



Russian Railroads Booking System

History

"Express – 3" is the successor of the „Express – 2" booking system, which handled all online ticket operations of the Russian Railroads. "Express – 2" was based on the use of dedicated lines, which connected the regional service centres (8 in total) with the travel agencies responsible for reservations and bookings for customers of the Russian Rail.

The main downsides of „Express – 2" were:

- high costs due to subscriber fees of the dedicated lines.
- lacking flexibility to allow the use of terminals connected through a dial-up connection (i.e. Modem).
- smaller agencies lacked the funds to support a dedicated line. As a result only the huge travel agencies were connected to „Express – 2".

In 2002 the Russian Transport and Rail Ministry set an order for "Express -3". Transactions and communication between the terminals and regional centres were required to be routed over open networks of private ISPs (i.e. Internet).

To comply with these requirements, the future „Express – 3" system had to feature a number of IT-security aspects. The system needed to be safe from attackers on the net trying to gain access to the network to gain customer information, or fraud the "Express – 3" system for tickets, etc.

After intensive comparison with the competition, the ministry chose the ViPNet Solution for several reasons: ViPNet is very scalable and flexible – instead of needing to buy additional security appliances to connect between the terminals and the network, or to have long-term negotiations about implementing a VPN agent in devices proposed by CISCO and other competitors. The ViPNet [Client] was implemented on "Express -3" terminals (based on Linux or Windows XP Embedded) with ease and without any delays.

Requirements

The ViPNet [Custom] solution solved all requirements of the „Express – 3" system including but not limited to:

- securing all TCP/IP traffic between the terminals and the mainframes in the regional centres. This makes „man-in-the-middle" attacks virtually impossible. That way it is not possible for an attacker to i.e. order tickets in the name of someone else.
- securing the mainframes in the regional centres from attacks from the internet; authenticate connection attempts from registered terminals; and a mechanism to validate the transactions, queries and orders from terminals. The ViPNet [Coordinator] component handles all these tasks after being installed in the regional centres. It handles all tasks to authenticate and validate all queries from the travel agencies' distributed terminals which are equipped with the ViPNet [Client] component. Furthermore ViPNet [Coordinator] implements a powerful network monitoring.
- securing the „Express – 3" terminals from attacks from the inter- AND intranet to „spoof/fake" authorized use of a registered terminal to gain all the possible advantages a successful attack would give the attacker. The security of the terminals is managed by the ViPNet [Client] component. It encrypts the TCP/IP traffic, authenticates and filters in- and outbound traffic by a huge amount of criterias, as known from "best-of-breed" desktop firewalls.

The flexibility of the client-based solution of ViPNet was one of the most important features to choose ViPNet in favour of the countless amounts of other products.

The security guidelines of "Express – 3" shows a terminal as a regular PC without the usual media (i.e. hard drive, cd drive, etc.). Instead an „on-chip“ flash memory incorporates the OS (Linux or Windows XP Embedded), the booking software and ViPNet[Client]. The individual keys for the call center agents, are saved on an USB-stick, which the agent is required to connect to the terminal to be able to authenticate in the system. This double-authentication allows the monitoring of actions made by a certain user or terminal.

Solution

The following 3 main features of ViPNet:

- full blown VPN solution
- a set of distributed firewalls
- integrated PKI (Public Key Infrastructure) system

allowed to solve three problems with one single integration task:

- create a VPN for the „Express – 3“system – successor for the old system based on expensive dedicated lines
- ensure the safety of all connected „Express – 3“network components from malicious attacks from the Inter- and intranet
- create a stable authentication mechanism to authorize the single network components of „Express – 3“

Facts about „Express – 3“:

- 7 000 terminals in 2004
- 40 000 terminals by end of Ende 2005