SECURITY

IDENTITY MANAGEMENT AND
USER AUTHENTICATION
The main advantage of using multi-factor authentication mechanisms is an improved security of IT-infrastructure, applications and data.

A strong multi-factor authentication is simple and widely applicable (remote VPN access, monitoring of access to applications and systems, or digital transaction signatures). Authentication allows organizations more confidence in the identity of users who use their information systems and services. This also means less business risk (lower risk from unauthorised access and misuse).

Multi-factor authentication system is not only reliable, but also easy to use for end users. This leads to lower user support-related costs, while users lose no time while adverse events are prevented.

Only a secure information infrastructure can be truly reliable and serve as an efficient platform for ensuring the smooth functioning of business processes.

Authentication, i.e. the process of proving the user’s identity, is one of the basic security mechanisms. It provides a basis to all information infrastructure access control systems (applications, networks, and data).

In many cases, unfortunately, it is precisely the authentication that is the weakest link in information security, as users are asked to prove their identity only based on one element (mostly a combination of username and freely chosen password). Such an approach does not meet modern security challenges and may jeopardize the business.

Therefore, many organizations opt for additional elements of authentication. In such environments, NIL is installing multi-layer authentication methods based on the most advanced technologies (so-called multi-factor authentication). By these, the user is asked to prove his/her identity by submitting at least two of the following elements:

- an item possessed by the user (e.g. authentication device or smart card);
- an item known by the user (e.g. password or PIN);
- an item identifying the user (e.g. fingerprint, voice, other biometric features).

A combined use of several authentication elements significantly increases the level of authentication reliability. These elements depend not only on the user’s choice, while disposal or failure of one component does not allow an identity theft directly.

Achieving a very high level of security, this authentication method is used to control access in many situations. The most common among them are the following:

- authentication for access to home network through public networks (VPN),
- authentication for access to sensible systems and applications,
- authentication for access to management interfaces of infrastructural devices and applications.

BENEFITS
### SOLUTION

**RSA SecurID Two-Factor Authentication System**

Multiple solutions and methods of use are available:

- user device (card or key-chain) generating one-time password based on a software solution for PC and smartphone
- sending a one-time password via SMS

It is very easy to replace or upgrade the existing security system that uses a simple password authentication. The system is user-friendly and very easy to use.

### SOLUTION

**Solutions based on RSA SecurID smart cards**

User device (smart card or smart token)

Strong authentication, digital signature and additional cryptographic services are provided through the public key infrastructure (PKI) for your applications. It enables other cryptographic services, such as digital signing and data encryption.

### USE

**PROPERTIES**