intertrust®

Distributed trust management for app store diversity

Executive Brief

PKI for IoT

Apps provide a wide variety of new capabilities to computing devices and are especially popular in smartphones. In 2020, a dispute between Epic Games, the studio behind the incredibly popular game Fortnite: Battle Royale, and Apple and Google led to Fortnite being removed from both Apple and Google's app stores. This fueled the long-standing controversy around the near duopoly these two major app stores hold over app developers.

One of the solutions being proposed is for both companies to allow "sideloading," that is, downloading apps from an app store not favored by the device maker. Since then, concern around the risks of sideloading have risen due to the threat of mobile malware. Mobile malware is a concern and has been used to harvest banking credentials and other sensitive information.

The efforts taken to combat malware by Google and Apple are significant and include app reviews, cryptographic signing of apps and verification of those signatures. Public Key Infrastructure (PKI) provided by Intertrust and others assures the authenticity and integrity of these signatures. Hardware measures, such as Qualcomm® security solutions, provide the resilience needed to assure signature verification. Due to this combination of hardware and software protection, mobile systems are some of the most secure ever created.

While the Apple and Google app stores are currently the dominant players, trusted diverse app stores and payment systems have been available for decades. macOS permits sideloading and the Samsung Galaxy app store continues to offer Fortnite for download.

Trust roots for app store providers can be embedded in the OS, and strongly protected by chipset hardware. This model has existed almost since the beginning of e-commerce on the web, starting with Netscape browsers. The concept has proven to be viable and has been applied at scale in the market for protected media for decades.

The mechanisms for designing and deploying distributed multi-party trust eco-systems are well understood. PKI, combined with hardware security measures, can support a plurality of heterogenous systems. Such systems hold the promise of catalyzing a new

ecosystem of multiple app stores that can help incentivize new innovative, trusted and popular apps, benefitting both app developers and consumers.

In fact, with proper integration between hardware security and a supporting key management system such as Intertrust PKI, it is possible for most companies to create and run their own app stores. Many larger companies do so today to distribute internal enterprise applications. The technology also exists for anyone to offer trusted apps commercially to consumers, either directly or through sideloading. Handset makers and device OEMs enjoy a unique relationship with consumers, making them a natural fit to do this. They have the potential to use mature hardware, software, and crypto security technologies to safely and securely offer their customers a wide range of quality apps, ultimately meeting pent up customer demand for the apps they love.

intertrust®

Building trust for the connected world.

Learn more at: intertrust.com/pki-for-iot
Contact us at: +1 408 616 1600 | iPKI@intertrust.com

Intertrust Technologies Corporation
400 N McCarthy Blvd, Suite 220, Milpitas, CA 95035