Case study

Strong Authentication

Background

Teva Pharmaceutical Industries Ltd. is a leading global pharmaceutical company and the world's leading generic drug maker, with a global product portfolio of more than 1,000 molecules and a direct presence in approximately 60 countries. Teva's specialty medicine business focuses on CNS, oncology, pain, respiratory and women's health therapeutic areas as well as biologics. Teva currently employs approximately 45,000 people around the world and reached $20.3 billion in net revenues in 2013.

The Challenge

Teva's employees were remotely accessing the organization's systems and restricted resources with the use of a username and a password only. This constituted a large threat to the IT security infrastructure of the organization. The challenge was to improve the IT Security of the organization with strong authentication while providing an easy to use solution. The goal was to advance to a strong access control authentication tool - a two factor authentication: something you have (token, smart card, smartphone) and something you know (password).

The solution

Implementing the RSA One Time Password (OTP) SecurID system, for approximately 25,000 global Teva employees engaged in various Teva companies around the world: USA, Hungary, Mexico, Brazil, Peru, UK, Japan, Spain, India, Israel and Czech.

The system enables remote access to the companies' servers through the use of a unique PIN code that changes every 60 seconds – which adds an additional safe level to the regular access means. The identification is based on a two-factor authentication and in such way provides a more trustworthy level of identity authentication than using a user and password identification method solely.

By implementing the SecurID solution in Teva, a strong authentication of the organization's users was achieved, with a more controlled remote access to a wide range of critical organizational systems.

The solution at Teva is a software solution that has various implementation options - a virtual token with a smartphone application, an SMS token with a PIN code sent to the mobile as a text message or a SecurID hardware token. When using software solutions, users have the luxury of being able to use their own, mobile resources, with no need to carry around any token or other device. Only a small part of the solution implemented at Teva is hardware in the form of a physical token withholding a constant changing PIN code (every 60 seconds).

Results

- ✓ An enhanced IT Security and controlled remote access to the organization's systems
- ✓ An additional means for protecting the organizations' resources
- ✓ A strong identification verification of users
- ✓ Simple and intuitive to use

comsignTRUST
Stands for your Values
www.comsigntrust.com

Corporate Headquarters
Tel: +972 3 648 5255
sales@comsigntrust.com