

Subvert Trust Controls: Code Signing Policy Modification, Sub-technique T1632.001 - Mobile

Archived: 2026-04-02 10:36:26 UTC

Adversaries may modify code signing policies to enable execution of applications signed with unofficial or unknown keys. Code signing provides a level of authenticity on an app from a developer, guaranteeing that the program has not been tampered with and comes from an official source. Security controls can include enforcement mechanisms to ensure that only valid, signed code can be run on a device.

Mobile devices generally enable these security controls by default, such as preventing the installation of unknown applications on Android. Adversaries may modify these policies in a number of ways, including [Input Injection](#) or malicious configuration profiles.

Source: <https://attack.mitre.org/techniques/T1478>