI versions. Solution providers must use a full ADK stack to not risk a tainted device or loss of functionality. Application developers can check the status and report to servers or show the status on application status screens. This is particularly important for headless devices like UX300, UX301 or UX410, if operated without UX100.
Reasons for change	Security: Although installations are password protected and should prevent installation of unwanted combinations, the tainted state mechanism was added to counter the increasing complexity of the system and simplify verification of certified version combination.
References	Secure installer interface documentation

secRSAPrivate() / SDI Remote Key Service - will no longer accept RSA keys with key usage 'K3' "Asymmetric Key Pair for Key Wrapping/Key Agreement".

Status of change	
Type of change	Added restriction on key usage.
New behavior available	K81 FW: SPFW_01.**05**.xx.xx (release line: 1.4.x)
Planned Deprecation version	K81 FW: SPFW_01.**05**.xx.xx (release line: 1.4.x)
ADK components	VOS3 / VAOS10
Changes	secRSAPrivate() / SDI Remote Key Service will no longer work with RSA keys with key usage 'K3'.
Impacts	No impact is expected as the ADK provides signing and data decryption functions, but not key wrapping / agreement. Key usages 'D1', 'S0', and 'S2' will continue to be supported. Besides, VRK key profiles reports confirm that no keys with key usage 'K3' were created for that purpose.

	Security:
Reasons for change	Turkey Custom RKL to be implemented in the planned deprecated version, requires loading an RSA key with key usage 'K3' for decrypting the payloads. This RSA key is accessible to apps that can potentially use it with secRSAPrivate() / SDI Remote Key Service to decrypt payloads on the non-secure side.
References	

Packages trying to install files to /mnt/flash via their /home subdirectories would fail to install

Status of change

Type of change	Restrictions enforced on installation packages to make those comply with the Secure Installer specification from the ADK programmer's guide.
New behavior available	All major ADK branches.
Planned Deprecation version	
ADK components	VOS/VOS2
Changes	During installation, Secure Installer prevents installation of files outside the directory tree of a package, even when using symlinks and enforces the behavior described in the installer documentation. • This applies specifically to user home directories like /home/usr1 and affects files in /mnt/flash, even if they are accessible via a symlink from the user home directory. • Secure installer allows the use of symlinks even during installation, as long as all files for usr1 will be extracted to - and only to - the /home/usr1/ subtree. • To install files to /mnt/flash, a dedicated SI installation package with "userflash" type must be used. This means, that the usage of the "flash" directory is not allowed in regular user packages. • Please consult the secure installer documentation for more details Packages not complying with this rule fail to install.
Impacts	Customers using packages that contradict Secure installer specification.
Reasons for change	Reduce the attack surface.

References	dl files can be verified with packman, starting version 1.4 with the validate command "packman.py validate -t vos2 -rd dl.file.tgz"

Remove "Unsigned packages" from VOS/VOS2

Status of change

Type of change	Remove support for installing "Unsigned packages"
New behavior available	ADK 4.10
Planned Deprecation version	N/A
ADK components	VOS/VOS2
Changes	Remove support for installing "Unsigned packages" • Installation packages that do not require signature, used for installing media files to device, will no longer be supported.
Impacts	Customers using "Unsigned packages" will require to use alternative methods for dowloading media files to their application.
Reasons for change	Reduce the attack surface.
References	

Old internal CWK APIs marked as deprecated for the compiler

Status of change

Type of change	Old internal CWK APIs marked as deprecated for the compiler
New behavior available	ADK 4.10
Planned Deprecation version	ADK 4.7
ADK components	VOS/VOS2

Changes	Following VOS/VOS2 internal APIs marked as deprecated for the compiler • cryptoRead • cryptoWrite • cryptoReadWrite
Impacts	Users compiling their applications against old CWK APIs. This should not be done, starting with ADK 4.7. ADK-SEC public APIs must be used instead: • secEncryptData • secDecryptData
Reasons for change	Gradual deprecation of replaced internal OS CWK APIs.
References	

Remove 'voltagesecurity' library from VOS1 build

Status of change

ADK components	VOS1
Type of change	Remove 'voltagesecurity' library from VOS1 build
Changes	Remove 'voltagesecurity' library from VOS1 build
Impacts	No one.
Reasons for change	During upgrade to openssl3 dependencies in 'voltagesecurity' library on VOS1 were identified. No users for the library were identified.
New behavior available	ADK 4.10
Planned Deprecation version	
References	

VOS2 VRK "key name" length limited to 32 chars

Status of change

Type of change	VOS2 VRKv1/VRKv2 "key name" length limited to 32 chars
New behavior available	ADK 4.9
Planned Deprecation version	ADK 4.9
ADK components	VOS2
Changes	User will be able to load only VRKv1/VRKv2 payloads with "key name" field length < 32 chars.
Impacts	VRKv1/VRKv2 payloads.
Reasons for change	Internal legacy OS structures do not allow handling longer key names. This soluiton resolves bugs related to handling of longer key names.
References	

MSR Service removed

Status of change

Type of change	MSR Service removed
New behavior available	ADK 4.9
Planned Deprecation version	ADK 4.9
ADK components	VOS1, VOS2
Changes	MSR is now a middleware component. Using "libvfimsr" is now deprecated, the "libvfimsrwrap" should be used instead.
Impacts	Applications that use msr_svc calls have to substitute these witht he new library. You must use the ADK package to load the SW or lose some of the functionality.
Reasons for change	MSR driver and decoder enhancements
References	

Sysmode file browser removed

Status of change

Type of change	Sysmode file browser removed
New behavior available	ADK 4.9, 4.8, 4.7
Planned Deprecation version	
ADK components	VOS2
Changes	Sysmode file browser exposed files to user that can be used in the vulnerability exploit. Sysmode file browser removed.
Impacts	Sysmode file browser
Reasons for change	Device security
References	

Deprecate ADK-EVENT APIs

Status of change

Type of change	Deprecate ADK-EVENT API on ADK 4.9
New behavior available	
Planned Deprecation version	ADK 5.1
ADK components	ADK-EVENT
Changes	ADK-EVENT component functionality is covered by ADK-IPC API. See the ADK-IPC Programmer's Guide for detailed information.
Impacts	Access to ADK-EVENT API
Reasons for change	Obsolete functionality
References	

Access to the sysmode-www for Bases removed

Status of change

Type of change	sysmode-www removal, new menus on the handset's sysmode to configure a connected base
New behavior available	ADK 4.8.14, ADK 4.9
Planned Deprecation version	
ADK components	VOS2

Changes	• access to the sysmode-www removed from bases
	• new menus on the handset's sysmode added (only Engage handset's):
	  ◦ new menu "Base Config" under the "Administration" if the handset is docked and paired with a base
	  ▪ sub-menu "Date/Time" to configure the date and time on the base
	  ▪ sub-menu "Static IP" to configure the static IP on the base
	  ▪ sub-menu "Unpair all handsets" to unpair all handsets that are connected to the base that is connected to the current handset

Impacts	sysmode-www removed from V400m base, V240m base, V210 base, CM5 base, T650p base new menus on Engage handsets only.
Reasons for change	Vulnerabilities on the sysmode-www
References	

OpenSSL upgraded from 1.0.2 to 3.0

Status of change

Type of change	OpenSSL upgrade
New behavior available	ADK 4.10

Planned Deprecation version	ADK 4.10 Attention: This change will **not** be back ported to existing branches
ADK components	VOS1 & VOS2
Changes	OpenSSL version on the device will be upgraded to 3.0
Impacts	All Engage and Ux users
Reasons for change	• OpenSSL 1.0.2 reached end of life. • OpenSSL 3.0 adds TLS 1.3 support
References	

The minimal sysmode password length now is 7 digits on all Engage and Ux

Status of change

Type of change	Sysmode password length validation
New behavior available	ADK 4.9
Planned Deprecation version	Attention: This change will be not backported to existing branches
ADK components	VOS1 & VOS2
Changes	If the current sysmode password value on a device is less than 7 digits long, then, during the next login the user will be prompted to enter a new password value that is at least 7 digits long. This change affects only users who change the password by password update/reset packages and set the new password that is less than 7 digits.
Impacts	All Engage and Ux users
Reasons for change	PCI and security requirements
References	

Drop networkapps service

Status of change

Type of change	Remove library from default integration
New behavior available	ADK 4.8
Planned Deprecation version	Attention: This change will be backported to existing branches
ADK components	ADK SYS on VOS1 & VOS2
Changes	Remove library integration of "libsvc_networkapps.so" This library was delivered as part of "vfiservices" package in "svcmgrstk" bundle
Impacts	No impact, as not used
Reasons for change	reduce RAM usage, download size and maintenance

References

Remove extra packages from V/OS1 integration

Status of change

Type of change	Remove packages from default integration:
New behavior available	ADK 4.8
Planned Deprecation version	
ADK components	VOS1 ADK integration

Changes	Remove packages from default Ux integration: • skimmerdetect - there is no AST support for Ux units (Mx units are not supported in branches higher than ADK 4.4) • libcpr- commerce platform is disable by default on V/OS1 units • libfps - no finger print scanner on V/OS1 units • libcpapp - commerce platform is disable by default on V/OS1 units The packages libcpr and libcpapp can be loaded with an application, if required
Impacts	Installations on ADK 4.8.x
Reasons for change	reduce RAM usage on UX units
References	

Drop bzip2 compression support for dlfiles/bundles/packages

Status of change

Type of change	Remove of packaging format Bzip2 compressed (extensions: tar.bz, tbz, tbz2) Use Gzip instead (extensions: tar.gz, tgz)
New behavior available	ADK 4.4 and previous releases support tgz and tar
Planned Deprecation version	Attention: This change will be backported to existing branches
ADK components	VOS-SI
Changes	Secure Installer on VOS2 will not support the Bzip2 decompression (extensions: tar.bz, tbz, tbz2) methodology in future for: • dlfile • bundles • packages Use the existing compression methods Gzip (extensions: tar.gz, tgz) instead.
Impacts	Installations on ADK 4.8.x

Reasons for change	Installation time and RAM usage reduction
References	

glib-2 to be removed

Status of change	
Type of change	Shared libraries removal. Gnome Input Output (libgio) will no longer be part of ADK release .
New behavior available	ADK 4.9.x
Planned Deprecation version	
ADK components	VOS-SYS
Changes	The complete glib-2 bundle will no longer be provided in adk release. Backwards incompatible changes: • Any application linking statically or dynamically to one of the following will break: ◦ libglib-2.0.so.0 libgobject-2.0.so libgio-2.0.so libgmodule-2.0.so libgthread-2.0.so
Impacts	Upgrade to ADK 4.9.0
Reasons for change	DL file size reduction to ease migrations
References	

ICWK-encrypted data will be lost on downgrade

Status of change	
Type of change	ICWK encryption scheme will change. Downgrade from ADK 4.9 to older release would lead to loss of ICWK-encrypted data.

New behavior available	ADK 4.9.0, ADK 4.8.24, ADK 4.7.39
Planned Deprecation version	
ADK components	VOS-SEC

Changes	Backwards incompatible changes:
	1. ICWK-protected data will be re-encrypted upon upgrade
	2. ICWK-protected data will be lost upon downgrade to older version
	    1. Warrantied keys (System keys)
	    2. AES DUKPT keys

Impacts	Upgrade to ADK 4.9.0
Reasons for change	Vulnerability closed in ICWK
References	

Weak keys, weak certificate hashes prohibited by default for SSL/TLS

Status of change

Type of change	Default configuration became more strict
New behavior available	ADK 4.8
Planned Deprecation version	**ADK 4.8.x**
ADK components	VOS-SEC, ADK-COM

Changes	• ADK-COM default SSL_POLICY will be updated to reject SSL/TLS connection with server authentication certificates:
	  ◦ With weak key sizes (e.g. RSA certificates<2048bits). Minimum RSA key size is 2048.
	  ◦ Signed using a weak hash (e.g. SHA1, MD5). Only algorithms from the SHA2 and SHA3 family are allowed.
	• Ciphers relying on SHA1, MD5 for MAC removed from OpenSSL default cipher list.
	• OpenSSL 1.0.2 X509_verify_cert() call behavior on VOS and VOS2 will now resemble the behavior for the same call from OpenSSL 1.1.1:
	  ◦ Following error codes were added from the upstream OpenSSL 1.1.1:
	  ▪ X509_V_ERR_CA_KEY_TOO_SMALL, error message "CA certificate key too weak"
	  ▪ X509_V_ERR_CA_MD_TOO_WEAK, error message "CA signature digest algorithm too weak"

Impacts	• SSL/TSL connection. • Certificate verification with OpenSSL.
Reasons for change	PCI requirements. PCI PTS 6 requirement:
References	TD9.2 In the case when certificates are used for server authentication, the tester shall execute tests to verify device behavior when receiving incorrect certificates, including: a) Expired certificates b) Self-signed (un-authenticatable) certificate **c) Certificate with weak key size?e.g., RSA less than 2048 bits** **d) Certificate signed using a weak hash e.g., SHA1 or MD5** e) Chaining error in certificate for cases a, b, c, or d SSL_POLICY: Please check the SSL policy chapter in the ADK programmers guide, section ADK COM for details.

VOS2: "Fixed key" PIN encryption no longer allowed, single DES disabled by default

Status of change

Type of change	Functionality removed

New behavior available	ADK 4.8
Planned Deprecation version	**ADK 4.8.x**
ADK components	VOS-SEC
Changes	In VOS2 IPP M/S the following changes apply: • Loading a master key with KeyUsage P0 is no longer allowed. P0 was required for 'Fixed Key' as the master key encrypts the PIN but now all master keys should have usage 'K0'. • M/S PIN encryption no longer supports 'Fixed Key'/ 'Zero GISKE session key'. So Bit5 of the IPP KMM no longer has any effect in IPP Packet Z60. • Using a single DES GISKE key for PIN encryption is no longer allowed. The session key must be 2key or 3key 3DES, otherwise Packet Z60 will return error '2', work key error. • Using a 'Key Only Format' (KOF) loaded key for PIN encryption is also no longer allowed. Again error '2', work key error, will be returned. • The default KMM for M/S is now 3DES.
Impacts	Key loading and key use for PIN encryption: Fixed key and single DES (see changes above for details)
Reasons for change	PCI 6 requirement
References	

Deprecated open source library headers: Fribidi

Status of change

Type of change	Removal of depricated fribidi library
New behavior available	ADK 4.6.0
Planned Deprecation version	ADK 4.7.0
ADK components	Open source library

Changes	Use of the private library fribidi is depricated since ADK 4.6. The header files have been added back in ADK 4.7 for compatibility reasons, but are still considered private. The library will be removed in a future version, including all header files without further notice,
Impacts	ADK 4.7.0
Reasons for change	• The library is private • It is replaced with a different open source library in most components
References	

Limiting access to diagnostic API

Status of change	
Type of change	Limit access to OS API
New behavior available	ADK 4.8.0
Planned Deprecation version	ADK 4.8.0
ADK components	ADK-SYS, VOS-SEC, VOS-SYS

Access to the OS diagnostic API "diag_counter_get_info" for regular users (usr1-15) is now restricted. Only system users (sys1-15) can access this information.

Use ADK-SYS APIs as an alternative to query system properties.

Values that are restricted:

Exposed by ADK:

- DIAG_COUNT_MSR_READS_ATTEMPTED
- DIAG_COUNT_MSR_READS_WITH_ERRORS_TRACK_1
- DIAG_COUNT_MSR_READS_WITH_ERRORS_TRACK_2
- DIAG_COUNT_MSR_READS_WITH_ERRORS_TRACK_3
- DIAG_COUNT_MSR2_READS_WITH_ERRORS_TRACK_1
- DIAG_COUNT_MSR2_READS_WITH_ERRORS_TRACK_2
- DIAG_COUNT_MSR2_READS_WITH_ERRORS_TRACK_3
- DIAG_COUNT_SMARTCARD_INSERTIONS
- DIAG_COUNT_SMARTCARD_ERRORS

Not exposed by ADK:

- [DIAG_COUNT_ID] = { "ID & Ver Maj,Min",OS,HEX,0,0 }
- [DIAG_COUNT_APPLICATION_FIRST ... DIAG_COUNT_APPLICATION_LAST] = { "App Counter",0,RESERVED,0,0 }
- [DIAG_COUNT_APPLICATION_LAST+1 ... DIAG_COUNTERS_ALLOCATED-1] = { "OS Counter",0,RESERVED,0,0 },
- [DIAG_COUNT_NAND_FLASH_ECC_ERRORS] = { "ECC Error",FLASH,SECRET,0,0 },
- [DIAG_COUNT_NAND_FLASH_ECC_CORRECTED] = { "ECC Corrected",FLASH,SECRET,0,0 },

Impacts	• access to OS API "diag_counter_get_info"
Reasons for change	System vulnerabilities regarding usr1-15 access to secure side
References	Please check the ADK programmers guide under sys info for more details

New user signing for V/OS2

Status of change

Type of change	• Introduction of new user signer cert tree for VOS2 • Licence check for legacy VOS/VOS2 signer cards
New behavior available	ADK 4.8.0
Planned Deprecation version	ADK 4.8.0
ADK components	VOS-SEC
Changes	• Introduction of new cert tree for VOS2 user signing • Added licence check for legacy VOS/VOS2 signer cards • Update 'crtreset' tool to handle new VOS2 user signing certs
Impacts	• Installation of legacy signed application packages will fail, until a proper licence package containing the new VOS2 user signing certificate with matching sponsor was installed on the device • The licence packge with the new VOS2 user signing certificate has to be installed after upgrading to ADK 4.8 and before installing legacy signed application packages • Already installed applications will continue running after upgrade to ADK 4.8 • New 'crtreset' tool has to be used with ADK 4.8 • The changes only affect VOS2 platform. VOS is not affected.

Reasons for change	• Separation of VOS and VOS2 application partition • Only clients with an approved **Software Licensing Agreement** will be able to sign and install applications Future outlook: • Enable Online Signing through Verifone Signing Portal • Retire physical signing cards after moving customers to Online Signing
References	Please check the ADK programmers guide "Guidance for new user signing feature"

Filter environment variables passed to a process when starting it

Change	Filter environment variables passed to a process when starting it
Status of change	
Type of change	• Deprecation of unused functionality
New behavior available	ADK 4.8.0
Planned Deprecation version	ADK 4.8.0
ADK components	V/OS

Changes	• Added blacklist of dangerous environment variables that can NOT be passed to an app when invoked from another user app
	  ◦ Blacklist applies to all 'usr' apps
	• Added whitelist of allowed environment variables that can be passed to an app when invoked from another user
	  ◦ Whitelist applies to all 'sys' apps

Impacts	• usr apps can no longer pass dangerous environment variables from the blacklist to new processes • sys apps can only pass allowed environment variables from the whitelist to new processes

Reasons for change

- Security improvement: Implement proper environment variable filtering using sudo. Allows to prevent certain attacks when new process is started with spoofed system environment variables.

Blacklist:

Environment variable	Description
IFS	
SHELL	
HOME	force-reset by -H or sudoers
LD_*	
PATH	
USER	force-reset by -u or sudoers
USERNAME	
OLDPWD	
PWD	

References

Whitelist:

Environment	Description
ADK_*	Prefix with the wildcard for future ADK environment variables.
GUI_REGION	ADK-GUI region id, which will be used to render application GUI
GUI_DISPLAY	If ARRS is active, this environment stores ARRS IP address and port for communication with Android unit.
MAC_APPID	Application id from manifest file
GUIPRT_APPNAME	Name of the resource folder from manifest file
SDISERVER	SDI server address

Deprecate 'u' (user) engine keys

Change	Deprecate 'u' (user) engine keys
Status of change	
Type of change	• Deprecation of unused functionality

New behavior available	ADK 4.8.0
Planned Deprecation version	ADK 4.8.0
ADK components	V/OS
Changes	• "u" engine keys can no longer be installed to the VOS/VOS2 device
Impacts	• "u" engine keys that can only be installed with VRK • No users of "u" engine keys were found
Reasons for change	• According to PCI PTS K21 requirement unused and/or unnecessary functionality must be removed from the device.
References	

Deprecate legacy Engage 2 piece solution

Change	Deprecate legacy 2 piece solution
Status of change	
Type of change	Deprecation of Engage 2 piece solution in favor of using the SDI 2 piece solution
New behavior available	ADK 4.7.6
Planned Deprecation version	ADK 4.8.0
ADK components	ADK EMV
Changes	Support for legacy Engage 2 piece solution on Engage will be removed
Impacts	Users of the legacy implementation need to use ADK 4.6 and ADK 4.7 maintenance releases, and migrate to the SDI based solution in future
Reasons for change	The SDI based solution provides P2Pe certification and is available accross platforms including new Trinity devices
References	Please check the SDI programmers guide for details

ADK functions and OS APIs not used by ADC applications

Change	Remove ADK functions & OS APIs no longer required.
Status of Change	
Type of Change	Removal of unused ADK functions and OS APIs from OS/ADK bundles.
New Behaviour	ADK 4.6
Planned Deprecation version	ADK 4.6
ADK Components	All ADK components. This will need to tie in with the other ADK changes on this page. The change also applies to the OS APIs in V/OS2.
Changes	• Removal of ADK functions no longer required / used • Removal of OS APIs no longer required / used
Impacts	• Reduced time spent successfully delivering test scripts as part of the OS Quality Improvement project • Smaller OS & ADK bundles - positive benefit to download / boot and extract times for OS/ADK stack in Manufacturing, Deployment & Repair.
Reason for Changes	• 391 ADK functions not used by ADC applications • 2580 Private OS APIs not called directly by ADC applications (care required here as these APIs should only be called internally or by ADK functions) • 244 Public OS APIs not called directly by ADC applications (care required here as additional APIs mnay be called indirectly by ADK functions called by ADC applications) • Avoid unnecessary effort in creating unit tests for all ADK functions & OS APIs that are no longer in use. • Remove unused code from OS/ADK bundles • Improve OS/ADK download times • Improve OS/ADK extraction times
Next Steps	

ADK-SEC-2.0 API changes

Change	Enhancement and restructuring of ADK-SEC
Status of change	
Type of change	New features and redesign of API library, configuration and security component
New behavior available	ADK 4.5

Planned Deprecation version	ADK 4.8
ADK components	ADK-SEC
Changes	• PIN entry functions removed • Changed API to reflect new features • More granular error codes • New configuration mechanism: flexible configurations by one JSON-formatted file, no dynamic changes (functions Sec_Set/GetSecurityConfig() are omitted) • Additional API functions for handling transaction data to provide encryption schemes with supplementary data
Impacts	• Users should use API functions with new interface (libsec.h) • Compatibility layer with ADK-SEC-1.5-interface (libseccmd.h) is provided for the time of migration. These API functions are not fully compatible to ADK-SEC-1.5 as some error codes and functions (Sec_SetSecurityConfig(), Sec_GetSecurityConfig()) are not supported. Old API functions in compatibility layer are marked with attribute 'deprecated' to generate compiler warning when using the old API functions. • Configuration was changed to a JSON-formatted file. ADK-SEC provides a conversion tool (on Windows) to convert legacy host configuration files to the JSON-formatted file.
Reasons for change	• Support of new encryption schemes (Voltage, Visa DSP, RSA) • Signing of ADK-SEC configuration file • Decoupling of Host and VSS script name • Extended key set ID for addressing more key sets • PIN input flexibility
References	see ADK-SEC Programmers Guide especially section 'Migration Guide'

EMV Client Library

Change	**Deliver EMV Client Library only as static library**
Status of change	
Type of change	• Delivery format for EMV CT / CTLS Client Libraries
New behavior available	ADK 4.4.0
Planned Deprecation version	ADK 4.5.0

ADK components	ADK Cards
Changes	• Deliver EMV Client Library only as static library • Remove EMV client shared libaries from ADK. • Two different shared objects (local / client server) are replaced with one static library serving both + a new link shared object. • **Note:** This will only impact EMV CT/CTLS client libs, but no the EMV ADK framework or L2 kernel libraries (still delivered as shared libraries)
Impacts	• Applications need to rebuild the application using the static variant for EMV CT and CTLS client libraries • Use Config API to drive the static lib in client/server or local mode. • Applications that bundled an already existing ADK EMV CT/CLTS client shared lib with their application do not need to recompile immediately, but should upgrade to the static lib variant once they use a new feature of ADK EMV.

Reasons for change	• Users installed new ADK EMV client CT/CTLS shared libs with ADK integration packages and experienced incompatibilities. This has been because of the following:
	  ◦ ADK EMV guarantees source code compatibility but not binary compatibility. This means any extension to the APIs of ADK EMV CT and CTLS client will not require changes to existing application code, but changing the shared libaries for these client libs will break runtime compatibility.
	  ◦ However the compatibility between ADK CT/CTLS client and corresponding framwork shared libries is guaranteed. This means the ADK EMV CT/CLTS framework shared libraries can be changed in the system without recompiling the application that has linked to an older client library.
	• Due to this we recommend users to use only ADK EMV client static library during application binary compilation and linking.

References	

EMV Libraries Installation under System User

Change	EMV Libraries Installation under System User
Status of change	
Type of change	• Install all available EMV kernels under sys and let the user config decide which kernels to use • Install the CTLS EMV framework component for VERTEX or VFI-Reader under sys • Install the CT EMV framework component under sys
New behavior available	ADK 4.5.0

Planned Deprecation version	ADK 4.5.0
ADK components	ADK Cards
Changes	• Remove the requirement to resign the VERTEX EMV kernels with apps signing cards but allow the app to select the needed kernels by config file instead. • Move the EMV framework components to sys
Impacts	• Reorganization of the apps loading packages since VERTEX kernels can not be freely mixed • New linking to be supported by app • Providing config file for certified kernels to use is mandatory for the app. Only app knows which of the (now) all available kernels fits to their local certification
Reasons for change	• Apps complaints to resign the usr kernels with their apps signing cards and creating usr specific bundles on their own • QA requires this process to support apps testing • We need to add protection by config files to avoid that apps using wrong or not certified EMV kernels, which turned out difficult with letting themc reate their own apps kernel bundles
References	see Cards Services - EMV ADK Release Notes "How to migrate to system-signed EMV component" see Cards Services - EMV Libraries Installation under System User

EMV Contactless Configuration Interface for Application Data

Change	EMV Contactless Configuration Interface for Application Data
Status of change	
Type of change	• API deprecation
New behavior available	ADK 4.0
Planned API removal version	ADK 4.5.0
ADK components	ADK Cards

Changes	• Replace global AID configuraition with configuration per scheme • Remove older application data configuration API EMV_CTLS_SetAppliData()
Impacts	• Application AID configuration is now specific for the scheme. Only allowed parameter for the scheme can be used in the APIs. • Applications have to use the new API function EMV_CTLS_SetAppliDataSchemeSpecific() instead of EMV_CTLS_SetAppliData()
Reasons for change	• configuration data from more than 15 different CTLS kernels cannot be mapped to a single configuration parameter set anymore • old API EMV_CTLS_SetAppliData() has been marked as deprecated since ADK 4.0 already. • configuration for new kernels (e.g. Girocard, PagoBancomat, MIR) will no longer be supported with old API function EMV_CTLS_SetAppliData() starting with ADK 4.4.0
References	see ADK EMV programmer's guide for details on the above mentioned configuration functions.

EMV ADK - CTLS LED Handling

Change	EMV ADK - CTLS LED Handling
Status of change	
Type of change	Alternative API
New behavior available	ADK 4.3
Planned Deprecation version	
ADK components	ADK-EMV, ADK-GUI
Changes	• With ADK 4.3 we are introducing an alternative way to show CTLS LEDs on screen.
Impacts	• Users should use the new ADK-GUI function to reserve part of the screen for LEDs (uiShowLEDArea(),uiHideLEDArea() functions) and configure the LEDs layout (uiConfigLEDs() function) • Users should use the existing ADK-EMV callback for LEDs and call the new ADK-GUI function to draw LEDs on screen (uiSetLED() function)

Background:

- On devices w/o physical CTLS LEDs we are emulating those on screen. Due to tight time requirements this cannot be done via the ADK GUI server, but writing straight to the framebuffer to fulfill the timing requirements.
- So far we had the following options in ADK-EMV
  - A) getting a callback and the application can draw the LEDs itself
  - B) let ADK-EMV draw things on its own with limited styling options for the LEDs (only rectangular and circles).
- In some applications CTLS LEDs are required to blink outside the payment transaction ("idle blinking")

Problem:

Reasons for change

- With introduction of Multi-App Controller (MAC) that allows switching between apps and shows CP apps, the direct framebuffer writing causes issues if the payment application doesn't turn this off before switching between applications. The net effect is that the LEDs will be drawn into other applications display regions.

Solution:

- we have now implemented a new API in ADK-GUI to reserve a particular part of the screen for direct frame buffer access
- we have also added APIs to draw LEDs into the defined reserved regions allowing use of PNG image definitions for the LEDs in ON and OFF state. This make things look much nicer in fact.
- The reserved part of the screen will then not be overwritten with any other application content

References see ADK GUI reference guide for the LED Area handling

Discontinue ADK Static Libraries

Change	Discontinue Static Libraries
Status of change	
Type of change	Remove ADK static libs for Verix and V/OS
New behavior available	ADK 4.2
Planned Deprecation version	ADK 4.5
ADK components	

Changes

- Remove ADK static libs from delivery and encourage users to use shared libraries

Impacts	• VOS users have to link against .so files instead of .a files and install the .so file on the terminal
	• Verix Users have to
	  ○ use Verix VSA-type applications only with ADK
	  ○ link against provide .so files instead of static libraries
	  ○ download VLS-type shared libraries to the terminal
	  ○ set the *VSOPATH to reference the shared libs on the device correctly

Reasons for change	• Currently ADK has static libs are provided in the following formats for Verix:
	  ○ no-pic: use with OUT and VSA applications
	  ○ lib-pic: use to link with LIB shared lib files
	  ○ vsl-pic: use to link with VSL shared lib files
	• Also ADK supported VSL-type shared libraries for most of the components
	
	With Verix OS QT000500 the Verix OS supports
	• ○ shared usage of code segments across processes with VSL-type shared libraries
	  ○ dlopen/dlsym/dlclose for late binding that had been possible only with LIB-type libraries before
	
	Due to this there are no need for static libraries any longer and we will retire them to reduce delivery packages and simplify deployment.

References	see ADK Deployment Overview

PIN Entry Handling via ADK-GUI

Change	PIN Entry Handling via ADK-GUI
Status of change	
Type of change	Remove deprecated API
New behavior available	ADK 3.1
Planned Deprecation version	ADK 4.3 (ADK-EMV), ADK 5.0 (ADK-SEC)
ADK components	ADK-EMV, ADK-SEC
Changes	• discontinue the support for PIN entry in EMV and SEC ADK components and replace this with a single PIN entry API for both offline and online PIN in ADK-GUI. • This ADK-GUI API via html and properties has more flexibility and is more powerful to control PIN entry options and PIN entry prompt style. The ADK-GUI API is available since ADK 3.1.

Impacts	Following functions will be discontinued: • ADK EMV: EMV_CT_EnterPIN() and EMV_CTLS_EnterPIN() • ADK SEC: EnterAndEncryptPIN() and EnterAndHoldPIN() These functions were originally introduced because Verix required to have PIN entry in the same task that later on processes the PIN.
Reasons for change	This restriction has been lowered in QT400 (in ADK 3.1) already and now we encourage the use of ADK-GUI for offline and online PIN entry. We had put a note in the ADK-EMV / ADK-SECrelease notes since ADK 3.1 that these APIs will be “will be removed after ADK 4.1.
References	see ADK GUI reference guide for PIN entry handling

Product Overview - Branches

PCI Version: The PCI version listed is only the initially approved version. Please check the official PCI webpage for the currently approved version and availability of LOAs

Product	Development branch	Release branch	Production branch	Active Maintenance	Sustain
UX115	ADK latest	Not supported	ADK 5.0 (3241) PCI N/A	ADK 4.8 (3161) PCI N/A	N/A
V210	ADK latest	ADK 5.1	ADK 5.0 (3241) PCI 6	ADK 4.8 (3161) PCI 6	N/A
CM5	ADK latest	Not supported	ADK 5.0 (3241) PCI 5	ADK 4.8 (3161) PCI 5	ADK 4.7 (3134) PCI 5
M440	ADK latest	Not supported	ADK 5.0 (3241) PCI 5	ADK 4.8 (3161) PCI 5	ADK 4.7 (3134) PCI 5

M424	ADK latest	Not supported	ADK 5.0 (3241) PCI 5	ADK 4.8 (3161) PCI 5	ADK 4.7 (3134) PCI 5
e280(v2)	ADK latest	Not supported	ADK 5.0 (3241) PCI 5	ADK 4.8 (3161) PCI 5	ADK 4.7 (3134) PCI 5
V400m 4G	ADK latest	ADK 5.1	ADK 5.0 (3241) PCI 6	ADK 4.8 (3161) PCI 5	ADK 4.7 (3134) PCI 5
V240m camera	ADK latest	Not supported	ADK 5.0 (3241) PCI 5	ADK 4.8 (3161) PCI 5	ADK 4.7 (3134) PCI 5
e235	ADK latest	ADK 5.1	ADK 5.0 (3241) PCI 6	ADK 4.8 (3161) PCI 6	N/A
e285	ADK latest	Not supported	ADK 5.0 (3241) PCI 5	ADK 4.8 (3161) PCI 5	ADK 4.7 (3134) PCI 5
M400	ADK latest	Not supported	ADK 5.0 (3241) PCI 5	ADK 4.8 (3161) PCI 5	ADK 4.7 (3134) PCI 5
V240m V205c	ADK latest	Not supported	ADK 5.0 (3241) PCI 5	ADK 4.8 (3161) PCI 5	ADK 4.7 (3134) PCI 5
V240 quectel	ADK latest	Not supported	ADK 5.0 (3241) PCI 5	ADK 4.8 (3161) PCI 5	ADK 4.7 (3134) PCI 5

V400m	ADK latest	ADK 5.1	ADK 5.0 (3241) PCI 6	ADK 4.8 (3161) PCI 5	ADK 4.7 (3134) PCI 5
V200t	ADK latest	Not supported	ADK 5.0 (3241) PCI 5	ADK 4.8 (3161) PCI 5	ADK 4.7 (3134) PCI 5
P400 DMSR	ADK latest	ADK 5.1	ADK 5.0 (3241) PCI 6	ADK 4.8 (3161) PCI 5	ADK 4.7 (3134) PCI 5
P200/P400/V200c	ADK latest	Not supported	ADK 5.0 (3241) PCI 5	ADK 4.8 (3161) PCI 5	ADK 4.7 (3134) PCI 5
UX410	ADK latest	Not supported	ADK 5.0 (3241) PCI 5	ADK 4.8 (3161) PCI 5	ADK 4.7 (3134) PCI 5
UX410 high mem MDB	ADK latest	Not supported	ADK 5.0 (3241) PCI 5	ADK 4.8 (3161) PCI 5	N/A
UX30x	ADK latest	Not supported	ADK 5.0 (3241) PCI 5	ADK 4.8 (3161) PCI 5	ADK 4.7 (3134) PCI 5
Ux30x high mem	ADK latest	Not supported	ADK 5.0 (3241) PCI 5	ADK 4.8 (3161) PCI 5	N/A
P630	ADK latest	ADK 5.1	ADK 5.0 (Linux 4.9) PCI 6	N/A	N/A
M425 / M450	ADK latest	ADK 5.1	ADK 5.0 (Linux 4.9) PCI 6	N/A	N/A
UX700 AIO / ML	ADK latest	ADK 5.1	ADK 5.0 (Linux 4.9) PCI 6	N/A	N/A

UX302	ADK latest	ADK 5.1	ADK 5.0 (Linux 5.15) PCI 6	N/A	N/A