# PeykAsa
# SMS
# Firewall

Higher Protection against SMS Frauds

## Mobile Network Vulnerabilities

During recent decades, the ubiquity of cellular networks and the abundance of smartphones has led to dramatic increase in the number of mobile users. Reports illustrate that the number of mobile subscribers was grown from 4.4 billion at 2015 to about 4.6 billion by the end of 2016. It is also estimated that the number of mobile users will be more than 5 billion by the end of 2020.

This impressive growth in mobile users has introduced the mobile industry as an essential motive force behind the global economy. Reports have shown that the revenue of mobile operators was 1.15 trillion dollars in 2014 and it will be about 1.4 trillion dollars at the end of 2020. This incredible increase in the rate of mobile network revenue declares that the industry is a tempting resource of income even for fraudsters. So like many other profitable industries such as banking, mobile operators should consider hazards of unauthorized access to their network. They should be absolutely certain about the security and impenetrability of any part of their networks. As mobile operators attempt to compensate existing defects in their networks and decline the revenue leakage, attackers also seriously try to exploit the vulnerabilities in the mobile networks.

## SMS Frauds

SMS is a key contributor to fraudsters to help them attack mobile networks and abusing their services. The vast majority of operators in the world usually face various messaging frauds such as:

▶ Spam Messages
▶ Fake SMS/SMSC
▶ SS7 SCCP Spoofing
▶ Special SMSs (Silent, Binary)
▶ Malicious Messages Containing Viruses and Malwares
▶ and so on

## How PeykAsa SMS Firewall Works

▶ Analyzing and Blocking Messages Based on Their Source/Destination Address (and other MAP fields)
▶ Near Real-Time Detection of Trusted Messages among Others
▶ Providing User-Defined Alarms Based on Flexible Thresholds
▶ Applying Advanced and Customizable Filters to Messages
▶ Protecting the Network against DoS Attacks

## PeykAsa SMS Firewall Guarantees

▶ A Secure and Reliable Network
▶ Full Control over SMS Traffic of the Network
▶ High Customer Experience by Protecting Them against Malicious SMSs
▶ Easy Deployment without Any Changes in the Network Topology
▶ Scalable, Flexible and Modular Architecture with Capability of Implementing New Features

## PeykAsa SMS Firewall

**PeykAsa SMS Firewall** address mobile network vulnerabilities related to SMS and allows operator to shield their networks and subscribers from different kinds of SMS attacks and malicious activities. This product is designed based on a multi-level architecture to monitor and control all fields of SMS packets and make decisions regarding them during different steps.

Using customized filters, **PeykAsa SMS Firewall** can recognize trusted packets and delivers them to the related receivers; whilst it hands over remained packets to the next level for more processing. In order to detect malicious packets as soon as they arrive at the network, **PeykAsa SMS Firewall** should be installed at the edge of the network to catch any packet before it can be spread over the network. The following image shows the topology of mobile network with SMS Firewall protection. The product sits on the edge of the network to capture any incoming SMS packets.

**PeykAsa SMS Firewall** is a transparent node; so other elements in the network know nothing about its presence. It does not manipulate safe messages and just forwards them to the next node, but for suspicious messages, it blocks them and adds the source number to the black list.

Spam detection process is done during multiple complicated steps using advanced statistical algorithms, artificial intelligence and data mining algorithms. This solution is equipped with various in-house developed text mining algorithms and utilizes them in a parallel way to decrease processing time for some special kinds of spam messages.In this way, the architecture provides a near real-time, high precise mechanism for recognizing safe packets.