

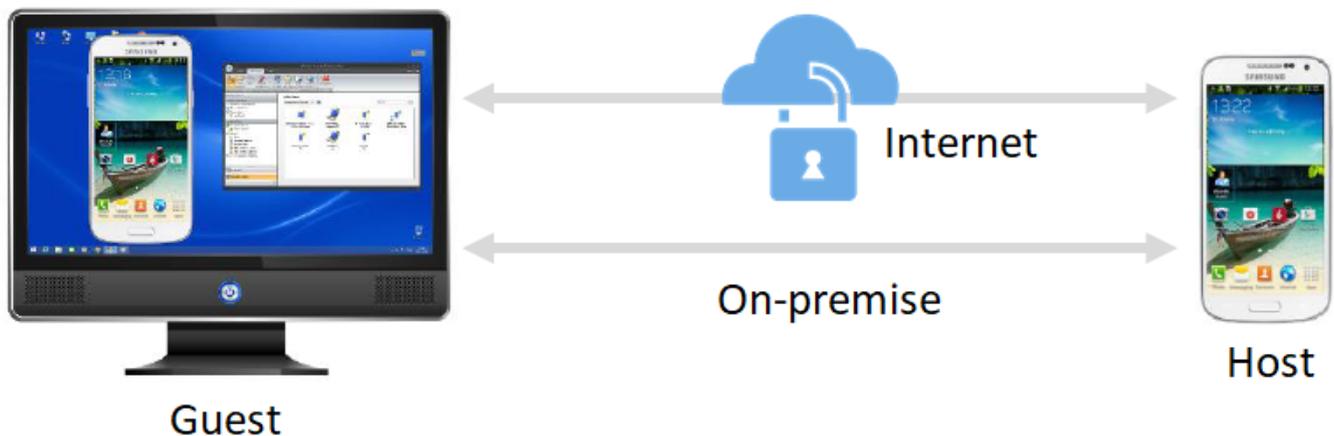
NETOP MOBILE FOR ANDROID – ADD-ON SIGNING

Netop produces remote control software for the Android operating system. In order to capture the screen and inject input, an Add-on component is necessary to bridge the access from the Remote Control Host App to the Android operating system. This Add-on component must be signed by the manufacturer of the Android device.

The outcome is that mutual and future customers will be able to remote control their Android devices.

Technical description

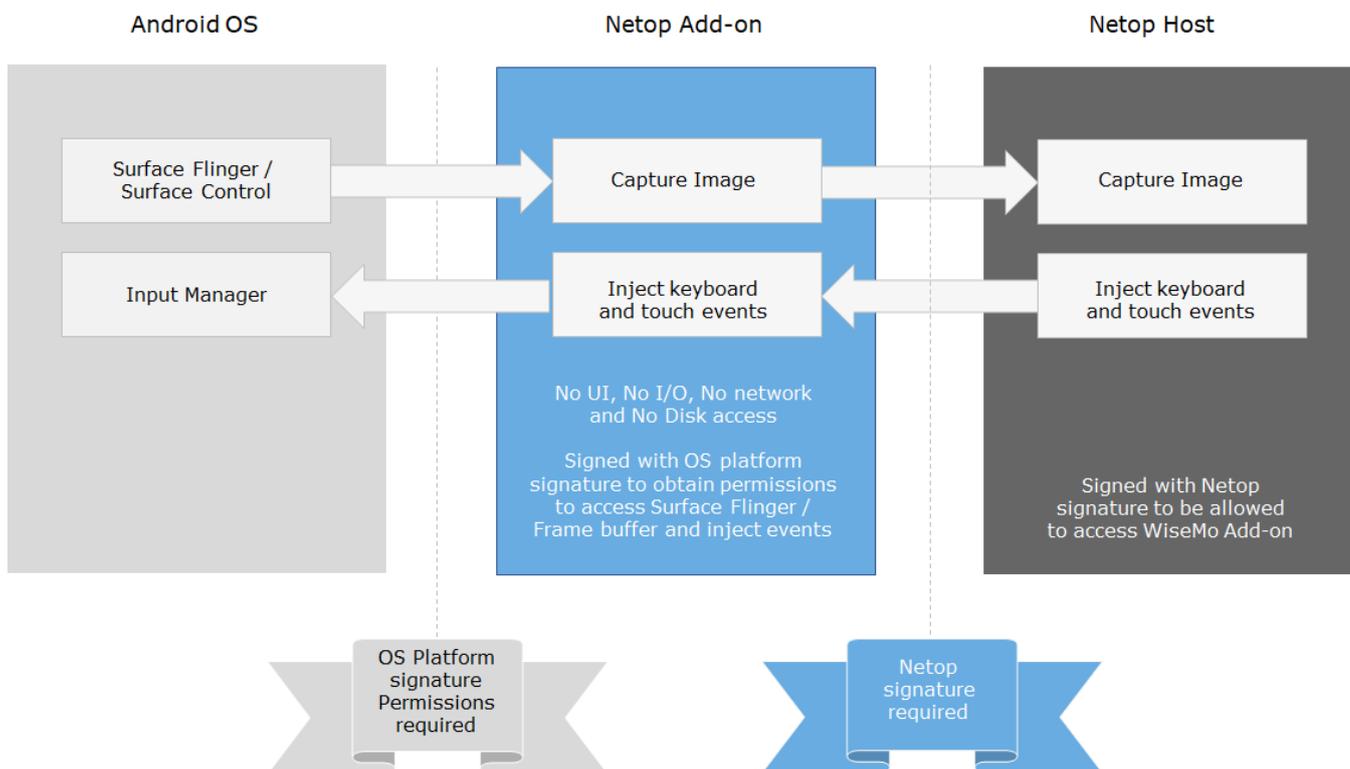
The basic functionality of a remote control product is to capture the screen and simulate input events.



The security mechanism in the Android operating system protects access to certain API functions so only authorized access is allowed. In order to capture the screen and inject keyboard and touch events the Remote Control app needs access to these functions.

This security mechanism works by looking at the identity of the calling App in terms of its signature. So when an app uses these Android API functions the operating system looks at the signature of the app and based on that allows the calls or rejects them. The operating system will allow calls from apps signed with the manufacturer's platform certificate; therefore, the app must be signed with the same platform certificate.

It would be a laborious job to sign the Remote Control App every time it is modified. Therefore, an intermediate Add-on app is used that serves as a bridge between the Remote Control App and the operating system.



The Add-on is very simple. It has the following advantages:

- It rarely changes and needs to be re-signed.
- The less outside interaction it has or does, the more secure it is. Hence there's no UI, no I/O, no network access, no disk access etc.
- It only does what we say it does and it is easy to inspect for a third party.

The signing process of the Add-on is a simple standard process done by a utility that takes the Add-on App as input and produces the signed version. It only takes a few minutes.

Add-on signing in Netop Remote Control for Android

The signing process of the Add-on is standard, done by an utility that takes the Add-on App as input and produces the signed version. It only takes a few minutes:

1. Netop prepares an Add-on APK with a unique Package name (for example *com.wisemo.rcbridge.[manufacturer name]_1*).
2. The manufacturer of the Android device signs the Add-on APK with the platform certificate that is used on the Android devices.
3. The manufacturer sends the signed Add-on to Netop.
4. Netop will verify whether the Add-on is signed for the device in question and if possible have a mutual customer verify it on a physical device.
5. Netop registers the Add-on so it can be automatically deployed and installed by mutual customers.

Note: If a manufacturer uses different platform certificates on the devices that should be supported, the above procedure must be repeated for each platform certificate used.

Questions? We have answers.

Please [contact us](#) for more information.