# InReality Android OS

# Security Measures

Prepared by:
**Technology Team**
**InReality Ltd**

## Document Version

**Version 3.0 30th Oct, 2017**

This document outlines InReality's Security Measures as it pertains to InReality's media player family of products and associated software utilities and management solutions.

# Table of Contents

# 1. InReality Android Media Players

Over the last three years, InReality has been developing both Android hardware configurations and Android Operating System improvements that allow Content Management Software developers, integrators and resellers to take full advantage of this low- cost media player platform, with the knowledge that these players were purpose- built for digital signage deployments. The InReality media players run a customized version of Android OS.

As a development team that focuses on Android development efforts, InReality has implemented a cadre of updates on the Android source code, kernel, and drivers as well as integration of a watchdog function which virtually eliminates hard failures. This makes InReality's operating system more robust and suitable for digital signage and other enterprise applications

# 2. Android Operating System

The stock Android Operating System consists of a many pre-loaded consumer apps and an Android OS configuration designed for tablets and phones. The preponderance of consumer apps and associated OS configuration create an untenable environment when attempting to run a digital signage application, and more often than not is the root cause for CMS application instability.

InReality has customized the Android Operating System as below

- Customization to kernel and drivers
- Preload only the needed apps
- Customized the Over the Air update management for patches and updates to Operating System
- Disabled the Android Debug Bridge / Debugging mode access
- Custom launcher or Home screen which limits the only whitelisted apps that can be opened or accessed by the users.

# 3. Custom Launcher or Home Screen

- InReality's custom launcher or Home screen only allows the whitelisted apps to be shown on the Home screen.
- Users will not be able to access any other apps or files on the device.
- This provides a level of security from users sideloading other apps or accessing the files on the device.

## 3. Android Debug Bridge (ADB) or USB Debugging is Disabled

USB debugging or ADB is a common method for remotely troubleshooting and debugging an Android platform and as such creates a security vulnerability. It allows users to install apps, as well as push and pull files from the device. InReality's Android OS has the ADB debugging disabled by default to prevent unauthorized access.

## 4. Operating System Updates and Patches Policy

InReality is committed to providing a simple and reliable methodology for keeping its media player family up to date with the latest system patches and security updates. InReality actively monitors the Android community for security vulnerability alerts.

The following below is InReality's process for a release of updates and patches.

- Step 1 - Risk Assessment and Prioritization
- Step 2 - Patch Deployment and Testing in Staging Environment
- Step 3 - Patch Deployment to Production

When an Android OS level security is discovered by the community and becomes available, the patches are integrated into our Custom Android OS and a new Over the Air update package is built. This package is then queued up delivery to the appropriate devices using our Device Management Solution (CDMS) at the scheduled delivery time.

## 5. InReality Device Management Solution (CDMS)

InReality has developed an integral Remote Device Management solution that enables network operators to perform diagnostic and routine maintenance tasks from any browser enabled device.

Software applications (APK's) can be installed, removed or updated through our Remote Device Management solution. Over the air operating system updates are also managed using this utility.

InReality's Remote Device Management solution is deployed on Amazon's Web Services platform and leverages its built-in security features. AWS uses AES 256 Bit encryption for all applications, data storage and communication and all data exchanges are via SSL-encrypted endpoints using HTTPS.

## 6. Support Contact

For further questions or additional support please submit your request here
https://cenique1.zendesk.com/hc/en-us