kaspersky BRING ON THE FUTURE

Kaspersky Mobile Security SDK

Kaspersky Mobile Security Software Development Kit (KMS SDK) is a powerful tool helping you design secure Android and iOS apps quickly and efficiently.

Any safety-conscious mobile app developer should build their products with robust security features. Since designing a truly secure solution requires a specific set of skills that few people have, it often makes more sense to license and integrate a dedicated mobile security product from a universally respected vendor.

Kaspersky Mobile Security SDK is a multi-layered security framework for building online protection directly into mobile applications. All recent versions of Android and iOS are supported.

Use Cases

Third party vendors can use Kaspersky Mobile Security SDK to enhance their products, for instance:

- Provide your customers with the protection needed to keep their mobile devices and valuable data secure
- Make sure any financial data entered in the app stays safe and reaches the intended recipient – and only them!
- Generate alerts if any financial Trojans, password stealers, phishing malware, etc. are detected on the device
- Improve your existing security features and ensure compliance with internal and external policies and requirements

Industry Applications

The following industry branches will especially benefit from deploying Kaspersky Scan Engine:

- Banks and other financial organizations
- Large retail networks that have in-app shopping features
- Car services (rental, sharing, taxi and more)
- Hotel/apartment booking services
- Airlines and rail ticket sale apps
- Governmental services
- And any other solutions with mobile components where use cases include entering or storing the user's financial data in the app

Key Benefits

Kaspersky Mobile Security SDK augments existing mobile applications and allows organizations to secure mobile transactions on devices running Android or iOS operating systems.

Products based on KMS SDK provide protection of mobile devices against known and emerging threats, block access to malicious and phishing websites, and ensure safe financial transactions online.

KMS SDK provides a five step approach to securing mobile transactions. These approaches are logically built to thwart an overwhelming majority of attack vectors against mobile devices and data:

Assess the device

Risky device settings can simplify successful attacks and data exfiltration. Furthermore, some applications can be recognized as malicious based on their behavior or reputation. KMS SDK uses multiple approaches to detect and mitigate the danger.

Protect the device

This group of technologies are 'classic' anti-malware tools designed to prevent malware from infecting the device. These include On-Demand scanner, On-Access scanner, and Application control.

Secure the connection

Internet access can bring many dangers. So you need to make sure the data exchange between the user's device and remote web resources remains secure at all times. These measures include DNS checker, Certificate validator, Wi-Fi safety analysis, and Web filter.

Secure the data

Obviously, mobile users need to input and store sensitive information in all sorts of apps during banking transactions, buying goods online, writing business emails, etc. KMS SDK uses secure input and secure storage to prevent data interception by fraudsters.

Protect the application

Self-Defense provides facilities that protect your application from exploitation by third parties. The self-defense mechanisms allow you to verify the application's digital signature, and to detect debugging and attempts to replace the method operations.

Why Choose Kaspersky Mobile Security?

We're a pioneer in mobile security

Back in 2004, we were the first security vendor to identify mobile malware when we found the Cabir worm. Ever since then, we've continued to build on the head start we had against all other security companies.

The threat landscape for mobile devices keeps evolving – so we keep developing new security technologies. In 2021, we detected almost 3.5 million malicious installation packages, including over 97,000 new mobile banking Trojans and over 17,000 new mobile ransomware Trojans.

Superior detection rates

The quality of the detection technologies that you use can have a significant effect on your anti-fraud operations and your bottom line.

Kaspersky is recognized across the world for its continued innovation in threat detection. We uncover 380,000 new threats every day. So every extra decimal point of worldwide threats that we can detect and block adds up to over a million threats per annum. That's a very sobering statistic… especially when you consider it only takes one successful attack to wreak havoc for a company and its customers.

Boost your systems' effectiveness

Results and findings generated by the Kaspersky Mobile Security can be fed directly into other anti-fraud systems that your company or organization operates. Our granular approach to data feeds ensures you're able to do more than just relay recommendations; you can feed actual results data directly into your systems.

Independently Certified

Don't just take our word! Independent testing labs, such as av-test.org, av-comparatives, and many others, test our mobile products each month, usually resulting in certifications of quality and 'best product' awards.

AV TEST av-test.org 01/2022 CERTIFIED ANDROID

AV comparatives APPROVED Mobile Product 2021

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com

www.kaspersky.com

More Protection Methods

KSN Integration

KMS SDK is fully integrated with Kaspersky Security Network (KSN), a complex distributed infrastructure dedicated to processing cybersecurity-related data streams from millions of voluntary participants around the world. It delivers Kaspersky security intelligence to every partner or customer who is connected to the Internet, ensuring the quickest reaction times, lowest false positive rate and maintaining the highest level of protection.

KSN integration complements conventional security techniques for malware and threat detection, so development teams can ensure their users are protected from the latest mobile attacks.

Multi-layered protection for your mobile customers

Excellent protection starts with excellent detection – and, whereas many vendors rely on just a handful of detection methods, we deliver multiple layers of detection technologies, including advanced heuristics engine and machine learning techniques.

With cybercriminals constantly trying to find new ways to ensure their malicious attacks can slip past conventional security technologies, our multi-layered approach helps us to identify and block new mobile malware and advanced threats.

Device Security Check

Launches several different security checks on the device as a single function, including:

- 'light' anti-malware check
- weak settings scan
- Wi-Fi network safety check
- device root status check

As a result, the user gets a complete overview of device security status.

Data Leak Checker (implementation in progress)

Checks the user's email account for matches in the data leaks registered by KSN.

Greater flexibility to fit your specific mobile application

Unlike other security offerings, Kaspersky Mobile Security includes a vast array of security components and tools that you can use within your application:

- You benefit from having just one SDK to work with – but it contains multiple technologies.
- Our SDK modules and components help you to cover more user security scenarios.

Your data needn't leave your site

By deploying our security technologies as part of your mobile applications, the data that you normally hold on only your site, won't need to leave your site.

Kaspersky Technology Alliances

Kaspersky technologies are offered for integration into third party hardware and software security products and services. All solutions are backed by professional technological partnership support.

Learn more at www.kaspersky.com/oem

Version 21 – March 2022