

Kaspersky[®]

Anti-Spam SDK 3.0

Kaspersky Anti-Spam Software Development Kit (SDK) 3.0 is the most reliable way to add anti-spam functionality to your software and hardware solutions.

Overview

Kaspersky Anti-Spam SDK 3.0 is a set of development libraries that allows integration of the Kaspersky Anti-Spam Engine with third-party hardware or software products. Initially designed for enterprises, the Kaspersky Anti-Spam Engine also meets the requirements of small and medium businesses and service providers. High detection rates of spam and phishing attacks, combined with minimal false positives and exceptional stability, makes the Kaspersky Anti-Spam Engine an ideal spam-filtering solution for all types of customers. The flexible and smart configuration using API and convenient architecture enables the Kaspersky Anti-Virus Engine to be integrated in a variety of software and hardware solutions.

What's new in Kaspersky Anti-Spam SDK 3.0

Kaspersky Anti-Spam SDK 3.0 retains all of the features of the previous version, while offering the following enhanced and new features:

- New generation of the core anti-spam engine:
 - Scans **4X-5X faster** on average with **improved stability**
 - Uses significantly fewer system resources during operation and less network traffic during updates
 - Smart and flexible configuration of KAS SDK 3.0 using APIs
- Perfected filtration methods:
 - **UDS (Urgent Detection System)** has made it possible to block even the newest and fastest-spreading spam through the creation of real-time connections to antispam databases on Kaspersky Lab servers.
 - Improved system for analyzing the IP address of the sender
 - Enhanced subsystem for **analyzing graphic attachments**
 - Use of SPF (Sender Policy Framework) for checking sender IP addresses
 - Additional capabilities for parsing message body and attachments

Antispam Protection Methods

The Kaspersky Anti-Spam Engine does not simply rely upon one single method for the detection of spam and phishing attacks, like many other spam filters which based on statistical and traffic analysis methods (so called zero-time methods). Instead, it uses an optimal combination of multiple methods:

- Blacklisting/whitelisting methods – checking mail for sender IP addresses that appear in DNSBLs (DNS-based blackhole lists), testing links in messages against a database of spam addresses using SURBL (Spam URL Real-time Blacklists).
- Sender identification methods – tests whether a message comes from its claimed source using SPF (Sender Policy Framework).

- Analysis of formal message attributes – header analysis, sender IP address analysis, etc.
- **Linguistic heuristics** – heuristic analysis of message text and attachments.
- Signature analysis – intelligent comparison against known spam templates.
- **Enhanced graphics attachments analyzing subsystem** – fuzzy analysis of image attachments against known graphics spam samples.
- Reverse DNS Lookup – checks for sender IP addresses in DNS

24x7 Anti-Spam Laboratory

Like Kaspersky Anti-Virus, Kaspersky Anti-Spam technology is also supported by human analysis. The team of professional linguists works **24x7x365** to analyze the global spam situation and to develop new spam filtering methods and rules. Why is this important? Only human analysis makes it possible to keep minimal rates of false positives combined with rapid reaction to new spam techniques. The Kaspersky Anti-Spam Engine needs no training, unlike many other anti-spam solutions – i.e., it requires minimal user interaction during setup and operation. The Kaspersky Anti-Spam Laboratory processes enormous quantities of spam, collected from all over the world, adding new spam samples to signature databases and analyzing new spammer tricks. Such human-created signatures and rules allow the solution to detect wide-spread spam attacks, even if the message is slightly changed. This is vital in fighting polymorphic graphical spam, because only humans can create signatures that will cover all varieties of messages sent from a distribution point. The combination of human analysis and the enhanced anti-spam engine provide excellent detection rates and accuracy.

Antispam Database Updates

Updates to the anti-spam databases are released **every 20 minutes**. Kaspersky Anti-Spam database includes not only signatures of known spam, but also new spam-filtering rules and heuristic algorithms. The fact that new spam detection rules and algorithms are also delivered to customers through regular updates, enables Kaspersky Anti-Spam to react on-the-fly to new spam techniques. All signature, rules and algorithms are created by a team of professional linguists, who work 24x7. Usually, it takes an anti-spam analyst several minutes to create a new signature once the new sample is received. Such a signature, created after the analysis of formal message attributes and linguistic analysis of the message body, covers not only a processed spam sample, but a lot of similar spam messages. After creation, this signature is immediately uploaded to the anti-spam database, and new **UDS technology** makes these signatures available to customers almost immediately upon creation. Thus, there is no need to wait 20 minutes until the next database update is released.

Certification and Awards



Kaspersky Anti-Spam 3.0 has been awarded the **Anti-Spam Premium** Checkmark Certification (**97% or higher detection rate**).



Kaspersky Anti-Spam 3.0 was the only commercial anti-spam software to be awarded the Linux New Media Award 2006.

Kaspersky Lab

10/1 1st Volokolamsky Proezd, Moscow, 123060 Russian Federation

Web site: <http://oem.kaspersky.com>; Email: oem@kaspersky.com

Tel: +7 495 797 8700; Fax: +7 495 780 3368