DEKRA

Whitepaper

Android's Private Space Research and Functional Testing

About DEKRA Digital & Product Solutions

Innovating safety and security by creating the intelligent testing solutions that contribute to making the digitalized and connected world a safer place. We are the experts in testing and certifying products and new digital technologies.

We deliver solutions from Cybersecurity, Artificial Intelligence, Big Data, to Connectivity, Product Safety, Electromagnetic Compatibility & Radiofrequency, Product Certification, Medical Devices and Automotive Testing.

Through a global network of 48 state-of-the-art test laboratories and facilities, we offer a broad portfolio of product testing services based on national and international standards as well as industry and customer requirements.

Would you like more information?

Author and Contact

Juan Manuel Martínez Hernández
juanmanuel.martinez@dekra.com

Contact

Table of Contents

1 Summary

The functional testing of the Private Space feature in Android 15 is designed to assess the robustness of its security mechanisms against potential external and internal threats. Private Space is a key feature that offers users an isolated environment within their devices where they can install sensitive applications, store confidential data, and maintain a separation from the main user environment. Given the rising concerns surrounding data privacy and device security, ensuring that Private Space remains highly secure against unauthorized access is critical.

The goal of this functional testing project is to **assess the core functionalities of Private Space, ensuring that it operates as intended across various scenarios**. Functional testing will validate features such as app management, data isolation, locking and unlocking mechanisms, and the integration with system components like notifications, file sharing, and the launcher. This testing provides Google with third party insights as it builds out additional security and privacy-related features in Android.

2 Theoretical Approach and Objectives

Theoretical Approach

The theoretical approach to this functional testing test is based on a layered security model, which assumes that the Private Space feature operates through a combination of isolation and permission-based access control. Understanding the underlying architecture is essential for this evaluation, as it guides the creation of test cases that target specific components of the system.

Android’s sandboxing mechanism ensures that apps operate in their own isolated environment, but with Private Space, there is an additional layer of isolation. This space is likely implemented as a separate user profile within the operating system. The hypothesis is that any communication or data exchange between Private Space and the primary user environment must be strictly controlled, with minimal information leakage to prevent unauthorized users or malicious apps from gaining access.

Objectives

The primary objective of this functional testing project is to validate that the Private Space feature within Android 15 functions are designed under a variety of real-world conditions. This involves verifying that the core functionalities, such as app management, data isolation, and user interface components, work seamlessly. The testing will cover key areas like locking and unlocking Private Space, ensuring the correct visibility and access of apps, and maintaining data separation between the main space and Private Space.

Secondary objectives include assessing the usability of Private Space from a user experience perspective, ensuring that it is easy to set up, manage, and use on a daily basis. Additionally, functional testing will look at system integration, such as how notifications, file sharing, and app permissions work in conjunction with Private Space, ensuring that they operate correctly when Private Space is locked, unlocked, or hidden.

3 Scope

The scope of the functional testing project includes verifying all critical user-facing functionalities of Private Space, ensuring that the feature works as expected under different use conditions. The following key areas are included in the testing scope:

Private Space Setup and Configuration

Verifying the ease of setting up Private Space from the system settings and ensuring that it can be locked and unlocked using a separate lock factor or the main device lock.

App Management

Testing the ability to add and remove apps from Private Space, ensuring that apps within Private Space remain isolated from the main space.

Locking and Unlocking Mechanism

Verifying the correct behavior of Private Space in locked and unlocked states, ensuring that apps, notifications, and recent app views behave as expected in both states.

Data Isolation

Ensuring that data generated in Private Space (such as downloaded files, photos, and app data) is kept separate from the main space and cannot be accessed or shared unless explicitly allowed.

System Integration

Testing how Private Space interacts with system components such as notifications, file sharing (sharesheet and photo picker), and the launcher to ensure smooth transitions between locked and unlocked states without data leaks.

Usability Testing

Assessing the user experience to ensure that setting up, managing, and using Private Space is intuitive and user-friendly.

State Transitions and System Feedback

Validating that when Private Space changes state (locked, unlocked, hidden), the system components (like the launcher and settings) accurately reflect these changes, maintaining a consistent and secure environment.

The scope will not include penetration testing or any detailed security analysis, as the focus is on ensuring that the feature operates as expected from a functional standpoint.

4 Environment Setup

To ensure a comprehensive and realistic testing process, the functional testing of Private Space will be carried out in a controlled environment that simulates real-world use scenarios. The following elements will be included in the environmental setup:

- An Android 15 device will be set up with the latest available build. Each device will be configured with both a primary user profile (main space) and a Private Space. Private Space will be populated with a variety of apps, including financial apps, social media apps, and file management apps, to reflect typical usage.
- Different authentication methods (PIN, password, biometric) will be tested to ensure compatibility with Private Space locking and unlocking mechanisms.
- As recommended in the private space setup experience, the device was configured with a dedicated Google account in the private space. This setup will be used to test data isolation and interaction across spaces. Accounts will be populated with data such as emails, files, and media to test separation of data between spaces.
- A variety of commonly used apps will be installed in both the main space and Private Space, including apps with high privacy and data security requirements (e.g., banking apps). Different versions of apps will be used to ensure compatibility with Private Space.

5 Functional Testing

Locking and Unlocking Mechanism

Test Case. Verification of Locking Mechanism

Objective

To verify that Private Space locks and unlocks correctly with both the device lock and a separate lock factor.

Preconditions

Private Space is set up on the device.

Separate lock factor is enabled for Private Space.

Test Steps

- Lock the Private Space using the separate lock factor.
- Attempt to access Private Space apps without unlocking.
- Unlock Private Space using the separate lock factor.
- Verify access to Private Space apps.
- Lock the Private Space using the device lock.
- Attempt to access Private Space apps without unlocking.
- Unlock Private Space using the device lock.
- Verify access to Private Space apps.

Expected Results

Private Space should lock and unlock correctly with both the device lock and the separate lock factor.

Apps within Private Space should be inaccessible when locked.

Final Results

Private Space locks and unlocks correctly, and apps within Private Space are inaccessible when locked as expected. It is important to mention that in the below animation the screens goes black because it is the time when user is requested to enter the pin to unlock the private space.

Click here to see Figure 1

Notification Management

Test Case. Visibility in Launcher and Recent Views

Objective

To ensure that Private Space apps are hidden from the launcher and recents view when Private Space is locked.

Preconditions

Private Space is set up on the device.

Private Space is locked.

Test Steps

- Lock the Private Space.
- Open the launcher and verify the visibility of Private Space apps.
- Open the recents view and verify the visibility of Private Space apps.
- Unlock the Private Space.
- Open the launcher and verify the visibility of Private Space apps.
- Open the recents view and verify the visibility of Private Space apps.

Expected Results

Private Space apps should not be visible in the launcher and recents view when Private Space is locked.

Private Space apps should be visible in the launcher when Private Space is unlocked.

Final Results

Private Space apps are not visible in the launcher or recents section while Private Space is locked, and they are visible after Private Space is unlocked as expected.

Click here to see Figure 2

Click here to see Figure 3

Content Separation

Test Case. Separation of User Data

Objective

To verify that user-generated and downloaded content is separated between Private Space and the main space.

Preconditions

Private Space is set up on the device.

User-generated content exists in both Private Space and the main space.

Test Steps

- Lock the Private Space.
- Attempt to access user-generated content from Private Space within the main space.
- Unlock the Private Space.
- Verify access to user-generated content within Private Space.
- Attempt to access user-generated content from the main space within Private Space.

Expected Results

User-generated content from Private Space should not be accessible within the main space when Private Space is locked.

User-generated content should remain separated between Private Space and the main space when unlocked.

Final Results

User-generated content from Private Space apps is not accessible from the main Space when Private Space is locked, and the content remains separated between Private Space and the main space when unlocked as expected.

Click here to see Figure 4

Interaction with System Features

Test Case. Access via System Share Sheet and Photo Picker

Objective

To verify that the system share sheet and photo picker allow access to content across spaces when Private Space is unlocked.

Preconditions

Private Space is set up on the device.
Content exists in both Private Space and the main space.

Test Steps

- Lock the Private Space.
- Open an app in the main space and access the system share sheet.
- Verify if content from Private Space is available.
- Open the photo picker in an app from the main space.

Verify if photos from Private Space are available.

Expected Results

Content from Private Space should be available in the system share sheet and photo picker when Private Space is unlocked.

Final Results

Content from Private Space is available in the system share sheet in the main space when Private Space is unlocked as expected.

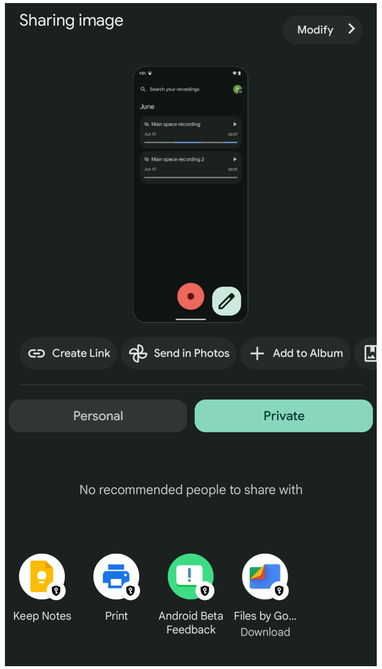

Figure 5. Keep Notes app is only installed in Private Space but is available in system share sheet when Private Space is unlocked

In the same way, when Private Space is unlocked, it is possible for Photo Picker in an app from the main space to access content from Private Space as it is expected.

Click here to see Figure 6

Visibility and Accessibility

Test Case. Verification of Data Isolation with Separate Account in Private Space

Objective

To verify that using a separate Google account for Private Space ensures data and history do not appear outside of Private Space.

Preconditions

Private Space is set up on the device.
A separate Google account is created and signed into within Private Space.
A different Google account is signed into the main space.

Test Steps

- Sign into the main space with the primary Google account.
- Sign into Private Space with the separate Google account.
- In Private Space, use the Google account to perform various activities such as browsing, downloading apps, and saving files.
- Lock Private Space.
- Switch to the main space.
- Open Google services (e.g., Google Photos, Google Drive, Google Search) and verify that none of the activities, files, or browsing history from Private Space appear in the main space.
- Perform various activities in the main space such as browsing, downloading apps, and saving files.
- Unlock Private Space.
- Open Google services in Private Space and verify that none of the activities, files, or browsing history from the main space appear in Private Space.

Expected Results

Activities, files, and browsing history from Private Space should not appear in the main space.
Activities, files, and browsing history from the main space should not appear in Private Space.
Data and history are completely isolated between the two spaces when using separate Google accounts.

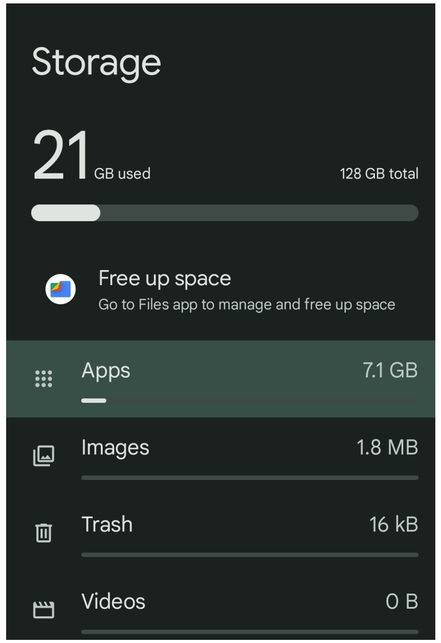

Figure 7. Private Space apps not showing up in main space

Click here to see Figure 8

Final Results

Activities, files, apps and browsing history from Private Space does not appear in the main space when Private Space is locked as expected.

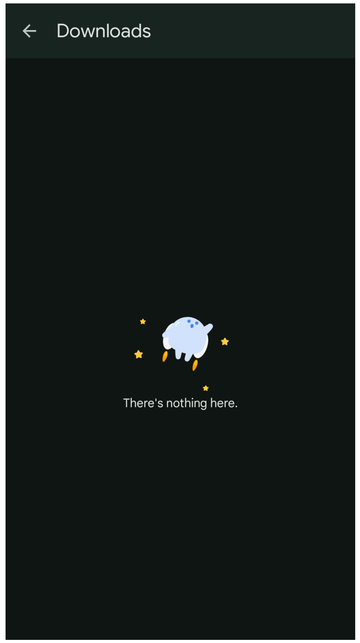

Figure 9. Image downloaded in Private Space not showing up in main space

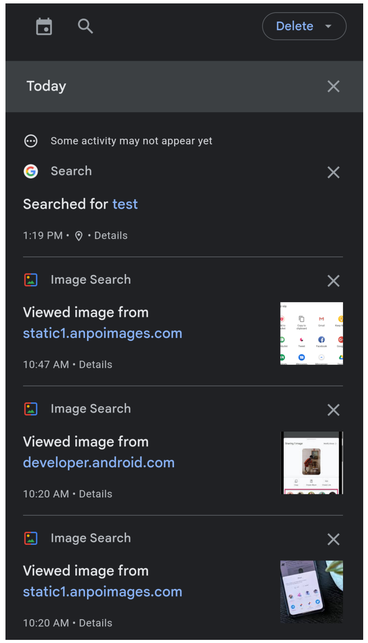

Figure 10. Browsing history from Private Space not showing up in main space

Likewise, activities, files, apps and browsing history from the main space do not show up in Private Space as expected.

The “apps” section in settings separates apps in “Personal” and “Private” as long as Private Space is unlocked. If it is locked, only the apps in the main space are shown and there seem to be no hints of apps from the Private Space.

Additionally, all data and history seems completely isolated between the two spaces when using separate Google accounts.

App Management in Private Space / Handling System Updates

Test Case. App Management in Private Space

Objective

To verify that apps can be correctly added to and removed from Private Space, and that they function independently from the main space.

Preconditions

Private Space is set up and unlocked.
The device is signed in with a Google account in the main space.

Test Steps

Adding Apps to Private Space

- Sign into the main space with the primary Google account.
- Sign into Private Space with the separate Google account.
- In Private Space, use the Google account to perform various activities such as browsing, downloading apps, and saving files.
- Lock Private Space.
- Switch to the main space.
- Open Google services (e.g., Google Photos, Google Drive, Google Search) and verify that none of the activities, files, or browsing history from Private Space appear in the main space.
- Perform various activities in the main space such as browsing, downloading apps, and saving files.
- Unlock Private Space.
- Open Google services in Private Space and verify that none of the activities, files, or browsing history from the main space appear in Private Space.

Removing Apps from Private Space

- Open Private Space.
- Navigate to the app management section within Private Space.
- Remove the previously added app from Private Space.
- Verify that the app is uninstalled from Private Space and does not appear in the main space.

Verifying App Independence

- Re-add the app to Private Space.
- Perform some activities within the app (e.g., login, create files, save settings).
- Lock Private Space.
- Open the main space and install the same app from the Google Play Store.
- Verify that the app in the main space does not have access to the activities, files, or settings from Private Space.

Switching App Usage Between Spaces

- In the main space, perform different activities within the app (e.g., login with a different account, create different files).
- Lock the main space and unlock Private Space.
- Verify that the activities and data within the app in Private Space remain unchanged and independent from those in the main space.

Testing App Updates

- Update the app in Private Space from the Google Play Store.
- Verify that the updated app continues to function correctly in Private Space.
- Lock Private Space and update the same app in the main space from the Google Play Store.
- Verify that the updated app in the main space does not affect the app in Private Space.

Expected Results

Apps should be successfully added to and removed from Private Space.
Apps within Private Space should be isolated from those in the main space, with independent data and settings.
Updates to the app in one space should not affect the app in the other space.

Final Results

Apps are added and removed from Private Space correctly and separately from the main space, and their data is also managed and isolated from the data from apps in the main space as expected.

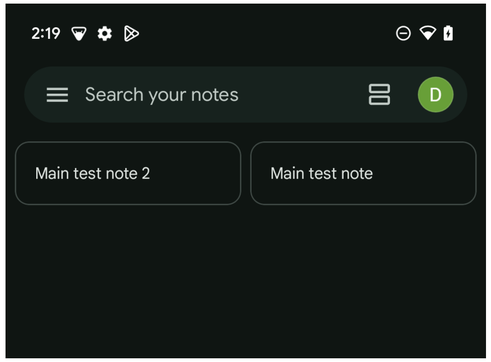

Figure 11. Google Keep app data in the main space

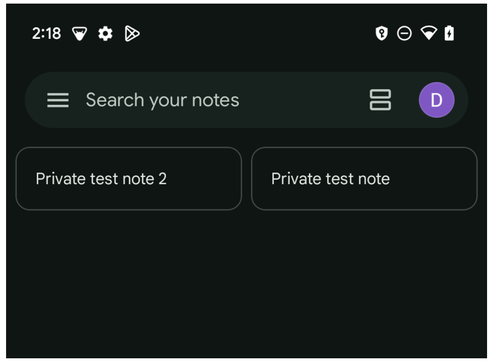

Figure 12. Google Keep app data in Private Space

It seems that updating an app from the Play Store within the Private Space also updates it in the main space.

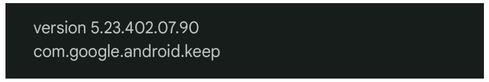

Figure 13. Outdated Google Keep app version in the main space before updating any of the apps

Figure 14. Google Keep app version in Private Space after updating it through the Play Store in Private Space

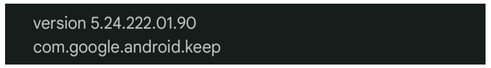

Figure 15. Google Keep app in the main space seems to have also been updated in the process

Cross-Space Sharing Restrictions

Test Case. Cross-Space Sharing Restrictions

Objective

To verify that content cannot be inadvertently shared between Private Space and the main space when Private Space is locked, ensuring data privacy and isolation.

Preconditions

Private Space is set up and unlocked.

The device is signed in with a Google account in both spaces.

Files and media are available in both Private Space and the main space.

Test Steps

Verify Sharing from Main Space to Private Space (Locked)

- Lock Private Space.
- In the main space, attempt to share a file (e.g., via system share sheet) to an app that is installed in Private Space.
- Verify that Private Space apps do not appear as sharing options when Private Space is locked.

Verify Sharing from Main Space to Private Space (Unlocked)

- Unlock Private Space.
- In the main space, attempt to share a file to an app that is installed in Private Space.
- Verify that Private Space apps appear as sharing options when Private Space is unlocked.
- Complete the sharing process and verify that the file is accessible in the target app within Private Space.

Verify Sharing from Private Space to Main Space (Unlocked)

- Unlock Private Space.
- In Private Space, attempt to share a file to an app that is installed in the main space.
- Verify that main space apps appear as sharing options when Private Space is unlocked.
- Complete the sharing process and verify that the file is accessible in the target app within the main space.

Expected Results

When Private Space is locked, apps in the main space should not be able to share content with apps in Private Space and vice versa.
When Private Space is unlocked, cross-space sharing should be allowed, and content should be accessible based on user actions.
Content and data privacy should be maintained with strict separation enforced when Private Space is locked.

Final Results

Sharing data from an app in the main space to an app in Private Space is not possible if Private Space is locked, and possible if Private Space is unlocked as expected.

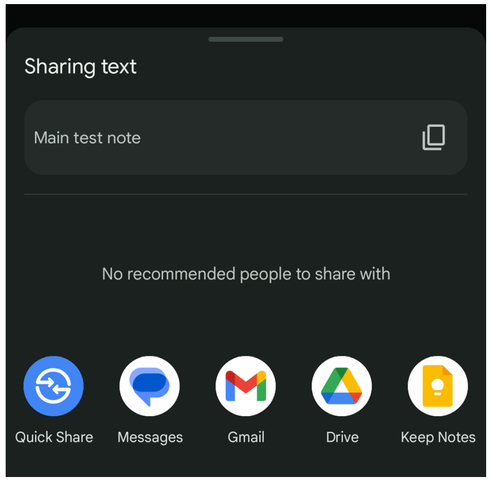

Figure 16. It is not possible to share content from the main space to the Private Space if it is locked

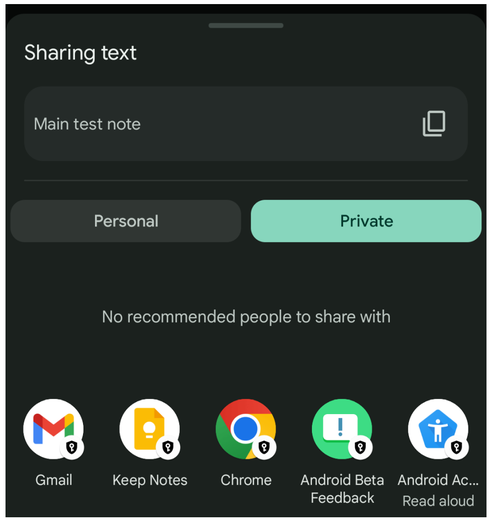

Figure 17. It is possible to share content from the main space to the Private Space if it is unlocked

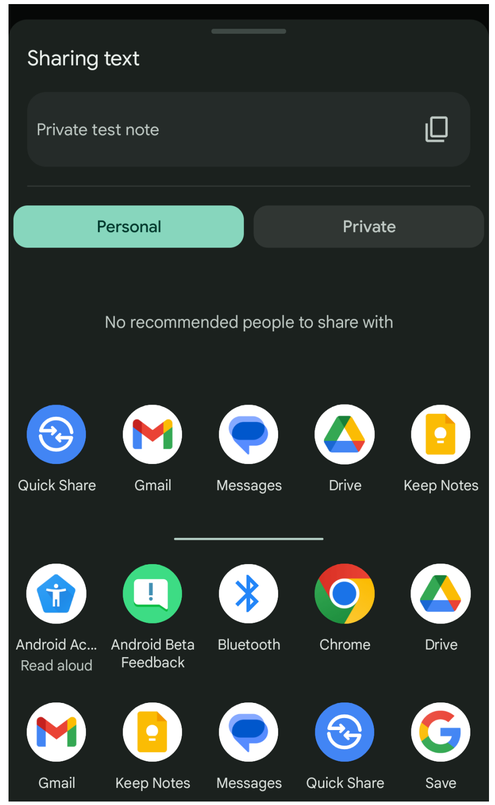

Figure 18. It is possible to share content from the main space to the Private Space if it is unlocked

6 Conclusions

The functional testing of Android‘s new “Private Space“ feature in Android 15 confirms that the system operates as intended, successfully providing users with an isolated and secure environment for handling sensitive data and applications. The testing has validated critical components, such as app management, data isolation, and locking/unlocking mechanisms, ensuring robust security measures are in place.

Private Space maintains a clear separation of data and apps between the primary user environment and the isolated environment, even when system transitions like locking and unlocking occur. Key functionalities such as cross-space sharing restrictions and app independence were tested successfully, highlighting the feature‘s strong ability to prevent unauthorized access.

From a usability perspective, the setup and day-to-day management of Private Space were found to be intuitive and user-friendly, making it accessible to non-technical users while maintaining strict data privacy and security protocols. The seamless integration with system components like notifications, file sharing, and app permissions also supports an uninterrupted user experience across both the main space and Private Space. In conclusion, the functional testing demonstrates that Private Space performs as expected, providing a robust solution for users seeking enhanced data protection and app isolation on Android devices. The feature is well-suited for environments that require high levels of privacy, making it a valuable addition to Android‘s security suite.