

---

ISS Engineering

# Apriva Guard User Guide

Version 0.04  
November 10, 2025

*Submitted by*

*ITC-ISS, LLC*  
7600 N 16th Street, Suite 230  
Phoenix, Arizona 85020

---

**ITC-ISS, A Division of ITC Federal 2014 - 2025**

7600 N 16th Street, Suite 230, Phoenix, Arizona 85020

Phone 703.894.4444 • Fax 802.242.0433 **Notice**

# Important Legal Information

THIS DOCUMENT CONTAINS IMPORTANT TERMS AND CONDITIONS REGARDING THE ACCOMPANYING ITC-ISS (formerly Apriva) PRODUCT. YOUR USE OF THE PRODUCT SHALL IRREVOCABLY INDICATE YOUR ACCEPTANCE OF THE ENCLOSED TERMS AND CONDITIONS. IF YOU DO NOT AGREE TO THE ENCLOSED TERMS AND CONDITIONS, PROMPTLY RETURN THE PRODUCT TO THE PLACE OF PURCHASE FOR A FULL REFUND. ALL RETURNED PRODUCTS MUST BE IN NEW CONDITION, IN ORIGINAL PACKAGING.

## Terms and Conditions

This publication is copyrighted by ITC-ISS, a division of ITC Federal (formerly Apriva ISS, LLC) and is intended solely for guidance use by ITC-ISS customers of the Apriva Guard product line. This publication may not be reproduced or distributed - in whole or in part - for any other purpose without the written permission of ITC Federal, LLC.

The information ITC-ISS furnished in this publication is believed to be accurate and reliable. However, ITC-ISS assumes no responsibility for its use, and reserves the right to make changes to the publication at any time without notice. This document applies to ITC-ISS (formerly Apriva ISS) products and supporting software.

\*Please note that changes in this document reflect only the transition of Apriva ISS, LLC to ITC-ISS, now a division of ITC Federal, LLC.

## Copyright

Copyright © 2014 - 2025 ITC Federal, LLC. All Rights Reserved. This software, manuals, and any copies or derivatives thereof may not be used, copied, modified, adapted, compiled, translated, executed, or provided to any other person or entity except as furnished under a license by ITC ISS or by an entity so authorized by ITC Federal, LLC, and only in accordance with the terms of such license and with the inclusion of the above copyright notice.

# Table of Contents

|                                                  |           |
|--------------------------------------------------|-----------|
| IMPORTANT LEGAL INFORMATION .....                | II        |
| TERMS AND CONDITIONS.....                        | II        |
| <br>                                             |           |
| <b>1 INTRODUCTION .....</b>                      | <b>1</b>  |
| <b>1.1 PURPOSE .....</b>                         | <b>1</b>  |
| <b>1.2 CAPABILITIES .....</b>                    | <b>1</b>  |
| <b>2 ENABLING APRIVA GUARD .....</b>             | <b>2</b>  |
| <b>2.1 ACCESS APRIVA GUARD SETTINGS .....</b>    | <b>2</b>  |
| <b>2.2 VERIFY APRIVA GUARD IS DISABLED .....</b> | <b>2</b>  |
| 2.2.1 READER SELECTION.....                      | 3         |
| 2.2.2 PROTOCOL SELECTION.....                    | 4         |
| 2.2.3 DOD BANNER MODE SELECTION .....            | 5         |
| 2.2.4 ENABLE APRIVA GUARD .....                  | 5         |
| <b>3 USING APRIVA GUARD.....</b>                 | <b>7</b>  |
| <b>3.1 UNLOCKING THE SCREEN.....</b>             | <b>7</b>  |
| <b>3.2 SUCCESSFUL UNLOCK .....</b>               | <b>7</b>  |
| <b>3.3 WEB BROWSER PAGE AUTHENTICATION .....</b> | <b>8</b>  |
| <b>3.4 SCREEN LOCKOUT TIME .....</b>             | <b>9</b>  |
| <b>3.5 TROUBLESHOOTING – USING THE LOG .....</b> | <b>9</b>  |
| <b>3.6 DISABLING APRIVA GUARD.....</b>           | <b>10</b> |
| <b>4 SUPPORTED CARD READERS .....</b>            | <b>12</b> |
| <b>4.1 IDENTIV .....</b>                         | <b>12</b> |
| <b>4.2 GEMALTO .....</b>                         | <b>12</b> |
| <b>5 OBTAINING SUPPORT .....</b>                 | <b>14</b> |

# 1 Introduction

## 1.1 Purpose

Apriva Guard for Android™ employs Public Key Infrastructure (PKI) authentication and login software to control user access to devices and applications that use the Google Android Operating System. ITC-ISS has partnered with device manufacturers to integrate the Apriva Guard for Android™ directly into the Android operating system to provide a strong PKI environment with transparent operation and an excellent user experience. Apriva Guard for Android™ supports U.S. Government Common Access Cards (CAC), Personal Identity Verification (PIV) and Commercial Identity Verification (CIV) cards. These smartcards can be used to unlock the device as well as to provide transparent application-level authentication within the standard Android Java Cryptography Architecture (JCA) Application Programming Interface (API).

Apriva Guard operates on the Google Android operating system. As a result, certain operating system features and functions used by AG – and others that remain user-configurable – are still available after Apriva Guard is enabled. Some of these settings, such as the device's idle timer, lock screen timer, and sleep time, can be configured by the device operator. For more information on these features, refer to official Google documentation or other reputable third-party sources available online.

## 1.2 Capabilities

Apriva Guard is also capable of performing Web Browser CAC authentication and Wi-Fi Protected Access (WPA) Enterprise authentication using a Smartcard. Information on these features is included in sections 3.3 and 3.4.

For device-related issues, please contact your device reseller or OEM directly.

For more information about Apriva Guard, its features, or other related topics, contact Apriva directly using the information provided in Section 5, Obtaining Support.

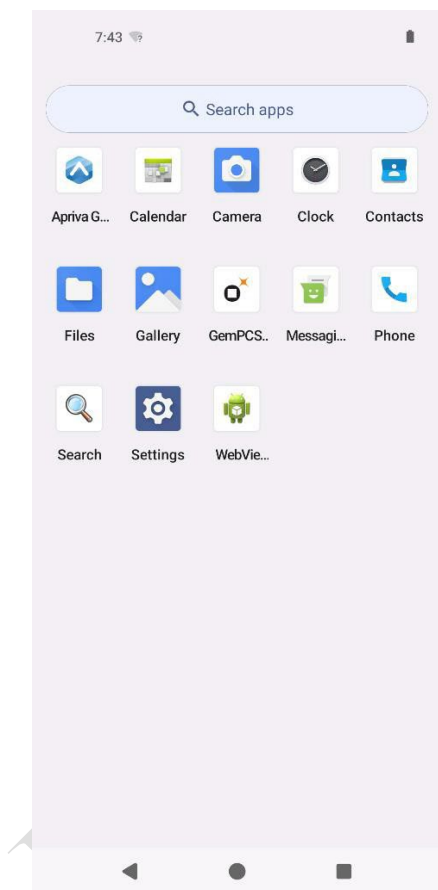
## 2 Enabling Apriva Guard

At initial start-up, Apriva Guard for Android™ is disabled to provide normal unlocked access to the Android platform. The lock screen will be disabled and use of smartcards for authentication will be disabled.

Before you can start using Apriva Guard, it must be properly configured to define the type of smartcard reader you will use, and for some cards with Identiv readers, the smartcard protocol. Follow the steps below to configure Apriva Guard for these mandatory settings. Once the configuration is complete in the **Settings** app, a functioning card reader and smartcard are required to unlock the screen.

### 2.1 Access Apriva Guard Settings

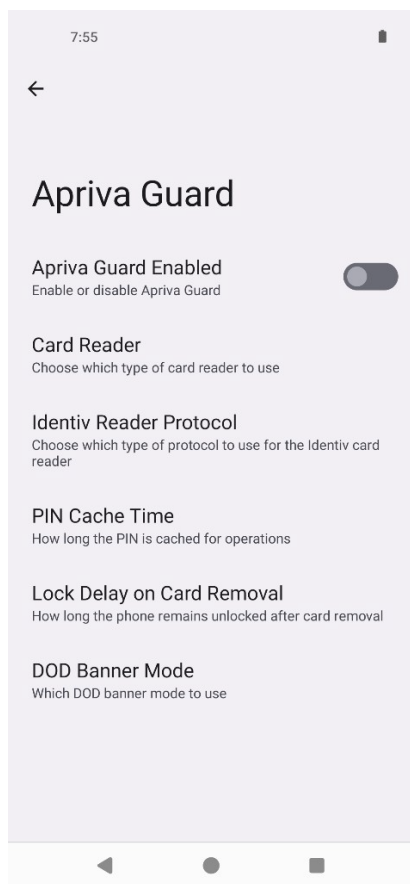
Open the Apriva Guard **Settings** to locate the items requiring proper setup.



### 2.2 Verify Apriva Guard is Disabled

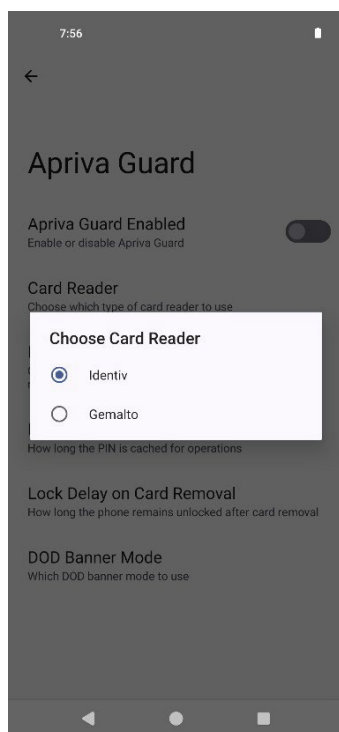
Select Apriva Guard and view the enable/disable switch. Verify the switch is in the left position to disable Apriva Guard. Note that enabling Apriva Guard will immediately lock the device screen before the other items are configured. Ensure that you have both a working card reader and a valid

smartcard that match your selection before enabling, otherwise it will not be possible to unlock the screen.



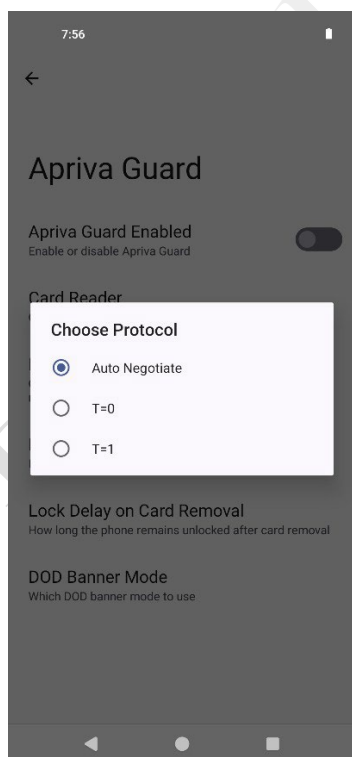
### 2.2.1 Reader Selection

Select the type of smartcard to be read – Identiv or Gemalto.



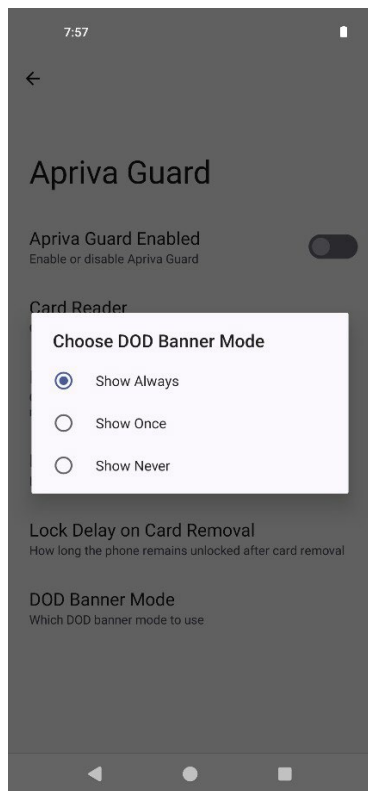
## 2.2.2 Protocol Selection

In most cases, select auto-negotiate (default selection). Note, there are some card types that do not work with auto-negotiate in Identiv readers and require the Protocol to be explicitly set.



### 2.2.3 DOD Banner Mode Selection

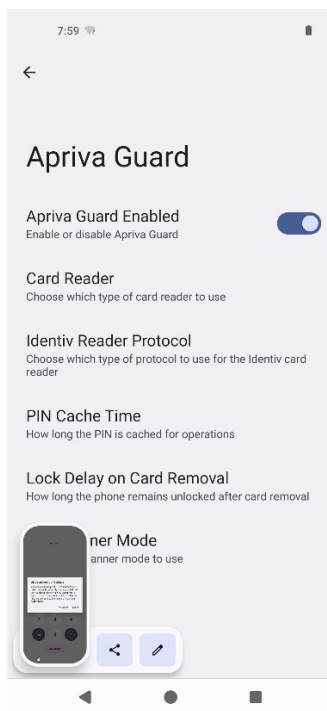
This screen determines how often to display the DOD Banner.



### 2.2.4 Enable Apriva Guard

To use Apriva Guard, it must be enabled. Click the enabled switch to enable Apriva Guard. This will immediately lock the device's screen. Ensure that you have both a working card reader and a smartcard before making this selection because it will not be possible to unlock the screen without these.





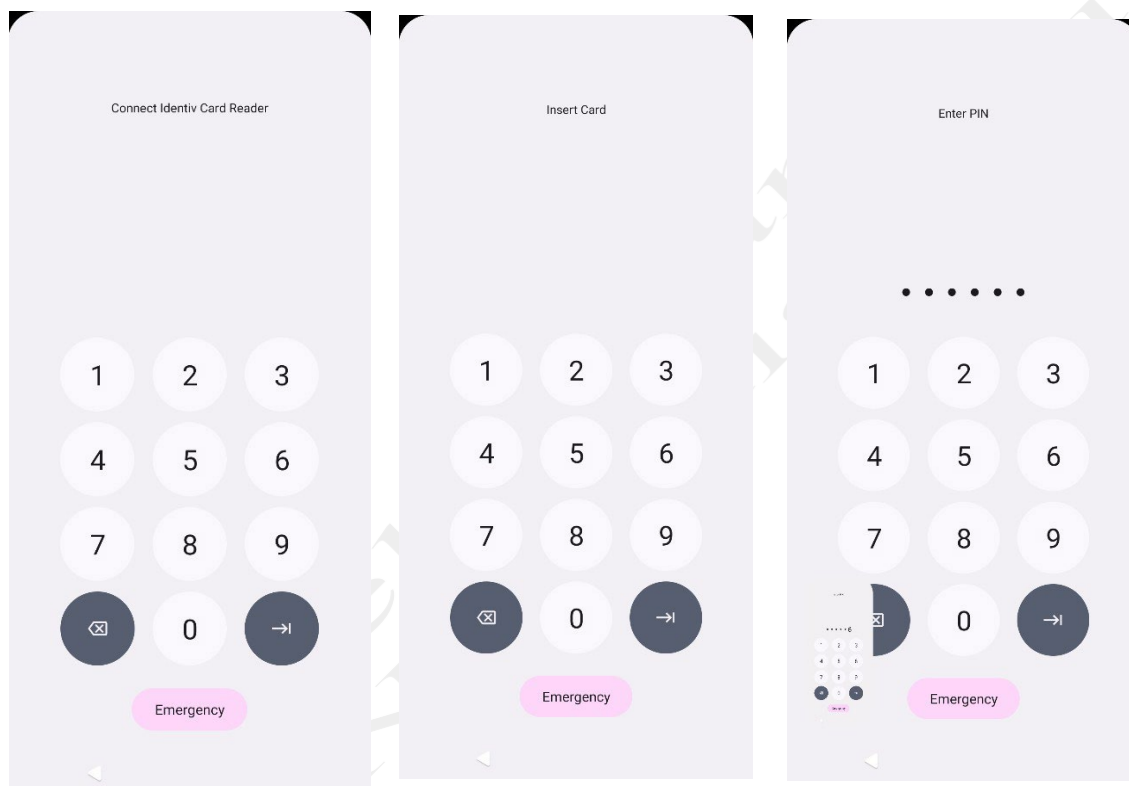
## 3 Using Apriva Guard

### 3.1 Unlocking the Screen

Apriva Guard locks the screen. To unlock the screen, the card reader, smartcard, and PIN programmed on the smartcard are required. The system displays a status, which will change from:

1. Connect Reader
2. Insert Card
3. Enter PIN

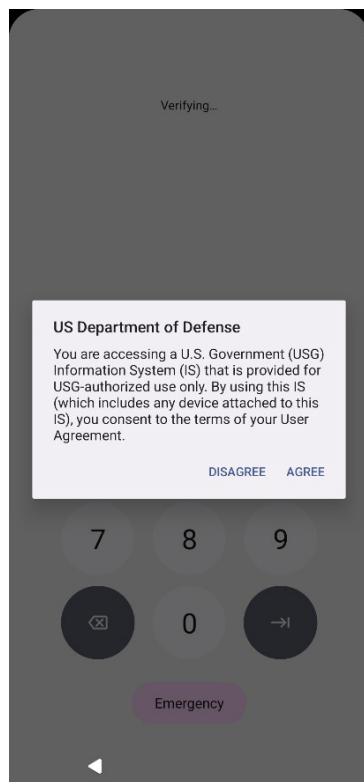
Do not attempt to submit the PIN before the status is Enter PIN.



The status may also display other information, such as errors.

### 3.2 Successful Unlock

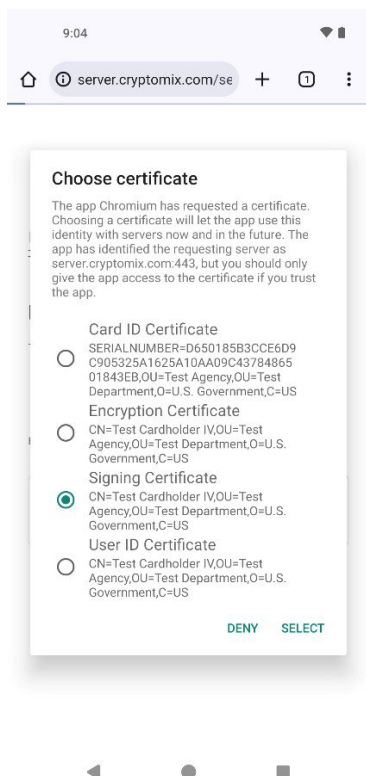
Once the user enters the correct PIN and the device unlocks, the first thing shown is the DOD Banner:



You must agree to the DOD Banner for the system to display the desktop.

### 3.3 Web Browser Page Authentication

To use the smartcard to authenticate to a web page, open a browser such as Chrome, enter the URL, and open the page. The system will display a certificate list. Select a certificate, and the web page will authenticate using the card.

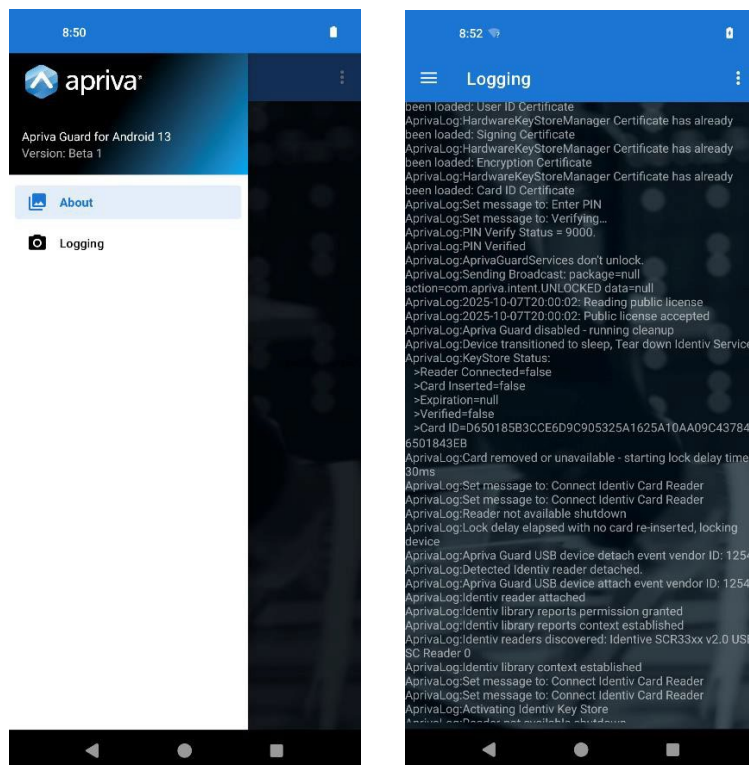


### 3.4 Screen Lockout Time

Apriva Guard is integrated into the Android Lock screen. To select the idle time before Apriva Guard locks, use the standard Android setting. Open the Android Settings and then select the Security item. Click the Screen Lock configuration and select the desired timeout.

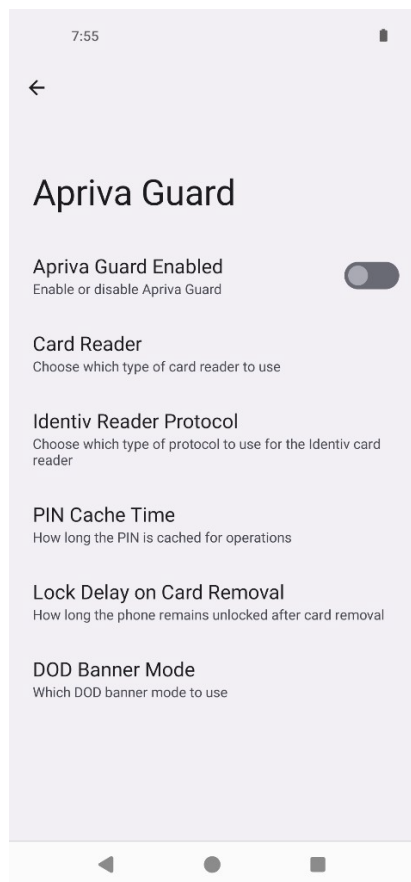
### 3.5 Troubleshooting – using the Log

To troubleshoot a problem, additional information is available in the logs. Open the Apriva Guard app, then select the Logging option. The screen displays the debug log details.



### 3.6 Disabling Apriva Guard

To disable Apriva Guard, return to the Apriva Guard settings, and switch off the Apriva Guard Enabled switch.



## 4 Supported Card Readers

Apriva Guard currently supports two types of readers – Identiv and Gemalto.

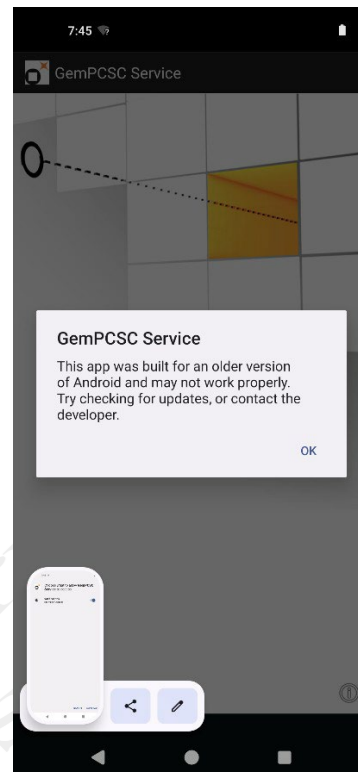
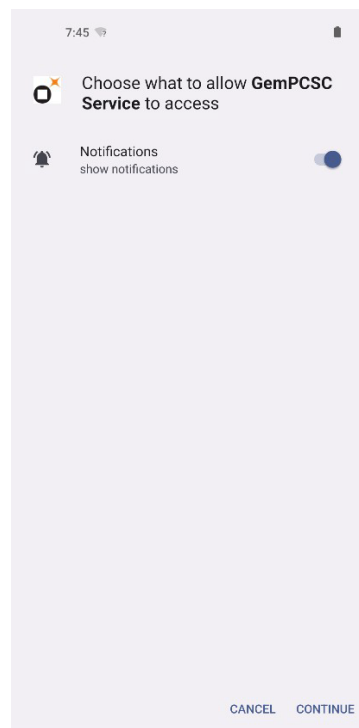
### 4.1 Identiv

Apriva Guard supports Identiv readers such as the SCR3310v2.



### 4.2 Gemalto

When using the Gemalto reader, it is necessary to open the Gemalto service and accept the prompts. This must be done BEFORE enabling Apriva Guard. Find the Gemalto app, open it, and accept the prompts.





## 5 Obtaining Support

Product support and sales information is available from ITC-ISS via the following methods:

- ITC Federal Website (Contact Us)
    - [itcfederal.com](http://itcfederal.com)
- 

DO NOT distribute  
Preliminary: